Manuale di conservazione

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	05/10/2015	Roberta Rosatone	*Supporto Archivistico*
Verifica	09/10/2015	Davide Madonnini	*Supporto Archivistico Enti*
Approvazione			

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Vers. 1.0 / Rev. 01	10/10/2015	Prima versione	
Vers. 1.0 / Rev. 02	13/10/2015	Revisione descrizione responsabili	
Vers. 1.0 / Rev. 03	20/10/2015	Revisione descrizione componenti fisiche	
Vers. 1.0 / Rev. 04	14/01/2016	Revisione per osservazioni AGID	
Vers. 1.0 / Rev. 05	16/02/2016	Revisione per osservazioni AGID	
Vers. 1.0 / Rev. 06	03/03/2016	Revisione per osservazioni AGID	

INDICE DEL DOCUMENTO

INDICE DELLE FIGURE

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale descrive il sistema di conservazione dei documenti informatici realizzato sulla base delle 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 di cui al DPCM 3 dicembre 2013.

Esso definisce, in particolare:

- i soggetti coinvolti nel processo di conservazione;
- gli obblighi e le responsabilità;
- l'oggetto della conservazione;
- il processo di conservazione;
- le modalità attuate per garantire la conservazione permanente dei documenti;
- le modalità per ottenere l'esibizione di un documento conservato.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Aggregazione documentale informatica: aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.

Archivio informatico: archivi di documenti memorizzati con procedure informatiche.

Conservatore accreditato: soggetto, pubblico o privato che svolge attività di conservazione dei documenti informatici e certificazione dei relativi processi anche per conto di terzi, che hanno ottenuto l'accreditamento presso l'Agenzia per l'Italia Digitale, come da art. 44bis del vigente CAD.

Disciplinare Tecnico: documento redatto da ogni Produttore, che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione digitale dei Documenti informatici.

Dispositivo sicuro per la creazione di una firma: dispositivi, che utilizzano procedure per la generazione delle firme come da art. 44bis del vigente CAD.

Documento: tutti i libri, le carte, le mappe, le fotografie o gli altri materiali documentari, indipendentemente dalla forma o dalle loro caratteristiche, prodotti o ricevuti da ogni pubblica o privata istituzione, nello svolgimento delle sue funzioni istituzionali o in connessione con la conduzione dei suoi affari particolari, e conservati, o degni di essere conservati, dalla stessa istituzione o dal suo successore, come testimonianza delle sue funzioni, della sua politica, delle decisioni, procedure, operazioni, o altre attività, o a causa del valore informativo dei dati ivi contenuti.

Documento conservato: documento sottoposto al processo di conservazione.

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.

Evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

Fascicolo informatico: aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.

Firma detached: firma digitale che è tenuta separata dai dati firmati, a differenza della firma digitale completa che è inglobata nel file stesso. Ciò permette di poter lavorare con il file originale senza dover aprire un file firmato digitalmente, ma ovviamente una qualsiasi modifica al file originale interrompe lo stretto legame con la firma, nel senso che un file differente non possiederà

la medesima firma (Fonte: Wikipedia).

Firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (CAD).

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 (CAD).

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 (DPR 445/2000).

Funzione di hash: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una 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.

Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (CAD).

Identificativo univoco universale (UUID): universally unique identifier o UUID è un identificativo standard ed è documentato come parte dell'ISO/IEC 11578:1996 "Information technology – Open Systems Interconnection – Remote Procedure Call (RPC)" e più recentemente in ITU-T Rec. X.667 | ISO/IEC 9834-8:2005.

Indice del Pacchetto di archiviazione (IPdA): l'evidenza informatica associata ad ogni Pacchetto di archiviazione, contenente un insieme di informazioni articolate in uno Schema XML (UNISINCRO).

Marca temporale: il riferimento temporale che consente la validazione temporale.

Metadati: elementi che descrivono il contesto, il contenuto e la struttura dei documenti e la loro gestione nel tempo (ISO 15489).

OAIS: ISO 14721:2012: Space data and information transfer systems -- Open archival information system - Reference model, OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

Pacchetto di versamento (SIP): il pacchetto informativo inviato ad un OAIS dal Produttore.

Pacchetto di archiviazione (AIP): il pacchetto informativo conservato in un OAIS..

Pacchetto di distribuzione (DIP): il pacchetto informativo inviato ad un Utente da un OAIS.

Pacchetto informativo (IP): 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.

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.

Riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (D.P.C.M. 30 marzo 2009).

Scarto: operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti per i quali non sussista l'obbligo di conservazione e che siano stati considerati irrilevanti dal punto di vista amministrativa e della ricerca.

Soggetto 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.

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 (CAD).

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 NORMATIVA

- 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;
- Deliberazione della Giunta Regionale n. 1039 del 30 luglio 2008 - Modalità Attuative del Programma Operativo (MAPO) della Regione Marche - POR-FESR - Competitività regionale e occupazione 2007-2013";
- Deliberazione del Consiglio Regionale n. 95 del 15 luglio del 2008 - Piano Telematico Regionale per lo sviluppo della banda larga ed il superamento del digital divide;

- Deliberazione della Giunta Regionale 1759 del 1 dicembre 2008 - Avvio della sperimentazione e dell'analisi finalizzata alla definizione del sistema di conservazione dei documenti cartacei e digitali della Regione Marche;
- Deliberazione della Giunta Regionale n. 252 del 23 febbraio 2009 - Programma Attuativo Regionale PAR FAS 2007-2013;
- Deliberazione della Giunta Regionale n. 1925 del 17 novembre 2009 - Partecipazione al partenariato interregionale con le Regioni Liguria, Piemonte, Lombardia, Emilia Romagna, Marche, Abruzzo, Campania, Puglia, Sicilia e la Provincia Autonoma di Trento ed il CISIS per la cooperazione nella realizzazione del progetto interregionale "PRODE-PROGETTO Dematerializzazione;
- Deliberazione della Giunta Regionale n. 167 del 14 febbraio 2010 - Definizione delle modalità operative di attuazione del polo di conservazione digitale della Regione Marche;
- Decreto della P.F. Sistemi informativi e telematici n. 213/INF_02 del 30 novembre 2010 - Procedura aperta per l'acquisizione di beni e servizi per la creazione e gestione del Polo regionale di conservazione degli archivi digitale;
- Decreto della P.F. Sistemi informativi e telematici n. 119/INF del 22 agosto 2012 – Aggiudicazione della procedura aperta e costruzione dell'infrastruttura organizzativa, tecnologica e giuridica per l'avvio dei servizi di archiviazione digitale a norma;
- Deliberazione della Giunta Regionale n. 265 del 10 marzo 2014 - Avvio dei servizi del Polo di conservazione digitale Marche DigiP;

Torna al sommario

3.2 STANDARD

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and

Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- ISO 15489 Record management – Code of practice

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Il DPCM 3 dicembre 2013 individua, all'art. 6, i seguenti ruoli: Produttore, Utente e Responsabile della conservazione.
Il Produttore, nelle PA identificato con la figura del responsabile della gestione documentale, produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
L'utente è colui 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 suo interesse.
Il Responsabile della conservazione, è il soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione. Il Responsabile della conservazione può affidare le attività definite previste dall'art. 7 del DPCM 3 Dicembre 2013 al Responsabile del servizio di conservazione.
Nel seguito è esplicitato l'assetto dei ruoli e delle responsabilità all'interno del Polo DigiP.

Ruolo	Nominativo	Attività associate al ruolo	Note
Responsabile del servizio di conservazione	Serenella Carota	- 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.	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile della funzione archivistica di conservazione	Mauro Ercoli	- 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;	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015

		- 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.	
Responsabile del trattamento dei dati	Massimo Trojani	- 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	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile della sicurezza dei sistemi per la conservazione	Maria Laura Maggiulli	- 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.	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile dei sistemi informativi per la conservazione	Cinzia Amici	- 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	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo addendum contrattuale del 22/12/2015
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Cinzia Amici	- 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	Funzioni parzialmente delegate: contratto n. 1212 del18/09/2012 e relativo

		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.	addendum contrattuale del 22/12/2015

Torna al sommario

4.1 PUBBLICO UFFICIALE

Il ruolo di Pubblico Ufficiale è svolto da personale di Regione Marche appositamente designato.
Il ruolo di Pubblico Ufficiale, per i casi in cui è previsto l'intervento di soggetto diverso della stessa amministrazione, sarà svolto da altro dirigente all'uopo individuato o da altro soggetto da quest'ultimo designato.

Torna al sommario

4.2 CERTIFICATION AUTHORITY

I certificarti di firma digitale utilizzati nel processo di conservazione sono forniti da Actalis S.p.A.

Torna al sommario

4.3 SOPRINTENDENZA ARCHIVISTICA PER LE MARCHE

Esercita funzioni di tutela e vigilanza sugli archivi degli enti pubblici territoriali e non e di enti privati dichiarati di interesse storico particolarmente importante (ai sensi dell'art. 4 e dell'art. 18 del D.lgs. 22 gen. 2004, n. 42 Codice dei beni culturali e del paesaggio e successivi aggiornamenti), autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 42/2004.

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 ORGANIGRAMMA

Il polo archivistico DigiP svolge per conto degli enti convenzionati il servizio di conservazione dei documenti e degli archivi informatici, con la finalità principale di garantirne la validità giuridica, attivando i trattamenti previsti dalla normativa in vigore. Allo scopo di garantire tale servizio il Polo si avvale di un sistema applicativo e di un'apposita organizzazione con personale altamente qualificato e del supporto di esperti esterni di comprovata esperienza in materia, dotati di competenze specializzate.

Figura 1 – Organigramma

Torna al sommario

5.2 STRUTTURE ORGANIZZATIVE

A supporto della struttura organizzativa indicata precedentemente il modello organizzativo sotteso al Polo Regione Marche DigiP prevede l'interazione dei seguenti soggetti:

- **Ente produttore**: produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di. Il rapporto tra soggetto produttore e Polo Marche DigiP è disciplinato da specifici contratti di servizio; può richiedere i servizi di consulenza offerti dalla Unità di Gestione del Polo per la definizione delle politiche di dematerializzazione e conservazione.

- **Comitato Regionale Utilizzatori (CRU)**: è un comitato inter-ente formato dalla Regione Marche e da altri enti del territorio rappresentativi delle diverse tipologie di soggetti che interagiscono con il Polo Marche DigiP; collabora alla valutazione dei livelli qualitativi dei servizi offerti (*customer satisfaction*), all'identificazione delle esigenze degli utilizzatori e alla formulazione di eventuali richieste di servizio e/o proposte di miglioramento.

- **Comitato Scientifico (CS)**: definisce gli indicatori e gli strumenti per assicurare la qualità dei servizi erogati; approva la documentazione elaborata dall' Unità di Progettazione, il piano di audit e monitoraggio; assicura il monitoraggio della evoluzione tecnologica, normativa e degli standard fornendo il know how per l'aggiornamento del modello conservativo e tecnologico.

- **Unità di Progettazione (UP)**: è formata da figure professionali che dispongono delle necessarie competenze giuridiche, archivistiche, informatiche e da referenti di dominio nelle aree tematiche per le quali si registra la maggiore produzione di documenti informatici (salute, servizi a cittadini/imprese, gestione delle risorse umane, strumentali e materiali, atti amministrativi). All'Unità di Progettazione è demandata:
    - l'elaborazione delle procedure e i processi che costituiscono il modello conservativo digitale del Polo;
    - la definizione ed implementazione del piano self-audit, di monitoraggio e di documentazione dell'attività;
    - la definizione e progettazione e pianificazione dell'aggiornamento tecnologico e professionale del personale del Polo Marche DigiP;
    - l'elaborazione degli schemi di contratto di servizio;
    - la supervisione e il coordinamento delle attività dell'Unità di Gestione e dell'Unità Data Center.

