Manuale di Conservazione

Digitaly srl

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	23/01/15	Mario Schiano	Responsabile dei sistemi informativi per la conservazione
	23/09/15	Elisa Angelone	Responsabile della funzione archivistica
Verifica	23/09/15	Elisa Angelone	Responsabile della funzione archivistica
		Mario Schiano	Responsabile dei sistemi informativi
		Sabatino Paoletti	Responsabile del servizio di conservazione
		Diego Melone	Responsabile del trattamento dati personali
Approvazione	23/09/15	Elisa Angelone	Responsabile della funzione archivistica
		Mario Schiano	Responsabile dei sistemi informativi
		Sabatino Paoletti	Responsabile del servizio di conservazione
		Diego Melone	Responsabile del trattamento dati personali

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	20/01/15	Prima Stesura	
2.0	25/05/15	Seconda Stesura	
2.1	23/09/15	Terza Stesura	
2.2	02/11/2015	Quarta Stesura	
2.3	20/01/2016	Quinta Stesura	

SOMMARIO

1 SCOPO E AMBITO DEL DOCUMENTO

Il seguente documento (d'ora in poi Manuale), ha come scopo la raccolta dei riferimenti tecnici e normativi utilizzato da Società srl in merito al processo di gestione della Conservazione dei documenti informatici.

Il manuale descrive dettagliatamente tutte le procedure amministrative e tecniche, i ruoli e le competenze dei soggetti coinvolti nel processo di archiviazione e conservazione dei documenti tecnici.

In particolare, è l'insieme delle attività e dei processi che, tramite l'adozione di regole, procedure e tecnologie, garantiscono l'accessibilità, l'utilizzabilità (leggibilità e intelligibilità), l'autenticità (identificabilità univoca e integrità) e la reperibilità dei documenti e dei fascicoli informatici con i metadati ad essi associati.

Torna al Sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Glossario dei termini e Acronimi	
AgID	Agenzia per l'Italia Digitale
Aruba Spa	Aruba S.p.A., fondata nel 1994, società in Italia per i servizi Web. La società propone 4 principali ambiti di servizi: Hosting e Domini, e-Security, Cloud e servizi Data Center . P.IVA: 01573850516
CA	Certification Authority
CED	Centro elaborazione dati
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un

	Client attraverso il protocollo FTP
***IdP*:**	strumento per rilasciare le informazioni di identificazione di tutti i soggetti che cercano di interagire con un Sistema; ciò si ottiene tramite un modulo di autenticazione che verifica un token di sicurezza come alternativa all'autenticazione esplicita di un utenteall'interno di un ambito di sicurezza.
Idc	Indice di Conservazione
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione ad un'evidenza informatica di una funzione di *hash.*
Indice di Archiviazione IPdA	L'IPdA è l'evidenza informatica associata ad ogni PdA, contenente un insieme di informazioni articolate come descritto nel seguito. Deve essere corredato da un riferimento temporale e dalla firma digitale o firma elettronica qualificata del soggetto che interviene nel processo di produzione del pacchetto di archiviazione.
Manuale di Conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione (allegato al DPCM 3 dicembre 2013).
More Information	Informazione aggiuntiva all'interno del file xml
PdA – Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche tecniche previste dalle regole tecniche allegate al DPCM 03/12/2013 per i sistemi di conservazione e secondo le modalità riportate nel Manuale di Conservazione.

PdV- Pacchetto di Versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato nel Manuale di Conservazione.
Pacchetto Informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
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
Protocollo HTTP	Specifica di trasferimento di dati in un'architettura client-server. Ne esistono due varianti: HTTP 1.0 documentato nel RFC 1945 ed HTTP 1.1 documentato nel RFC 2616.
Protocollo HTTPS	Protocollo che integra l'interazione del protocollo HTTP attraverso un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS). Questa tecnica aumenta il livello di protezione contro attacchi del tipo man in the middle. La porta di default per il protocollo HTTPS è la numero 443 (mentre per il protocollo HTTP è la numero 80).
RdV- Rapporto di Versamento	Ricevuta in documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Responsabile dei sistemi informativi per la conservazione	Soggetto incaricato della gestione dell'esercizio dell'infrastruttura hardware e software che compongono il sistema di conservazione, nonché del monitoraggio dei livelli di servizio erogati dal sistema stesso.
Responsabile del trattamento dei dati personali	Soggetto incaricato della definizione ed della vigilanza delle modalità di trattamento dei