- **Unità di Gestione (UG)**: implementa e gestisce il modello conservativo digitale disegnato dall'Unità di Progettazione; rende disponibile un servizio di help desk sulle tematiche di archiviazione e conservazione, interagendo con gli enti produttori.

- **Unità Data Center**: è formata da figure professionali idonee che svolgono le attività di natura tecnologica assicurando il corretto funzionamento del Polo Marche DigiP con modalità e tempi definiti dai responsabili del sistema.

Per rispondere altresì agli orientamenti governativi nazionali ed europei in materia di Agenda digitale e nel contempo dare piena operatività ai servizi di DigiP, è stata istituita la Community network degli enti utilizzatori dei servizi denominata **DigiPCommunity**, ovvero una comunità dinamica di settore che si aggrega secondo un modello a geometria variabile e condivide le informazioni contenute nella knowledge base attenendosi ad ontologie semantiche. Tale community promuove ai fini della conservazione di archivi digitali:

- il trasferimento tecnologico e lo scambio di conoscenza tra i portatori di interesse del sistema;
- la fornitura di strumenti condivisi per superare il limite attuale dei processi di automazione dei procedimenti amministrativi;
- funzioni di promozione sul territorio per creare un potenziale bacino di utenti consapevoli dei reali vantaggi del modello di lavoro a rete che vede DigiP come infrastruttura abilitante.

Il servizio riguarda principalmente, ma non esclusivamente, i documenti sottoscritti con firma digitale, ed ha inizio nel momento in cui il documento entra nel patrimonio documentario dell'ente. Il servizio ha come output primario la restituzione da parte del conservatore di documenti correttamente conservati, principalmente per finalità di esibizione.

Il servizio riguarda i documenti digitali e costitutivi dell'archivio informatico dell'ente (con particolare attenzione per il documenti sottoscritti con firma digitale).
Il servizio fornisce attività finalizzate a garantire un primo consolidamento dei documenti informatici e delle loro aggregazioni per l'eventuale esibizione (soprattutto con riferimento alle categorie individuate in seguito) e per supportare i successivi processi di conservazione nel tempo a fini amministrativi e di ricerca e previe operazioni di selezione e scarto.

L'applicativo dell'ente versante può eseguire il versamento del documento in conservazione (e dei metadati di contesto amministrativo e archivistico) nel momento in cui questo viene acquisito nell'archivio corrente dell'Ente oppure eseguire il versamento in un momento successivo, attraverso un'estrazione dei documenti presenti in archivio (tipicamente con una procedura batch). Il modello si riferisce sia ai documenti che costituiscono l'archivio, quindi sia quelli interni prodotti all'interno dell'ente (mantenuti internamente o spediti a soggetti terzi), sia i documenti ricevuti da soggetti terzi in varie modalità.

La realizzazione del sistema di conservazione è basata sul modello di OAIS e garantisce la conservazione di documenti digitali per conto di più enti e organizzazioni assicurando i più elevati livelli di sicurezza.

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 OGGETTI CONSERVATI

Di seguito vengono elencate le tipologie di documenti per la cui accettazione è attualmente configurato il sistema di conservazione DigiP:

- Documento protocollato
- Documento non protocollato
- Registro giornaliero di protocollo

Il Polo Marche DigiP accetta i formati elencati nell'Allegato n. 2 al DPCM 3/12/2013 e, inoltre, è in grado di gestire, su richiesta del soggetto produttore e previa valutazione e approvazione da parte del Polo Marche DigiP, anche formati non compresi nel suddetto elenco, ma specificati nel manuale di conservazione del soggetto produttore e riportati nel disciplinare tecnico.
Per i file opportunamente elencati nel disciplinare tecnico, che sono trasmessi al sistema di conservazione in un formato diverso da quelli specificati secondo il processo precedentemente descritto sarà garantita esclusivamente la ricerca e il recupero con garanzia dell'integrità binaria.

Per quanto riguarda i metadati si fa riferimento all'Allegato n. 5 del DPCM 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione.
Per quanto riguarda le politiche di conservazione si rimanda alle specificità del contratto definite nel Disciplinare Tecnico.

Torna al sommario

6.2 PACCHETTO DI VERSAMENTO (SIP)

Il Sistema di conservazione DigiP è stato progettato per accogliere Pacchetti di versamento (SIP – Submission Information Package) disegnati principalmente secondo lo standard SINCRO.
Tuttavia il sistema è altamente configurabile e personalizzabile ed è quindi in grado di accogliere qualsiasi tipo di Pacchetto di Versamento, garantendo in tal modo un elevato livello di flessibilità. Questa caratteristica ha permesso fin da subito la compatibilità (sebbene con alcune limitazioni, ad esempio il vincolo di 1 SIP => 1 documento) con il Sistema di conservazione preesistente.
Il SIP è definito da:

- un contenitore, dipendente dal canale trasmissivo scelto, che racchiude i contenuti del pacchetto informativo (es: file in formato zip, HTTP Request di tipo POST ...);
- un file XML, descrittore del contenuto, dei metadati del Produttore e delle eventuali aggregazioni; detto indice può essere validato contro il proprio schema XSD;

- l'insieme dei file elencati nell'indice, con i propri metadati.

Il caricamento di un pacchetto di versamento (SIP) può avvenire in tre diverse modalità, dipendentemente dagli accordi di servizio:

- **Flusso**: i pacchetti SIP, definiti come file .zip, vengono posizionati in una specifica cartella ftp assegnata all'utente (Soggetto Produttore). Il sistema tramite periodici controlli troverà il file e avvierà il processo di versamento.
- **Form web**: l'utente versatore, autenticato ed autorizzato, inserisce tramite apposita form del sistema il testo dell'indice descrittore in una casella di testo e allega i file associati.
- **Interfaccia REST**: l'applicazione versante, autenticata ed autorizzata, trasmette al sistema i pacchetti di versamento utilizzando l'apposita interfaccia webservice REST.

Il Soggetto produttore avrà la possibilità di monitorare in tempo reale la gestione dei Pacchetti di versamento tramite apposito portale al quale potrà accedere con credenziali personali fornite dal Polo. Il portale DigiP permette, infatti, di controllare la Data del versamento, i documenti Ricevuti, i documenti Presi in carico, il Rapporto di versamento e i Pacchetti di Archiviazione. Informazioni, queste, racchiuse in un Registro dei pacchetti che è possibile scaricare in formato excel, che riportano i dettagli dei Pacchetti e dei log. Dal medesimo portale sarà possibile visualizzare anche i Pacchetti di Distribuzione.
Per i dettagli tecnici si rimanda al documento allegato "Manuale di Utilizzo DigiP".

Torna al sommario

6.3 PACCHETTO DI ARCHIVIAZIONE (AIP)

Il sistema di conservazione DigiP è conforme allo standard OAIS ISO 14721:2012 e in particolare per tutto quanto riguarda l'acquisizione dei Pacchetti di Versamento (SIP- Submission Information package) e la loro trasformazione in Pacchetti di archiviazione (AIP - Archival Information Package).

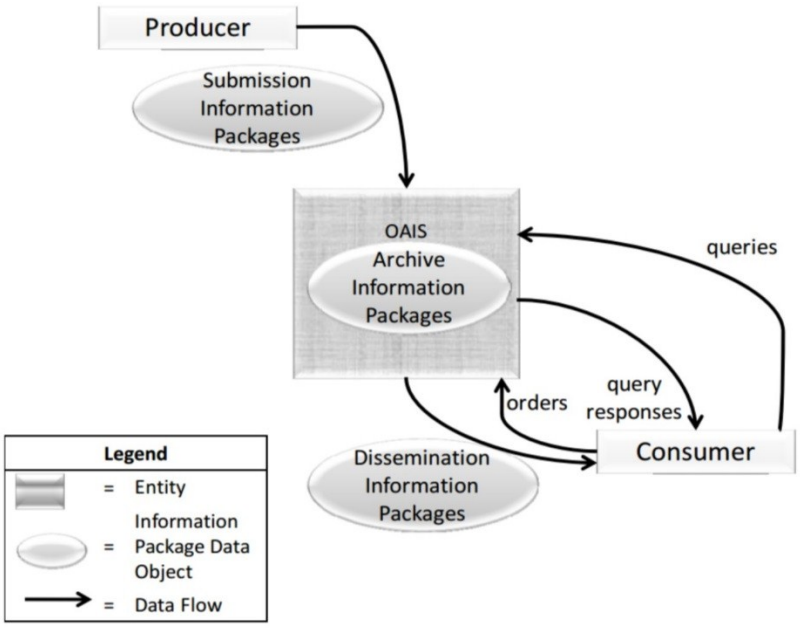

Figura 2 - Modello OAIS

Il sistema di conservazione DigiP individua nella fase di Ingest il momento in cui il SIP conferito dal Soggetto Produttore viene validato e quindi trasformato in AIP. Durante questo processo non banale, i risultati delle validazioni e delle conversioni di formato richieste dagli accordi di servizio e dalle politiche prestabilite vengono raccolti e aggregati in una struttura di IP idonea alla successiva generazione dei corrispondenti Pacchetti di archiviazione. Questa struttura transitoria identificata come KIP – Kernel Information Package - è indipendente dai formati scelti per l'archiviazione. La struttura di questi ultimi segue lo standard SINCRO così come indicato nelle Regole tecniche in materia di conservazione.

Si riporta di seguito la struttura dell'indice del Pacchetto di Archiviazione:

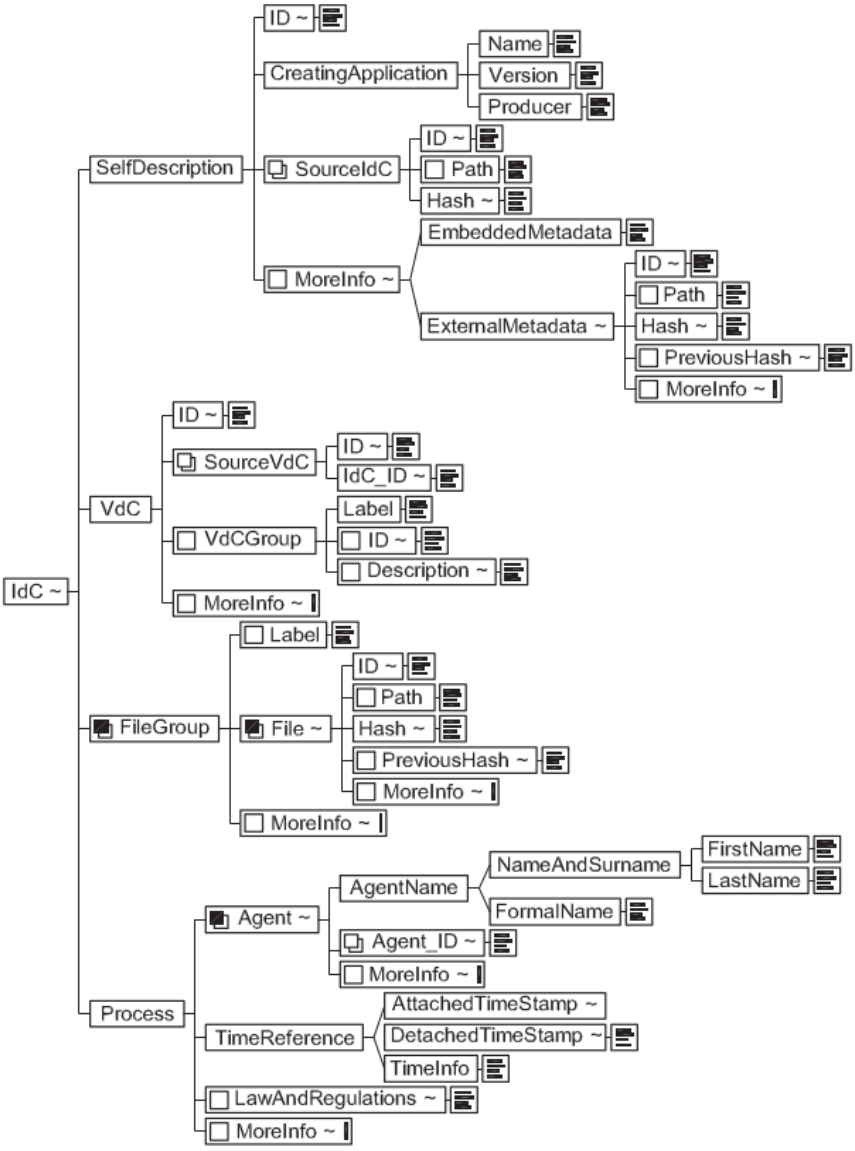

Figura 3 - Indice PdA

Il tag MoreInfo nella struttura SINCRO rappresenta la naturale estensione dello schema e nell'implementazione attuale del Sistema accoglie le tipologie di metadati previste dal modello OAIS che non sono contemplati da SINCRO e tutti i metadati descrittivi specifici del documento aggiunti dal Produttore.

Torna al sommario

6.4 PACCHETTO DI DISTRIBUZIONE (DIP)

I pacchetti di distribuzione (DIP – Dissemination Information Package) vengono creati a seguito

della richiesta da parte di un utente.
Per la formazione di tali pacchetti il sistema DigiP effettua un processo di riconversione dall'AIP al KIP.

La struttura del DIP è conforme allo standard SinCRO, soprattutto per quanto riguarda l'interoperabilità con altri sistemi di conservazione.
Per gli utenti consultatori tale struttura è dipendente anche dagli accordi fra il Polo DigiP ed il produttore dei documenti

Per i dettagli della struttura del DIP e le politiche di distribuzione si rimanda agli allegati "Manuale di Utilizzo DigiP" e "Disciplinare Tecnico".

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

Il sistema di conservazione DigiP, conforme allo standard OAIS è composto dalle seguenti aree funzionali:

1. INGEST, dove si tratta il flusso di documenti dal Produttore al Polo;
2. ARCHIVAL STORAGE, che racchiude le funzionalità di base per garantire la persistenza dei documenti;
3. DATA MANAGEMENT, l'unità di gestione dei metadati e del catalogo di ricerca;
4. ADMINISTRATION, per la gestione del Sistema da parte degli Amministratori;
5. PRESERVATION PLANNING, funzionalità di previsione e monitoraggio degli utenti e degli oggetti del Sistema;
6. ACCESS, dove si gestisce il flusso di richieste di documenti in uscita e la ricerca da parte del Consumatore.

Nel seguito sono descritte le funzioni dei processi di gestione relativi alle suddette aree funzionali.

Torna al sommario

7.1 INGEST

Questa area funzionale è costituita dall'insieme dei processi che sovraintendono l'accettazione delle risorse digitali inviate dai Produttori e della loro preparazione per l'inclusione nel sistema di archiviazione.
I suoi passi procedurali sono descritti nei paragrafi successivi.

Torna al sommario

7.1.1 Trasferimento di SIP

Passi procedurali:

- il Produttore trasmette il SIP nei modi definiti dall'accordo formale (memorizzato nel Sistema sotto forma di configurazione specifica del Produttore), in particolare il Produttore può scegliere se utilizzare un flusso di deposito all'interno di una zona di memorizzazione condivisa (file system remoto, FTP, etc..) oppure un servizio REST di versamento asincrono;
- il Sistema rileva un nuovo trasferimento e
    - verifica la corrispondenza tra il Soggetto Produttore indicato nei metadati del SIP con l'utente versatore che ha conferito il pacchetto stesso e ne lascia traccia tra i log

applicativi. In caso di controllo positivo il SIP viene validato formalmente e in caso di conformità:

- trasferisce il SIP localmente al servizio di ricezione: indipendentemente dal metodo di conferimento scelto dal Produttore, i Pacchetti Informativi vengono depositati in una zona temporanea di lavoro appositamente configurata e segregata sulla base del nome in codice (scelto univocamente all'interno del Sistema) del Produttore;
- trasferisce il SIP ad Archival Storage nella sezione corrispondente e ne notifica la ricezione al Produttore aggiungendolo alla lista dei SIP ricevuti ricevuti (documento csv – registro giornaliero dei sip versati per Soggetto Produttore);
- il SIP ricevuto viene messo in coda per la validazione di qualità (UC 1.2);

o i SIP non attribuibili ad alcun Soggetto Produttore o non conformi vengono spostati in una zona terminale (denominata "cestino") per le valutazioni in merito alle cause di mancata conformità da parte degli Utenti abilitati. Si prevede un periodo configurabile di ritenzione dei SIP cestinati, trascorso il quale saranno eliminati fisicamente dal Sistema senza ulteriori formalità.

- il Produttore può consultare la lista dei SIP ricevuti dal Sistema, lista presente sia nell'area di deposito condivisa (condivisa tra Soggetto Produttore e Polo) che nell'area Ingest accessibile dal sito web, e verificarla.

Quando il trasferimento è completato il Sistema abilita i successivi casi d'uso.

Torna al sommario

7.1.2 Quality Assurance

Passi procedurali:

- il Sistema processa la coda dei SIP ricevuti sottoponendoli all'analisi dei formati dei file in essi contenuti ed alla verifica delle eventuali firme digitali con conseguente recupero dei dati dei firmatari;
- il Sistema recupera le Regole da applicare per la validazione in base al Produttore e alla tipologia documentale;
- il Sistema valida il trasferimento del SIP applicando le regole di validazione attive selezionate al passo precedente utilizzando i risultati delle analisi dei formati e delle verifiche già effettuate;

- i dati derivati dalla validazione confluiranno sia nel Rapporto di versamento, sia tra i metadati del futuro AIP;
- il Sistema emette, a seconda dell'esito della validazione, una ricevuta di presa in carico (validazione positiva) oppure una comunicazione di anomalia (validazione negativa con descrizione delle anomalie) opzionalmente firmata (Rapporto di Versamento, per i contenuti vedi figura) a disposizione del Produttore sia nella zona di deposito condivisa che scaricabile dall'interfaccia web. Prima dell'apposizione eventuale della firma digitale, il Rapporto di versamento è (opzionalmente) protocollato dal Sistema di Protocollo dell'Ente Polo. La segnatura di protocollo così ottenuta rappresenta un valido riferimento temporale opponibile a terzi in quanto il Sistema di Protocollo che lo ha prodotto è il Protocollo Informatico di un ente pubblico. La marcatura temporale ottenuta per tramite del Protocollo viene mantenuta in associazione con il SIP e inclusa tra i metadati del Pacchetto di Archiviazione prima della necessaria apposizione della firma digitale del Conservatore. Il Rapporto di Versamento viene inoltre aggiunto al contenuto informativo del SIP originale. Questa parte del processo di acquisizione garantisce la qualità del trasferimento nei confronti di Terzi.

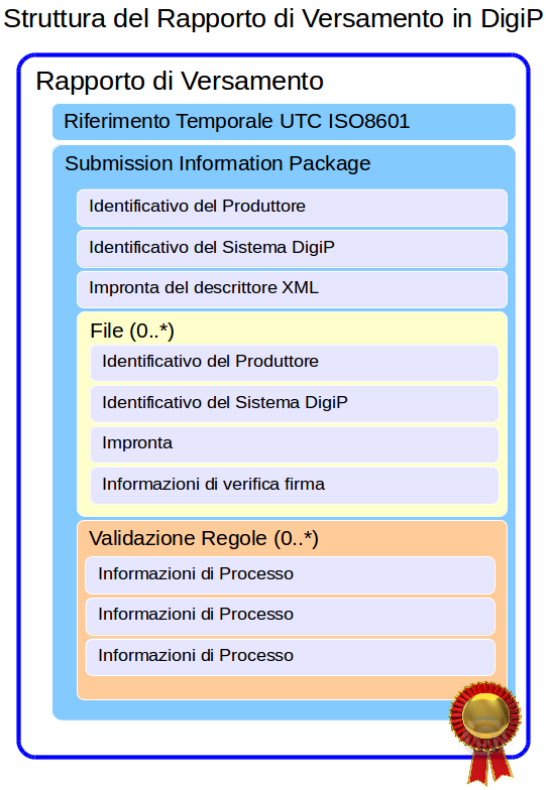

Figura 4 - Struttura RdV

- in caso di successo il Sistema abilita il SIP per il passo successivo.

Torna al sommario

7.1.3 Generazione di AIP

Passi procedurali:

- il Sistema riceve la posizione temporanea nella zona di lavoro del SIP validato e spacchettato;
- il Sistema estrae il contenuto informativo dal SIP e lo inserisce in una struttura di IP in formato interno universale KIP (Kernel Information Package):
    - il Sistema estrae le informazioni descrittive di conservazione (PDI) dal SIP e le aggiunge al KIP;
    - il Sistema integra eventualmente i PDI estratti con modifiche o inserimenti nel KIP;
    - il Sistema recupera le politiche e gli standard di archiviazione;
    - il Sistema, sulla base delle politiche e degli standard, esegue le necessarie conversioni, trasformazioni, riorganizzazioni sul SIP corrente e ne salva temporaneamente i risultati nel KIP;
    - al termine del processo di generazione la documentazione delle operazioni effettuate sul SIP viene inserita nel KIP
- il KIP viene trasformato tramite XSLT nel formato di IP scelto (attualmente lo standard ISO SINCRO), per come è stato progettato il ruolo del KIP tale trasformazione è reversibile;
- il Sistema abilita il KIP al passo di generazione PDI verso Data Management (compilazione del catalogo di ricerca con le chiavi dei metadati);
- in caso di successo complessivo il Sistema contrassegna l'IP come conforme agli accordi negoziati di (formato di) versamento, con il risultato che il Sistema ha generato un AIP a partire dal SIP; l'AIP testé generato viene persistito dall'Archival Storage ed associato ad un identificativo univoco della posizione di memorizzazione;
- eventuali fallimenti occorsi durante il processo sono tracciati nello stato di avanzamento da SIP ad AIP, lasciando all'utente Amministratore la possibilità di ripristinare la situazione ad un punto noto e rilanciare il processo stesso.

Torna al sommario

7.2 ARCHIVAL STORAGE

La funzione gestisce l'immagazzinamento a lungo termine delle risorse digitali affidate al sistema. Si tratta di un'area funzionale non direttamente acceduta dagli Utenti del sistema e pertanto il suo ruolo è accennato sinteticamente di seguito.

Alla richiesta di memorizzazione di un contenuto informativo proveniente dall'area funzionale Ingest, il Sistema seleziona e prepara il corretto dispositivo di memorizzazione recuperando l'informazione dalla configurazione del Soggetto Produttore e si predispone per ricevere l'informazione in streaming. Al termine del trasferimento dello stream di informazioni il Sistema notifica al chiamante la correttezza della procedura comunicando l'identificativo univoco sotto il quale è memorizzato il contenuto informativo.
L'identificativo unico del contenuto informativo memorizzato all'interno di Archival Storage è rappresentato dall'indirizzo univoco composto da:

- un identificativo unico universale che contiene riferimenti al partizionamento ed alla segregazione;
- una gerarchia a otto livelli derivata dal partizionamento di un UUID;
- l'impronta del contenuto informativo.

Il recupero dei contenuti memorizzati all'interno di Archival Storage avviene sempre tramite l'identificativo unico della risorsa.

Completano le funzionalità di memorizzazione e di recupero delle informazioni la funzione amministrativa di controllo degli errori e di calcolo delle statistiche di memorizzazione.