	documenti e delle aggregazioni documentali conservate all'interno del sistema di conservazione nel rispetto della normativa in materia di protezione dei dati personali.
Responsabile della Conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 7, comma 1 delle regole tecniche del sistema di conservazione.
Responsabile della funzione archivistica di conservazione	Soggetto incaricato della definizione delle modalità di trasferimento, di esibizione e di accesso al set di documenti e di aggregazioni documentali conservati all'interno del sistema di conservazione.
Responsabile della sicurezza dei sistemi per la conservazione	Soggetto incaricato della definizione e della vigilanza del rispetto dei requisiti di sicurezza del sistema di conservazione.
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Soggetto incaricato del coordinamento delle attività di sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione.
SInCRO	UNI 11386:2010; Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali. Standard nazionale avente come obiettivo la definizione della struttura dell'insieme dei dati a supporto del processo di conservazione, che individua gli elementi informativi necessari alla creazione di un Indice di Conservazione (il cosiddetto 'file di chiusura'), e ne descrive sia la semantica che l'articolazione. Questo consente agli operatori del settore, di utilizzare una struttura-dati condivisa e di raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, grazie all'adozione dello Schema XML appositamente elaborato e reso disponibile.
Sistema di Conservazione	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del CAD (Codice dell'Amministrazione Digitale).
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VdC	Volume di Conservazione
Web Server	Programma che, utilizzando il modello

	client/server e il protocollo HTTP, fornisce i file che costituiscono una pagina web, agli utenti che ne fanno richiesta utilizzando un programma client: il browser.
Web Device	Sistema software progettato per consentire l'interoperabilità tra diversi elaboratori su di una medesima rete ovvero in un contesto distribuito. Ciò avviene tramite lo scambio di messaggi che usano i protocolli per il web: HTTP o HTTPS (da cui il nome).

Torna al Sommario

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

L'erogazione di servizi di conservazione documentale si inserisce in un contesto normativo molto ampio che ha subito numerosi evoluzioni a partire dalla prima definizione dell'attività, avvenuta nel 1994. L'evoluzione tecnologica e la progressiva definizione di un complesso normativo più dettagliato, hanno permesso di arrivare all'attuale scenario che regolamenta tutti i requisiti tecnici a cui le aziende che vogliano svolgere il ruolo di conservatori ad norma ed essere pertanto accreditati in tal senso, devono rispondere. Si tratta di un insieme di aspetti legali e tecnici, enucleati nelle seguenti fonti normative di riferimento:
− Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], 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 ex al Decreto Legislativo n. 82 del 2005;

− Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna al Sommario

3.2 Standard di riferimento

Nella definizione del contesto normativo tramite il quale regolamentare l'operato dei conservatori, il legislatore ha provveduto ad identificare un set di standard tecnologici di valenza internazionale a cui riferirsi, sia al fine di recepire le ricerche e gli studi effettuati a livello internazionale sull'argomento, sia al fine di definire un percorso che permetta agli operatori Italiani di rispondere in maniera proattiva alla nascente normativa europea. Segue quindi l'attuale scenario tecnologico a cui qualsiasi soggetto accreditato come conservatore è tenuto ad attenersi:
− 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 V 1.3.1 (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 V 1.3.1 (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.

Torna al Sommario

4 RUOLI E RESPONSABILITA'

Di seguito sono indicati i ruoli dei soggetti coinvolti nel progetto.
Per ogni ruolo previsto nel processo di gestione del sistema di conservazione sono richiesti specifici requisiti di esperienza minima e rispettabilità nel ruolo.

Come previsto è possibile che alcuni ruoli vengano delegati per un periodo di tempo prestabilito. Nella seguente tabella, per ciascuna delega, saranno indicati i dettagli del nominativo, il relativo periodo di riferimento e le attività oggetto di delega.

ruoli	Nominativo	attività di competenza	periodo nel ruolo	eventuali deleghe
Responsabile del servizio di conservazione	Sabatino Paoletti	-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		
Responsabile Sicurezza dei sistemi per la conservazione	Diego Melone	Verifica e monitoraggio dei requisiti di sicurezza del sistema di conservazione come stabiliti dalle normative in vigore. Porre segnalazione di eventuali difformità al Responsabile del servizio di conservazione,		
Responsabile funzione archivistica di conservazione	Elisa Angelone	-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.		
Responsabile trattamento dati personali	Diego Melone	-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.		