Torna al sommario

7.3 DATA MANAGEMENT

La funzione di Data Management gestisce il database dei metadati (descrittivi e PDI) inclusi nel catalogo di ricerca ed i dati amministrativi e statistici del sistema.
Il suo ruolo all'interno del processo di conservazione è finalizzato al mantenimento di informazioni sul processo stesso, che verranno incluse tra i metadati dell'IP, e all'ottimizzazione (denormalizzazione rispetto al pacchetto di archiviazione) dei percorsi di ricerca mediante chiavi multiple.
La natura dinamica del Data Management permette inoltre di tracciare il log forensico delle attività in corso sull'intera applicazione Polo DigiP e di restituire reportistiche in tempo reale. Il report può essere di due tipologie: generato da una ricerca per metadati (access) o dall'analizzatore pianificato di coerenza e integrità con i dati statistici (numero file, dimensione file…) accessibile da Administration.
Il data management è specifico dell'applicativo e non gestisce i dati rilevanti alla conservazione.

Torna al sommario

7.4 ADMINISTRATION

L'area funzionale Administration raggruppa l'insieme delle funzioni rivolte alla gestione delle configurazioni del Sistema, al monitoraggio, all'interazione con gli utenti, agli accordi di servizio con i produttori ed al mantenimento degli standard di archiviazione definiti.

Torna al sommario

7.4.1 Negoziazione accordo di versamento

Opera sulla base delle politiche di versamento negoziate tra il Produttore ed il Polo Marche DigiP in particolare:

- il Sistema mantiene la configurazione della struttura dei SIP;
- il Sistema mantiene la configurazione dei parametri di interazione tra Soggetto Produttore e l'Applicazione Polo DigiP;
- il Sistema valuta il design del SIP come parte del processo di approvazione del versamento.

Nota: l'ultimo passo è implementato tramite la SandBox nel modulo di Preservation Planning.

Torna al sommario

7.4.2 Monitor della configurazione del Sistema

Si tratta di una funzione di monitoraggio del sistema che richiama funzionalità sviluppate nei rispettivi moduli di competenza, in particolare:

- il Sistema raccoglie informazioni di sistema dal modulo Data Management;
- il Sistema raccoglie statistiche dal modulo Archival Storage;
- il Sistema permette di monitorare le operazioni di sistema;
- il Sistema permette di monitorare l'utilizzo di sistema.

Il sistema archivio viene valutato nelle configurazioni correnti.

Torna al sommario

7.4.3 Definizione di standard e politiche

Il Sistema permette di configurare gli standard e le politiche sulla base delle informazioni ricevute, tra cui:

- Formati

- Documentazione e metadati descrittivi
- Obiettivi della migrazione
- Politiche di gestione della memorizzazione
- Politiche di migrazione
- Politiche di sicurezza
- Politiche di evoluzione del Sistema

Torna al sommario

7.4.4 Visualizzazione degli AIP

Si tratta di una funzionalità di monitoraggio sul processo di conservazione, grazie alla quale l'AIP è reso in formato ispezionabile.

Torna al sommario

7.4.5 Processo di Scarto AIP

Si tratta di una funzione avanzata di gestione del patrimonio informativo già acquisito, prevista dalla normativa. Quando si creano i presupposti l'Amministratore crea un nuovo processo di scarto, specificando gli estremi del documento di autorizzazione allo scarto. A questo punto il processo è in corso e:

- il Sistema identifica gli AIP scartabili in base al massimario di scarto (vedi configurazione della tipologia documentale);
- l'Amministratore seleziona per lo scarto tra gli elementi identificati al passo precedente;
- al termine della selezione (multipla) l'Amministratore lancia il processo (asincrono) di scarto;
- il Contenuto Informativo dell'AIP è rimosso fisicamente dal Sistema, insieme a tutti i SIP e i DIP corrispondenti. Il rapporto prodotto al termine del processo di scarto viene mantenuto nel Sistema ed associato ai metadati degli AIP scartati.

In 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, secondo quanto disposto dall’art. 21, comma 1, lettera d del Codice dei beni culturali.

Torna al sommario

7.4.6 Migrazione

In ogni momento la funzione di migrazione è attivabile per singolo Produttore: di ogni file di formato obsoleto viene creata una versione in formato migrato che lo sostituisce in una nuova revisione del AIP.

Torna al sommario

7.4.7 Riversamento

Tutti gli AIP sono resi disponibili sotto forma di DIP standard, per essere riversati su un nuovo Sistema di conservazione, senza eliminare alcuna informazione dal Sistema corrente.

Torna al sommario

7.5 PRESERVATION PLANNING

E' l'area funzionale che si occupa della progettazione della strategia di conservazione del sistema e delle sue modifiche a fronte dei cambiamenti tecnologici riguardanti gli oggetti archiviati e del mutamento dei bisogni espressi dalla Comunità di riferimento.

Torna al sommario

7.5.1 Osservazione della Comunità designata

E' una funzionalità di indagine/feedback mediante questionari. Gli attori sono il Sistema Polo Marche DigiP, il Produttore, il Consumatore.
La procedura invia le specifiche di conservazione al modulo funzionale che si occupa di design del packaging e di piani di migrazione; invia reports, avvisi e standard emergenti al modulo funzionale di sviluppo strategie di conservazione.

Torna al sommario

7.5.2 Prototipazione

La funzione è svolta dal componente del sistema denominato SandBox ed è una funzione ad euristica esplorativa. Il risultato della prototipazione è disponibile istantaneamente per essere esportato in ambiente di produzione.

Torna al sommario

7.5.3 Sviluppo di strategie di conservazione

Sono funzioni parzialmente automatizzabili, per le quali si prevede l'uso massivo della SandBox.

Torna al sommario

7.5.4 Sviluppo di standard di conservazione

La funzionalità, appoggiandosi sempre sul componente SandBox, segue il medesimo iter della Prototipazione.

Torna al sommario

7.5.5 Sviluppo di standard di migrazione

E' un insieme di funzioni eterogenee per le quali viene fornito a tecniche "what-if" esplorabili tramite la SandBox durante le fasi di prototipazione e design, sia degli IP che del software di trasformazione/migrazione di standard di formato per l'IP.
La funzionalità mette istantaneamente a disposizione dell'utente amministratore gli artefatti studiati, per l'installazione in ambiente reale di produzione.

Torna al sommario

7.5.6 Sviluppo di Packaging design

E' una funzione basata sulle funzionalità di indagine fornite dalla SandBox e consente di produrre AIP/SIP destinati a implementare l'accordo di versamento.

Torna al sommario

7.6 ACCESS

Attraverso l'area funzionale Access gli utenti del sistema possono ricercare, richiedere ed ottenere i diversi tipi di oggetti informativi conservati dal sistema stesso. Rappresenta inoltre il canale preferenziale per il monitoraggio della Comunità di Riferimento, attraverso il quale vengono somministrati i questionari e forniti i feedback.

Torna al sommario

7.6.1 Generazione di DIP

La funzione, a seguito di una richiesta specifica da parte di un utente, recupera l'AIP ricercato/selezionato e genera un DIP, notificando il completamento del recupero al modulo di

accesso. Durante questo processo non banale i risultati delle conversioni di formato richieste dagli accordi di servizio e dalle politiche prestabilite vengono raccolti e aggregati in una struttura di IP idonea alla successiva generazione dei corrispondenti Pacchetti di Distribuzione.
Questa struttura transitoria identificata come KIP – Kernel Information Package - è indipendente dai formati scelti per la disseminazione e viene gestita in un'apposita area di lavoro dedicata. Il processo di trasformazione da AIP a KIP è la funzione inversa della trasformazione da KIP ad AIP: questo garantisce coerenza e consistenza ai pacchetti destinazione.
La struttura del Pacchetto di Distribuzione segue lo standard SINCRO, così come indicato nelle Regole tecniche in materia di conservazione, per interoperabilità tra Conservatori. Resta comunque possibile configurare una diversa conversione per tutti i casi in cui sia necessario adeguare i Pacchetti di Distribuzione alla Comunità di riferimento.
I Pacchetti così costituiti sono resi disponibili per la fruizione singolarmente via web o attraverso un canale FTP dedicato in via massiva, ma senza precludere la possibilità di accordo di servizio per la fornitura di supporti rimovibili (CD, DVD, BlueRay ...), in alternativa al canale FTP.
E' inoltre possibile prevedere un tempo massimo di ritenzione dei Pacchetti di Distribuzione, tempo oltre il quale i DIP possono essere eliminati dal Sistema.

Torna al sommario

7.7 RICHIESTE DI DUPLICATI E COPIE INFORMATICHE DEI DOCUMENTI CONSERVATI, ATTESTAZIONE DI CONFORMITÀ

Il modulo Access consente agli utenti autorizzati di ottenere una copia (o duplicato, nel caso in cui non siano necessarie conversioni di formato) dei documenti conservati tramite la richiesta di generazione DIP. Al momento non è prevista l'espressa richiesta di attestazione di conformità per i documenti prodotti dalla disseminazione pertanto, ove richiesto, si procederà esternamente al Sistema con la creazione di un supporto (CD, DVD, e-mail …) contenente sia il DIP che l'attestazione richiesta nella forma attualmente ritenuta valida ai fini legali. Il sistema può fornire tutti gli elementi necessari ad evadere simili richieste (ad es.: impronta Hash del DIP, etc.).

Nel caso in cui venga richiesto l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal Responsabile del servizio di conservazione.
Si precisa che tali supporti fisici non presentano riferimenti esterni tali da permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia. Inoltre, il tipo di contenitore individuato per i DIP permette di impostare credenziali crittografiche tali da proteggere i dati in essi contenuti limitatamente alla distribuzione tramite supporti fisici.

Torna al sommario

7.8 PREDISPOSIZIONE DI MISURE A GARANZIA DELL'INTEROPERABILITÀ E TRASFERIBILITÀ AD ALTRI CONSERVATORI

Il Sistema di conservazione DigiP è pienamente conforme al dpcm 3 dicembre 2013 e rispondente all'art. 9 comma 1, lett. h), nel quale viene dichiarato che il sistema di conservazione garantisce "ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione". DigiP, infatti, assicura l'interoperabilità e la trasferibilità sia in fase di acquisizione dei Pacchetti da parte di altro conservatore, sia in fase di trasmissione ad altro soggetto conservatore. DigiP, inoltre, come specificato in precedenza, risponde allo standard UNI 11386:2010 SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

8.1 COMPONENTI LOGICHE

Il processo di conservazione è realizzato tramite il sistema DigiP che si compone dei moduli descritti precedentemente:

- Ingest
- Archival Storage
- Data management
- Administration
- Preservation Planning
- Access

Di seguito lo schema rappresentativo delle aree funzionali di DigiP. Si noti a tale proposito come le aree funzionali di base (Archival Storage e Data Management) corrispondano - nella metafora di un Sistema vivente - ai piedi del Sistema, le aree funzionali responsabili delle operazioni di I/O siano le braccia, l'area di amministrazione identificata dalle funzioni razionali del cervello ed il cuore dell'Archivio – l'area Preservation Planning.

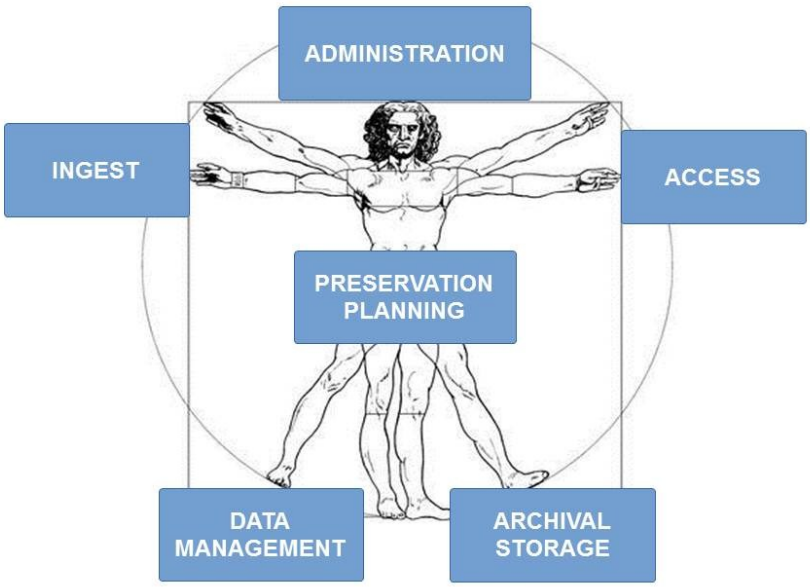

Figura 5 – Aree funzionali DigiP

La soluzione implementata per il Sistema Polo Marche DigiP combina e armonizza i seguenti pattern emergenti:

- Domain driven design component-based (per la parte generale), consente di rilasciare in successione moduli verticali come componenti dell'applicazione garantendo comunque i passi di integrazione con il software prodotto. Il partizionamento del dominio in contesti limitati e aggregati è naturale conseguenza della riorganizzazione delle classi del dominio.
- CQRS-based (per le parti comuni), la diversificazione dei percorsi di lettura e scrittura segue la struttura tipica del modello OAIS e ne rinforza l'implementazione aderente allo standard.

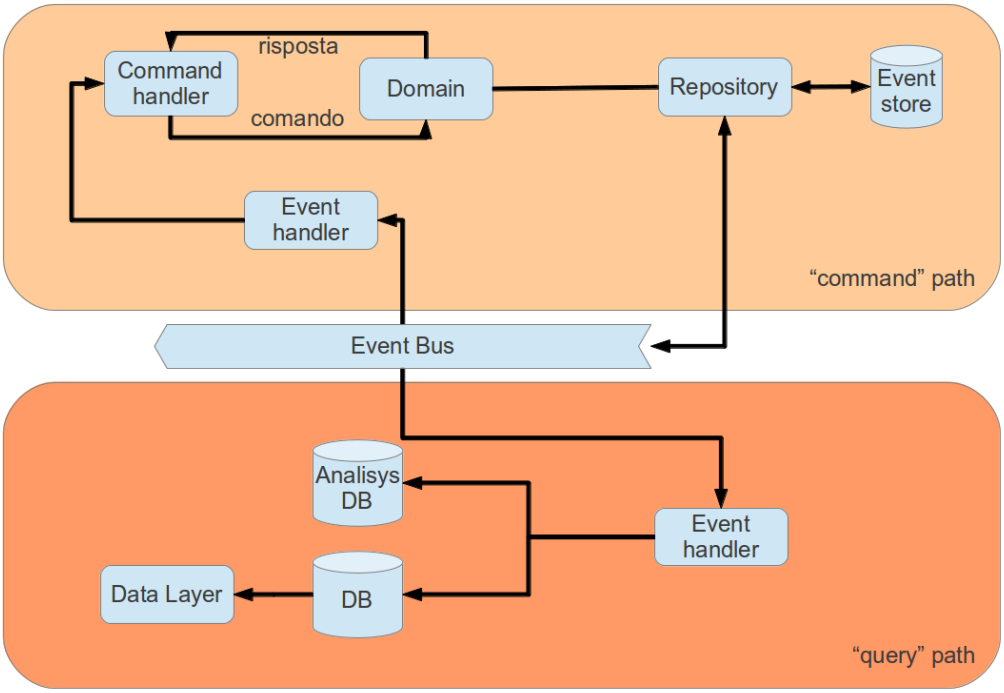

Figura 6 – Schema di principio del Pattern Command Query Responsibility Segregation (CQRS)

- Event Driven (per le parti di comunicazione inter-processo), il disaccoppiamento esteso anche ai processi e la scelta di un modello di comunicazione asincrono aumenta la scalabilità complessiva e riduce l'incidenza del single-point-of-failure.
- Rule-based (per le parti decisionali), la scrittura delle regole di business in una forma comprensibile all'uomo e che mantiene la possibilità di elaborazione automatica e condizionale realizza il requisito di flessibilità e di configurabilità, permettendo allo stesso tempo al Sistema Polo Marche DigiP di essere sempre in linea con le tecnologie e la Comunità di riferimento.

Torna al sommario

8.2 COMPONENTI TECNOLOGICHE

L'immagine che segue schematizza dal punto di vista tecnologico le principali componenti del Sistema di conservazione di DigiP.

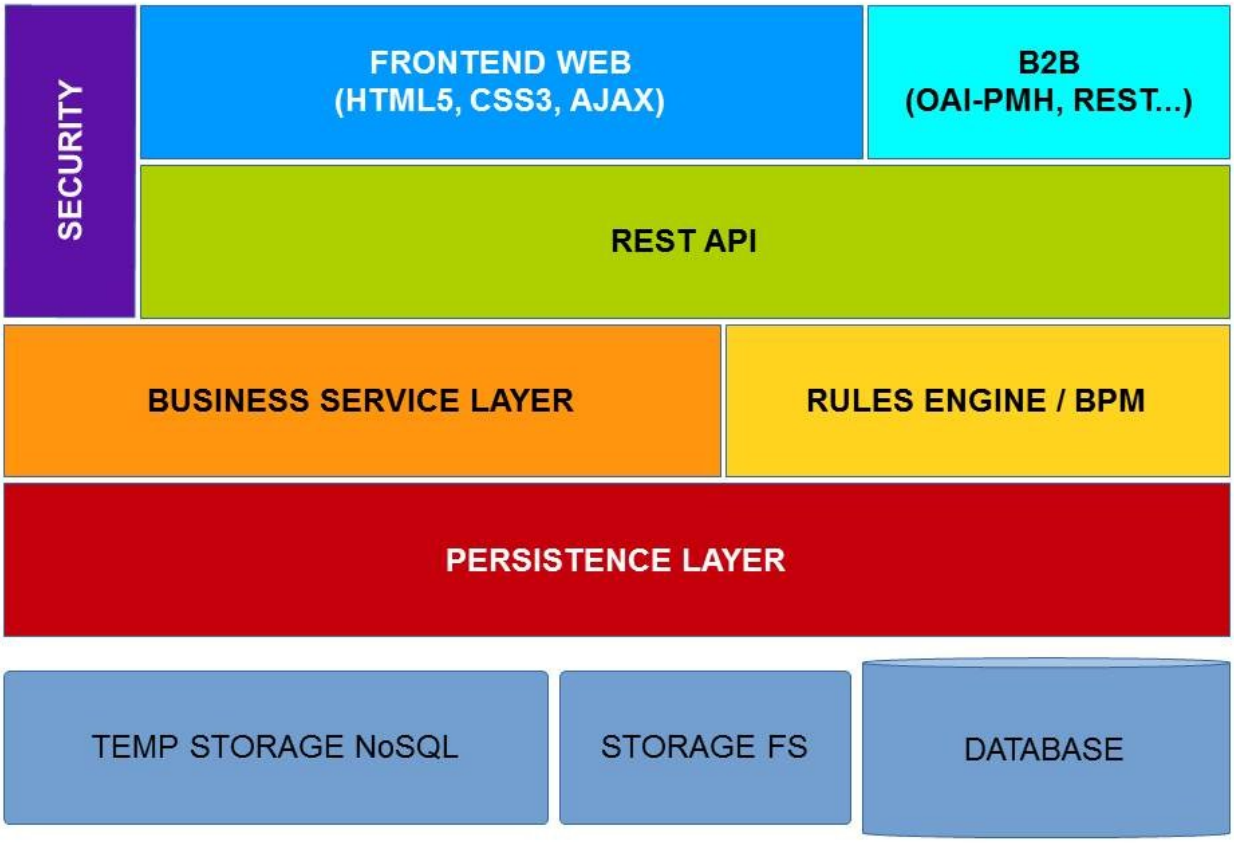

Figura 7 - Componenti tecnologiche e livelli architetturali di DigiP

Trattandosi di una web application verticale, in modo del tutto naturale sono state identificate responsabilità diverse nei diversi strati del software che realizzano le funzionalità elencate in OAIS, quindi è stata definita l'architettura a tre livelli come illustrata in figura:

1. Il livello di presentazione, costituito da:
   - un sistema di sicurezza integrabile a livello di container con il Portale Servizi di Regione Marche (Cohesion);
   - le interfacce web user-oriented realizzate in HTML5, personalizzate con i fogli stile CSS e dinamicizzate mediante l'impiego di Ajax (librerie Dojo);
   - l'interfaccia standard REST per le comunicazioni B2B interoperabili;

- uno strato intermedio di servizi REST, allo scopo di disaccoppiare client e server migliorando la scalabilità, la configurabilità e la robustezza del sistema.

2. Il livello di business logic, costituito da:
   - servizi generali e specializzati, invocati direttamente dai servizi REST per l'implementazione delle funzionalità OAIS;
   - un gestore di processi come implementazione ampiamente configurabile dei workflow e dei controlli a cui sono soggetti i diversi Information Package (IP). La realizzazione prevede l'impiego di un message broker ad alte prestazioni (RabbitMQ), inoltre è previsto un modulo per estendere l'implementazione di workflow personalizzati basati su BPM (modulo workflow).

3. Il livello della persistenza, diversificato tra
   - deposito temporaneo ad alta disponibilità, dove i diversi IP vengono parcheggiati in attesa del completamento dei controlli previsti, capace di accogliere notevoli picchi di versamento parallelo, per il momento identificato da una porzione condivisa del file system del nodo;
   - storage di grande capacità, dove vengono mantenuti inalterati i diversi IP, predisposto per diversificare la memorizzazione in base alla priorità/qualità del supporto;
   - database, ottimizzato per le ricerche di catalogo, dove vengono raccolti e organizzati tutti i metadati.

I componenti software utilizzati sono i seguenti:
- Server: Apache Tomcat;
- Database: PostgreSql;
- Storage FS e Temp Storage NoSql: Jackrabbit (JCR 2.0), file system;
- Persistence layer: realizzato su ORM (Object-Relational Mapping) e precisamente Hibernate 3.6.x;
- Business service layer: realizzato su Spring 3.1.x;
- Rules Engine / BPM: realizzato con l'impiego di RabbitMQ.

Torna al sommario

8.3 COMPONENTI FISICHE

Dal punto di vista tecnico il sistema è progettato e realizzato in maniera da fornire un'elevata continuità di servizio, garantire l'integrità degli oggetti conservati, gestire grandi volumi di dati, mantenere performance stabili indipendentemente dai volumi di attività ed assicurare la riservatezza degli accessi.

Il Sistema è sviluppato con tecnologie di larga diffusione open source con eccezione del software di gestione del mirroring degli storage che è legato alla tecnologia degli storage stessi e del software di backup su nastro.

L'immagine che segue schematizza le principali componenti infrastrutturali del Sistema di conservazione di DigiP e le principali relazioni con altri sistemi interessati dal processo di conservazione descritto nelle sezioni precedenti del presente Manuale.