Responsabile sistemi informativi per la conservazione	Mario Schiano	Gestione degli apparati hardware e software del sistema di conservazione Controllo e monitoraggio degli apparati di rete 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.		
Responsabile sviluppo e manutenzione del sistema di conservazione	Mario Schiano	Pianificazione e coordinamento delle attività informatiche (hardware e software) , gestione dello sviluppo dei siti ed applicazioni web destinati al progetto. Pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; Monitoraggio degli SLA relativi alla manutenzione 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		

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Figura 1 – Organigramma aziendale

L'attività di conservazione coinvolge globalmente i vari settori aziendali, per completare tutte le fasi di caricamento, controllo e memorizzazione dei documenti digitali.

Nello specifico :

- Area Commerciale/Amministrativo
- CED , area diretta dal Responsabile dei Sistemi Informativi per la Conservazione.
- Area Sviluppo, diretta dal Responsabile per lo Sviluppo del Sistema di Conservazione
- Area Digitale , diretta dal Responsabile del Servizio di Conservazione ed il Responsabile della Funzione Archivistica di Conservazione con compiti di supervisione delle firme digitali e marcatura temporale ai pacchetti di Versamento, Archiviazione e Distribuzione
- Area Archivistica, diretta dal Responsabile dell'Archiviazione

Torna al Sommario

5.2 Strutture organizzative

La gestione operativa del processo di conservazione prevede due principali aree:
- Area commerciale, dove ci si rapporta con il cliente/produttore sia per la fase di registrazione al sistema, sia per tutte le operazioni di ambito commerciale.
- Area Customer Care, predisposta alla post assistenza con il cliente/produttore in modalità ticket, live chat, telefonica ed email.

Tali procedure sono documentate nelle manualistiche interne con particolare riferimento alle procedure *PRO PP01 del Manuale della Qualità ISO 9001:2008 "Offerte ed ordini"* e *PRO PP03 del Manuale della Qualità ISO 9001:2008 "Pianificazione, produzione, erogazione, monitoraggio e misurazione".*

- La struttura organizzativa dell'*IT Services* è responsabile dell'insieme di attività relative all'acquisizione, alla verifica ed alla gestione dei pacchetti di versamento presi in carico.
Tali attività riguardano: 1) il mantenimento dei documenti e delle loro caratteristiche significative, con specifica attenzione alla completezza, coerenza e accuratezza degli elementi descrittivi delle entità documentarie e delle relazioni di contesto che danno significato al documento; 2) la verifica dell'adozione di corrette politiche per gestire il trasferimento di custodia e la selezione; 3) la documentazione nel tempo dei processi delle attività di gestione e tenuta in tutte le fasi;
- La struttura garantisce la preparazione e la gestione del pacchetto di archiviazione che svolgerà, con processi automatici di gestione, con la collaborazione e supervisione del *Responsabile della Funzione Archivistica di Conservazione*.

La gestione del PdA riguarderà, oltre alle componenti descrittive, i requisiti gestionali e le attività rilevanti per il servizio di conservazione: avvisi di gestione, controllo terminologico e di coerenza, registrazione di schemi di metadati, autorizzazioni. Ogni servizio sarà adeguatamente documentato. Per l'automazione avanzata dei sistemi documentari saranno utilizzati standard per la conservazione degli archivi informatici che garantiscano gli obiettivi di autenticità e accessibilità;

- La struttura organizzativa dell'*IT Services* è altresì responsabile dell'insieme di attività relative alla produzione dei pacchetti di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta, attività che svolgerà con la collaborazione e supervisione del *Responsabile della Funzione Archivistica di Conservazione*.