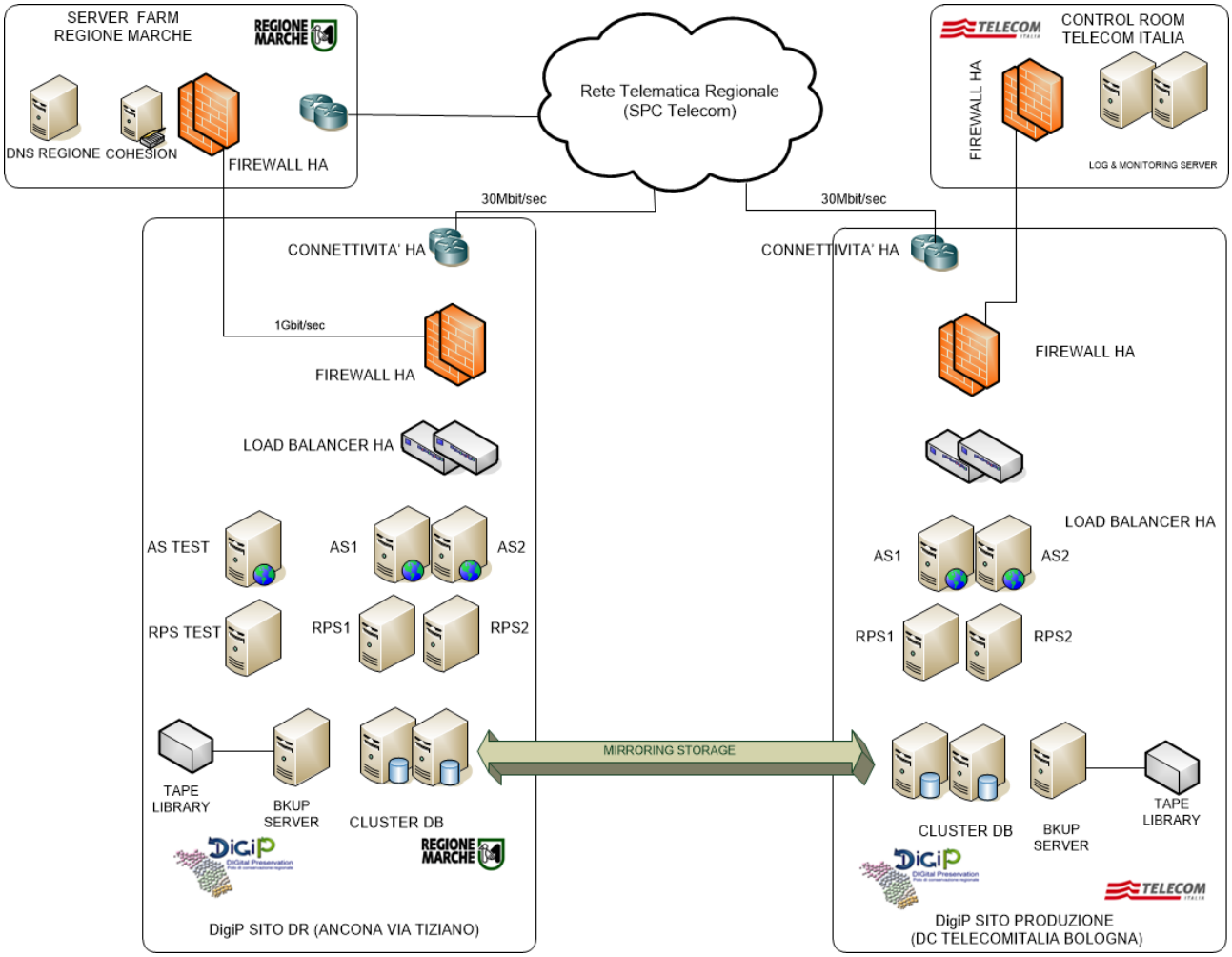

Figura 8 - Componenti fisiche

Il Sistema è realizzato su due siti che distano circa 200 chilometri l'uno dall'altro: un sito primario, (produzione) installato presso il Data Center di Telecom Italia a Bologna, che svolge funzioni di normale operatività e un sito secondario installato presso una sala dedicata nella Server Farm di Regione Marche, che ha lo scopo di subentrare come sito di Disaster Recovery nel caso di caduta irreparabile del sito primario. I due siti sono gestiti dalla Control Room di Telecom Italia.

Entrambi i siti sono interconnessi alla Rete Telematica Regionale della Regione Marche mediante accessi in fibra ottica totalmente ridondati.

La Rete Telematica Regionale della Regione Marche è l'infrastruttura principale per trasporto dati attraverso la quale è possibile usufruire dei servizi DigiP.
Enti contribuitori non dotati di accesso alla rete telematica regionale possono connettersi al sistema via rete pubblica INTERNET attraverso un SISTEMA di FRONT END .

La figura sottostante illustra l'interconnessione dei siti primario e Disaster Recovery DigiP alla Rete Telematica Regionale.

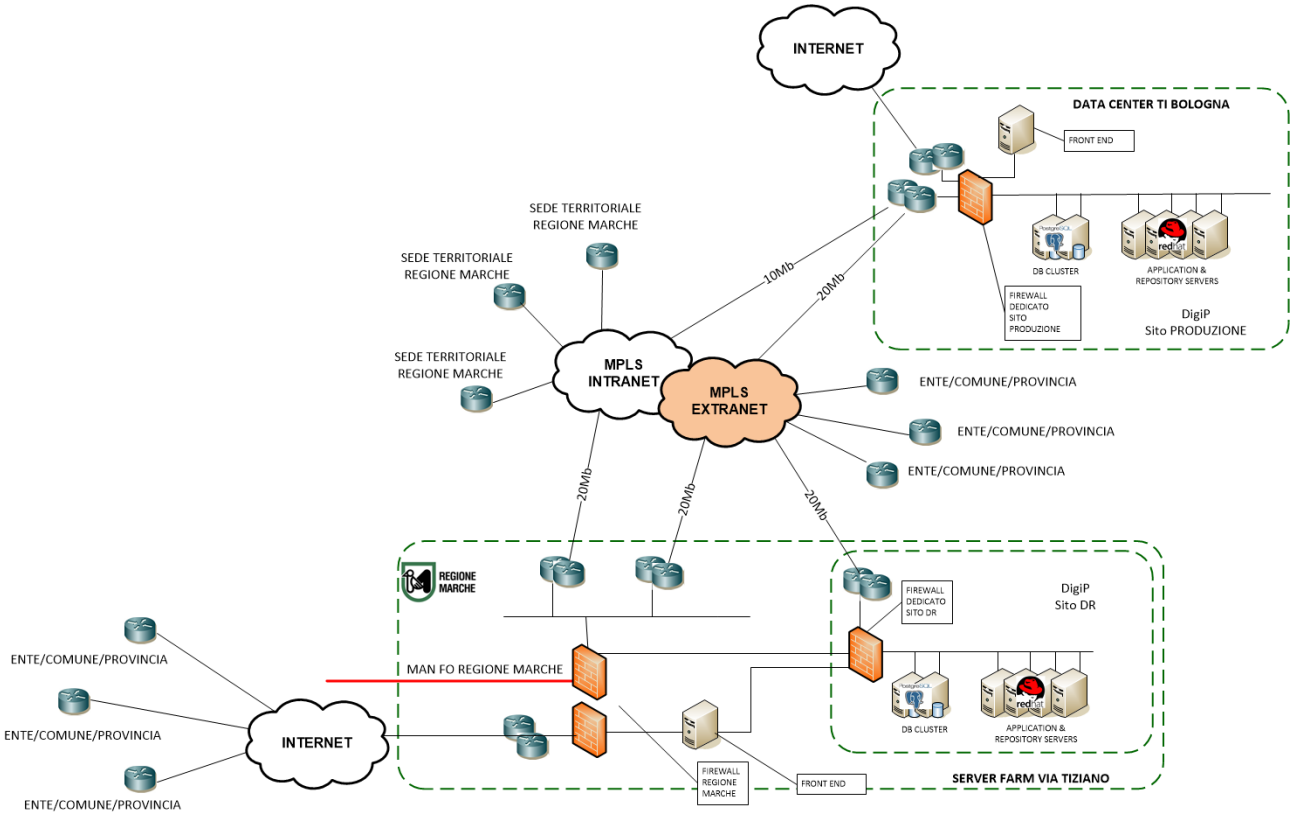

Figura 9 - Interconnessioni sito primario/DR alla Rete Telematica Regionale

Tutti i componenti del sito primario e Disaster Recovery sono ridondati.

Alcuni sistemi di supporto, impiegati dalla Control Room di Telecom Italia sono installati (sistemi di log & monitoring), ridondati, presso le server farm Telecom Italia di Rozzano e Pomezia.

La Control Room di Telecom Italia è direttamente connessa, mediante collegamenti specializzati, protetti da opportuni separation firewall, al sito di Disaster Recovery .

La figura sottostante illustra la modalità di connessione della Control Room alle installazioni DigiP.

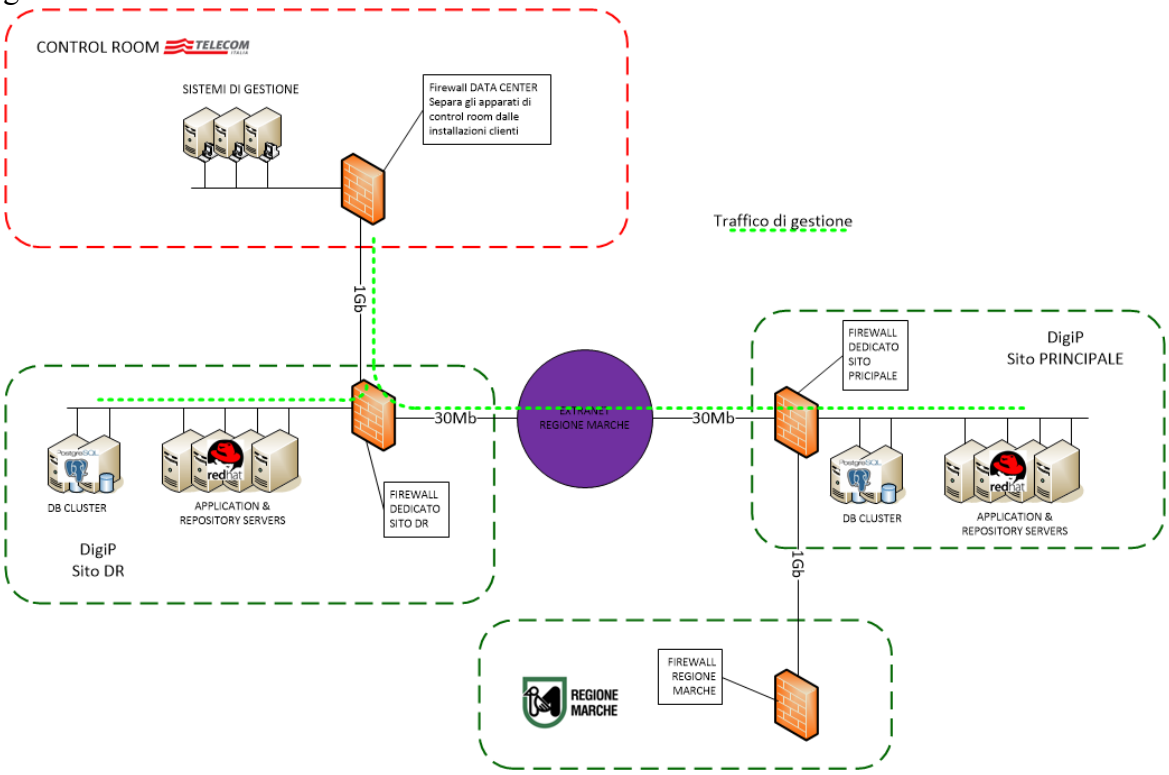

Figura 10 - Modalità di connessione Control Room a DigiP

In situazione di funzionamento normale il Sistema è attivo solo sul sito primario; il sito secondario si limita a replicare le informazioni del sito primario in maniera asincrona man mano che vengono generate e a compiere funzioni di backup.

In caso di caduta irreparabile del sito primario (disastro) il sito secondario viene posto in stato di attività e vi si reindirizza il traffico.

I sistemi di sviluppo risiedono presso la server farm di Regione Marche su ambienti fisicamente diversi da quelli che ospitano il sito primario DiGiP.

Torna al sommario

8.4 CARATTERISTICHE TECNICHE DEL SITO PRIMARIO

Lo schema illustra le componenti del sito di produzione

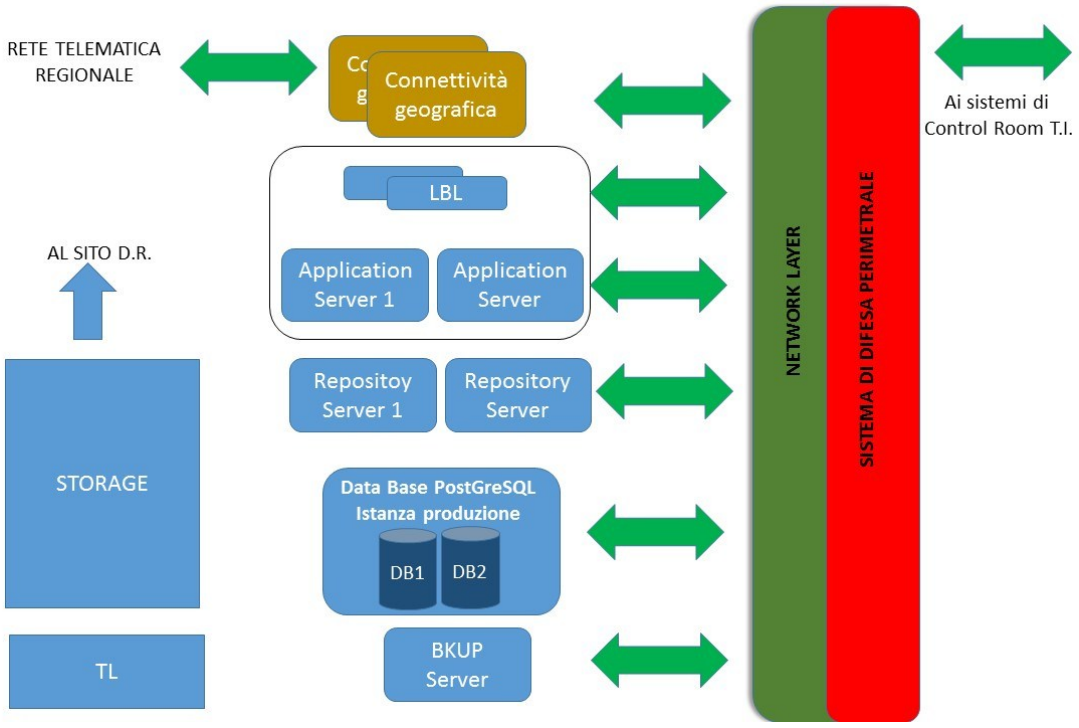

Figura 11 - Componenti sito di produzione

- **Connettività geografica**, costituita da collegamenti in fibra ottica (30Mbit/sec) totalmente ridondati su percorso fisico differenziato che consentono l'esposizione del servizio DigiP sulla Rete Telematica Regionale e l'allineamento degli storage dei due siti DigiP;
- **Network Layer** (CISCO), costituito da una coppia di switch, che provvede all'interconnessione delle varie componenti del sistema;
- **Sistema di difesa perimetrale** (FORTINET) in cluster, che si occupa di separare i veri layer del sistema;
- **Bilanciatore di carico LBL** (CISCO) in cluster, che si occupa di ripartire il carico sulla coppia di application server;
- **Application server TOMCAT** la batteria di application server è composta da due server;
- **Repository Server JACKRABBIT**la batteria di application server è composta da due server;
- **Data Base PostGreSQL** in cluster di sistema operativo;Il Cluster ospita due distinte istanze PostgreSQL una per il DB di Produzione e una per quello di test/pre-produzione

- **Sistema di Storage** composto da un apprato IBM Storewize V700 dotato di una capacità lorda di 24 TB
- **Sistema di Backup** composto da un backup server (Symantec) e una tape library IBM TS3100.

Gli accessi al sistema avvengono esclusivamente passando da firewall tramite protocolli sicuri (HTTPS e FTPS).
Lo ***storage*** su disco è suddiviso in due categorie:

- **Data Base** per la *memorizzazione* delle informazioni e di parte degli ***Oggetti-dati*** conservati in forma di Bytea (ByteArray);
- **File system** per la *memorizzazione* temporanea degli ***Oggetti-dati*** che, in base alle politiche configurate nel sistema, verranno archiviati su cassette; il ***file system*** contiene inoltre tutti i file di servizio (log, configurazioni, ecc.);

Lo ***storage*** su disco è ospitato su uno storage array ed è costituito da un'area di storage primario con dischi ad alta velocità e da un'area di storage secondario con dischi a media velocità; in questo modo è possibile ottimizzare la distribuzione dei dati sui dischi in ragione delle necessità applicative.

Lo ***storage*** su nastri magnetici (backup) si basa su un sistema a cassette (***tape library***), completamente governato da Symantc Backup Exec che gestisce cassette in standard LTO4 su cui vengono mantenuti in **modalità di backup**, i backup full e gli archive log del Data Base, immediatamente disponibili per qualsiasi attività di restore che si rendesse necessaria.

La replica dei dati sul sito secondario è garantita dalla tecnologia Remote Mirroring di IBM in modalità Global Mirroring.

Global Mirroring è una modalità di scrittura asincrona che assicura che le richieste di scrittura vengono effettuate sul sito remoto nello stesso ordine nel quale sono state effettuate sul sito principale, garantendo in questo modo la consistenza dei dati.

Global Mirroring è in grado di assicurare un RPO prossimo allo zero.

La funzionalità di Change Volume (specifica dei sistemi V7000) garantisce il corretto funzionamento del Global Mirroring anche in presenza di sovraccarico della rete di collegamento fra i due siti.

Torna al sommario

8.5 CARATTERISTICHE TECNICHE DEL SITO DI DISASTER RECOVERY

Il sito di disaster recovery, ubicato presso la Server Farm Regionale di Via Tiziano ad Ancona è realizzato in maniera speculare rispetto al sito principale , sul sito di Disaster Recovery è presente un Ambiente di PRE-PRODUZIONE.
L'immagine che segue schematizza le principali componenti tecniche del sito secondario di disaster recovery di DigiP

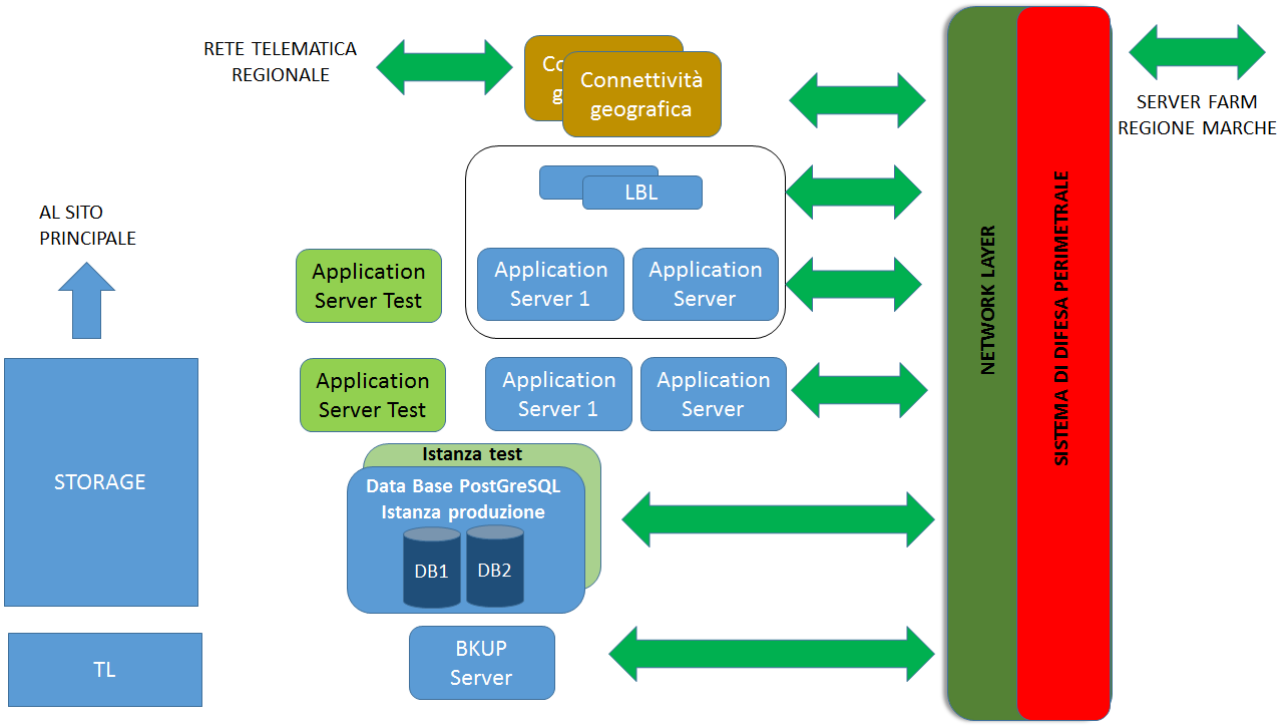

Figura 12 - Componenti tecniche sito disaster recivery DigiP

Il Sistema è sviluppato in Java su sistemi operativi Red Hat utilizzando i seguenti componenti principali:

- **Connettività geografica**, costituita da collegamenti in fibra ottica (30Mbit/sec) totalmente ridondati su percorso fisico differenziato che consentono l'esposizione del servizio DigiP sulla Rete Telematica Regionale e l'allineamento degli storage dei due siti DigiP;
- **Network Layer** (CISCO), costituito da una coppia di switch, che provvede all'interconnessione delle varie componenti del sistema;
- **Sistema di difesa perimetrale** (FORTINET) in cluster, che si occupa di separare i veri layer del sistema;

- **Bilanciatore di carico LBL** (CISCO) in cluster, che si occupa di ripartire il carico sulla coppia di application server;
- **Application server TOMCAT** la batteria di application server è composta da tre server;dei quali uno è dedicato all'ambiente di PRE-PRODUZIONE
- **Repository Server JACKRABBIT** la batteria di application server è composta da tre server;dei quali uno è dedicato all'ambiente di PRE-PRODUZIONE
- **Data Base PostGreSQL** in cluster di sistema operativo; il Cluster ospita due distinte istanze PostgreSQL una per il DB di Produzione e una per quello di test/pre-produzione
- **Sistema di Storage** composto da un apparato IBM Storewize V700 dotato di una capacità lorda di 24 TB
- **Sistema di Bkup** composto da un backup server (Symantec) e una tape library IBM TS3100.

Il sistema di storage è configurato in modo speculare a quello del sito principale e sincronizzato con quest'ultimo tramite i meccanismi di mirroring dell'apparato.

Torna al sommario

8.6 PROCEDURE DI GESTIONE E DI EVOLUZIONE

Le procedure di gestione ed evoluzione del sistema sono affidate ad un insieme di unità funzionali:

- **Unita di Gestione:** che esegue la normale attività di conduzione del sistema.
- **Unità di Progettazione e Sviluppo Software:** che si occupa della manutenzione correttiva ed evolutiva del software di conservazione.
- **Unità Data Center:** incaricata della gestione sistemistica infrastrutturale.
- **Supporti di secondo livello**: costituiti dai Comptence Center di Telecom Italia che cooperano con l'Unità Data Center nella rimozione di guasti e anomalie infrastrutturali.
- **Unità di Progettazione infrastrutturale**: che cura la progettazione e l'implementazione dell'evoluzione dell'infrastruttura HW.

Torna al sommario

8.7 CONDUZIONE E MANUTENZIONE DEL SISTEMA DI CONSERVAZIONE

L'Unità di Gestione (UG) è il gruppo di lavoro che gestisce operativamente il funzionamento quotidiano del sistema di conservazione e costituisce inoltre il punto di riferimento per gli utenti finali del sistema stesso.

Oltre all'esecuzione dei processi descritti nel Manuale della Conservazione (ad esempio il controllo della corretta esecuzione delle regole di formazione degli AIP di conservazione, l'abilitazione di

nuovi utenti, ecc.), l'UG si occuperà delle funzioni di help desk verso gli Enti produttori (I° livello) sulle tematiche operative di conservazione ed archiviazione.

Torna al sommario

8.8 GESTIONE E CONSERVAZIONE DEI LOG

Il sistema di gestione e conservazione dei log si basa sul prodotto Syslog-ng Store Box di Balabit. Di seguito l'architettura logica:

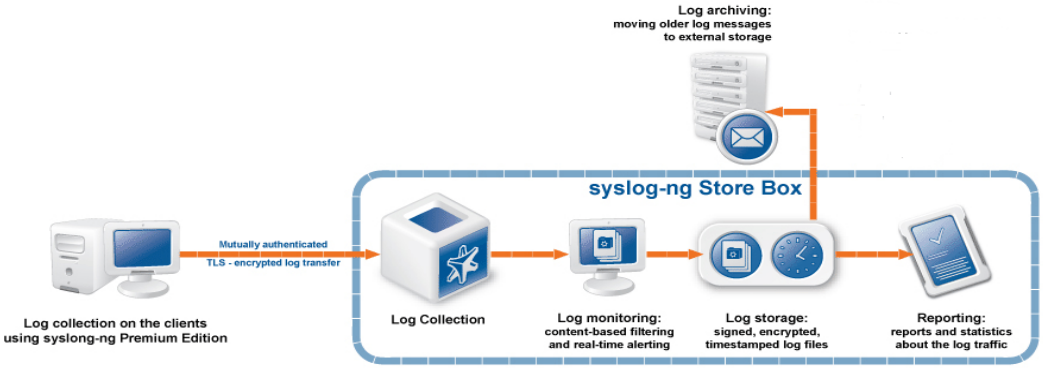

Figura 13 - Architettura logica

Sui sistemi in perimetro vengono attivate le funzionalità standard di sistema operativo di logging degli accessi (login/logoff). Sui DB server viene inoltre attivato il tracciamento degli accessi al DB, mediante la soluzione TOLL, integrabile con syslog-ng.

Su ciascun server in perimetro viene installata la componente client di syslog-ng PE 3.0

Presso i Data Center di T.I viene predisposta una coppia di Syslog-ng Store Box (SSB5000) in configurazione HA.

I syslog-ng client inviano, in modo sincrono e sicuro (canale cifrato, controllo integrità) gli eventi di loging/logoff al SSB di riferimento.

I log di accesso raccolti (archiviazione cifrata) sono fruibili mediante accesso al SSB, previa disponibilità della chiave privata di cifratura. Su specifica richiesta del Cliente potranno essere forniti i log di pertinenza in formato leggibile.

I log ricevuti dagli host remoti sono memorizzati in file binari compressi, cifrati, firmati e timestamped; sono inoltre sottoposti a backup su storage/server esterni.

E' previsto, mediante analoga modalità, il tracciamento degli accessi e di tutte le attività effettuate sul server SSB (conservazione dei log di accesso e delle attività effettuate su file cifrati).

E' prevista una gestione di tipo RBAC (Role-Based Access Control) dei privilegi degli utenti di sistema.

Syslog-Ng ha la funzionalità del "buffering" che permette di archiviare i messaggi localmente (lato syslog-ng client) e di rispedirli quando la connessione con il server di raccolta si è ristabilita dopo un eventuale fault, garantendo di fatto la continuità di registrazione degli eventi.
È possibile gestire i log ricevuti in path separati e configurabili sulla base delle sorgenti dati (IP o hostname).

Il servizio garantisce la tenuta in linea dei dati riferiti ai 6 mesi precedenti quello in corso.

Torna al sommario

8.9 MONITORAGGIO DEL SISTEMA DI CONSERVAZIONE

Il monitoraggio infrastrutturale del sistema è affidato all'Unità Data Center che si compone di una Unità di Presidio della sala dati del sito principale e da un insieme di strutture centralizzate di Telecom Italia che collaborano nella gestione sistemistica dell'infrastruttura:

L'Unità di Presidio cura tutte le attività On Site, quali:

- gestione degli accessi fisici alla sala macchine del sito principale;
- la verifica visiva dello stato del sistema;
- controllo dei bkup;
- controllo dello stato di allineamento dei sistemi di storage dei due siti;
- verifica dell'operato delle ditte manutentrici dell'hardware;
- collabora con le strutture centralizzate per la risoluzione dei guasti di sistema.

La Control Room di Telecom Italia si occupa di tutta l'attività di gestione sistemistica, dal sistema operativo al middleware, e cura le attività di log & monitoring sistemistico.

Il Centro Nazionale Assistenza e il NOC (Network Operation Center) di T.I. si occupano della gestione sistemistica del network Layer (Switch e Bilanciatori).

Il Centro Nazionale Assistenza e il SOC (Security Operation Center) di T.I hanno in carico la gestione degli apparati di sicurezza perimetrale.

Il Centro di Gestione TIDS (Telecom Italia Digital solution ex PathNET) ha la responsabilità del corretto funzionamento delle linee di interconnessione alla Rete Telematica della Regione Marche.

Tutte le componenti dell'Unità Data Center sono supportate dai Competence Center di Telecom Italia che costituiscono l'HelpDesk di secondo livello per la componente infrastrutturale.

Torna al sommario

8.10 CHANGE MANAGEMENT

Le attività di change management sono classificate in attività di tipo ordinario o evolutivo.
Il change management ordinario comprende tutte quelle attività hardware e software che non alterano l'architettura del sistema. Tali attività non richiedono di norma il coinvolgimento dell'Unità di Progettazione Infrastrutturale e sono eseguite dall'Unità Data Center direttamente o con il supporto del fornitore.

Tutte le attività di change management ordinario vengono tracciate e documentate dalla richiesta all'espletamento.

Le attività di change management evolutivo hanno un impatto sull'architettura del sistema, richiedono uno studio di fattibilità e la redazione di un' apposito progetto che dovrà essere approvato da Regione Marche.
Le attività di change management evolutivo sono eseguite dall'Unità Data Center direttamente o con il supporto di un fornitore.
Tutte le attività di change management evolutivo vengono tracciate e documentate dalla richiesta all'espletamento.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

9.1 VERIFICA PERIODICA DI CONFORMITÀ A NORMATIVA E STANDARD DI RIFERIMENTO

La struttura di progetto costituita dal Comitato Scientifico procederà periodicamente ad eseguire audit interni sull'intero sistema al fine di verificarne la conformità alla normativa cogente ed agli standard di riferimento.

Torna al sommario

9.2 PROCEDURE DI MONITORAGGIO

Vengono prodotti dal personale delle strutture di costituenti l'Unità Data Center e resi disponibili periodicamente report di monitoraggio tecnico, su tutte le aree infrastrutturali (rete, server, storage, database, backup). Si tratta di report tra loro eterogenei, prodotti dal software di base dei sistemi e dal software di monitoraggio tecnico installato sui medesimi.

Periodicamente i report di monitoraggio tecnico vengono esaminati congiuntamente all'Unità di Progetto con lo scopo di individuare eventuali aree di miglioramento negli aspetti tecnici dell'applicativo.

Torna al sommario

9.3 VERIFICA E MANTENIMENTO DELL'INTEGRITÀ DEGLI ARCHIVI

Le procedure di monitoraggio illustrate nel paragrafo precedente, le politiche di conservazione dei backup illustrate nel Piano della Sicurezza e le caratteristiche delle tecnologie utilizzate garantiscono la completa integrità di quanto archiviato in DigiP, ovvero di quanto depositato nel Data Base, nel file system e negli archivi su cassetta, una volta che sia stato duplicato nel sito di Disaster Recovery e salvato tramite opportuno backup sia nel sito primario che nel sito secondario.
Le funzionalità di Archiviazione consentono:

- l'amministrazione del data base, che si basa sulle funzionalità del data base e si occupa di gestire tutti i dati che transitano nel sistema, a parte i file memorizzati nel file system. Gli accessi al data base sono effettuati tramite opportuni moduli applicativi, che garantiscono l'indipendenza dell'applicativo dallo specifico data base (purché sql) e dalla sua specifica release;
- la manutenzione del data base. Le funzionalità di remote mirroring dello storage assicurano la replica del data base e del file system del repository nel sito di disaster recovery, mentre le funzionalità di recovery management consentono backup del data base completi e

incrementali, a caldo, secondo le politiche di sicurezza descritte nel piano della sicurezza. la gestione sistemistica del data base è effettuata tramite prodotti certificati, ed è tracciata nel log di sistema. il data base fornisce periodicamente informazioni statistiche utili a valutarne il dimensionamento e le performance, e quindi a pianificare attività di manutenzione del data base stesso e degli applicativi che lo utilizzano;

- il controllo dell'integrità del data base, che avviene sfruttando funzionalità native del data base. Per quanto attiene alla componente di data base degli archivi, l'integrità è garantita dalle funzionalità intrinseche di PostGreSQL per tutti i metadati descrittivi, in particolare dalle funzionalità di backup del data base e di raccolta degli archive log (file WAL).

Per quanto attiene invece alla componente di file system degli archivi, l'integrità è garantita da funzionalità intrinseche del modulo di archiving di Symantec Backup Exec per tutti i dati archiviati su cassetta.

Qualora nonostante le garanzie fornite dalle tecnologie impiegate si verificassero anomalie nell'integrità degli archivi, sono previste le opportune procedure applicative di ripristino illustrate nel paragrafo seguente.

Non sono considerati facenti parte del Sistema, e quindi non fruiscono della stessa garanzia di integrità, i dati in ingresso presenti su aree temporanee (es. spazi FTP, ecc.), per i quali le procedure di soluzione di cui al paragrafo seguente prevedono la ritrasmissione nel caso di anomalie.

Il Piano della Sicurezza di DigiP descrive le modalità con cui DigiP assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i back up degli archivi, il Disaster Recovery e la Continuità Operativa.

Torna al sommario

9.4 SOLUZIONI ADOTTATE IN CASO DI ANOMALIE

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

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

- tutte le funzionalità del sistema che inseriscono o modificano dati nel Data Base e file nel

File System operano in modalità transazionale;

- il backup del Data Base assicura il restore all'ultima transazione completata correttamente;
- il File System di DigiP è sottoposto a backup full a caldo con frequenza quindicinale. Non è quindi possibile far fronte a tutte le possibili anomalie con le stesse procedure, ma sono necessarie procedure specifiche secondo la natura dell'anomalia stessa.

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

File System del PreIngest	Si richiede la ritrasmissione dei SIP
Data Base di DigiP	Si effettua la restore tramite le funzioni standard di PostGres dal sito primario o dal sito secondario (nel caso di indisponibilità del DB primario)
File System di DigiP	Si effettua la restore tramite le funzioni standard del file server per tutti i file inseriti nel *file system* fino all'ultimo back up; per i file inseriti successivamente all'ultimo back up si eseguono opportune procedure di quadratura tra Data Base e *file system*, che provvedono a riportare il sistema in stato di congruenza. Le procedure di recupero debbono essere eseguite sia sul sito primario che sul secondario.

Torna al sommario

ALLEGATI

PIANO DELLA SICUREZZA

MANUALE DI UTILIZZO DIGIP

DISCIPLINARE TECNICO