Tale scopo sarà garantito dalla tenuta del documento in condizioni adatte all'uso nella forma originale e/o in un formato persistente che garantisca l'integrità della configurazione logica e del contenuto (standard ISO 14721 – Open Archive Information System). Per rendere possibile la conservazione si avrà cura di preparare per tempo la transizione e utilizzare standard per gestire formati dei dati compatibili con l'interoperabilità e la conservazione (saranno esclusi formati binari, formati proprietari, formati orientati all'applicazione);

- scarto dei pacchetti di archiviazione:

Trascorso il termine stabilito dalla legge (per ciascun tipo di documento), si realizzeranno tutte le operazioni di cernita critica del materiale archivistico tese ad individuare i documenti destinati alla conservazione permanente e a predisporre gli elenchi del materiale archivistico destinato alla eliminazione fisica. Al termine delle operazioni di cernita critica del materiale, sarà compilato un elenco di pezzi dei quali si propone lo scarto, che servirà all'ente committente per deliberarne l'eliminazione ed acquisire l'autorizzazione prevista dalla legge (D. lgs. 42/2004, art. 21). L'elenco conterrà il numero de pezzi che si intendono scartare, la loro descrizione sommaria, gli estremi cronologici, i motivi per cui si propone lo scarto.

- Coadiuvate dalla struttura organizzativa dell'*Amministrazione*, le strutture organizzative dell'*Help Desk* e dell'*IT Services* svolgono le attività relative alla chiusura del servizio di conservazione. Specificamente il gruppo dell'*Help Desk* si occupa della disattivazione delle funzionalità relative alla conservazione all'interno del sistema di conservazione, mentre il gruppo di *IT Services* si occupa della preparazione dei supporti fisici necessari per il rilascio dei documenti in conservazione. Questa attività viene coordinata nelle tempistiche dalla struttura organizzativa dell'*Amministrazione* e supervisionata per quel che concerne il rispetto delle normative dal *Responsabile della Funzione Archivistica di Conservazione*.

- Tali procedure sono documentate nelle manualistiche interne con particolare riferimento alle procedure *PRO PP01 del Manuale della Qualità ISO 9001:2008*
"Offerte ed ordini" e *PRO PP03 del Manuale della Qualità ISO 9001:2008*
"Pianificazione, produzione, erogazione, monitoraggio e misurazione"

Attività proprie di gestione dei sistemi informativi:

- Conduzione e manutenzione del sistema di conservazione

Il processo di conservazione sarà gestito automaticamente e strettamente correlato ai processi di formazione del documento e alla gestione delle informazioni di contesto, utilizzato come componente specifica di una catena della conservazione. I metadati resi disponibili nei processi di formazione dei documenti e rilevanti ai fini conservativi saranno finalizzati ad acquisire informazioni significative in relazione agli aspetti gestionali e alle transazioni che avranno per oggetto i documenti. Sarà effettuata una mediazione descrittiva da parte dell'archivista.

Per le finalità conservative, i metadati saranno necessari per la identificazione certa e univoca della risorsa, per documentare l'integrità del documento in fase di trasmissione nello spazio e nel tempo.

- Monitoraggio del sistema di conservazione

I controlli saranno realizzati tecnologicamente e determinati sulla base di principi e criteri definiti in base alla natura dei documenti. Sarà conservata copia dell'oggetto digitale (con livello di dettaglio sufficiente), sarà restituita forma e contenuto dell'oggetto grazie ad un accurato sistema di riproduzione delle caratteristiche ritenute essenziali, sarà verificata l'accuratezza dell'intero processo.

- Change management

La conservazione nel tempo sarà garantita tramite migrazione in formati standard.

- Verifica periodica di conformità a normativa e standard di riferimento

Per i documenti si verificherà periodicamente la robustezza, la stabilità (compatibilità retroattiva e prospettica), l'auto-documentazione (possibilità di includere metadati nel file), l'indipendenza dal dispositivo o la portabilità rispetto alla piattaforma, l'assenza di meccanismi tecnici di protezione (possibilità di riproduzione vs password o crittografia), l'assenza di limitazioni all'utilizzo, l'accessibilità, la non modificabilità, la sicurezza, l'efficienza

Torna al Sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Gestisce le politiche sulla tipologia dei documenti con un determinato cliente, per poter garantire in maniera bilaterale il corretto trasferimento dei documenti stessi con i corretti set di metadati .

In merito alla classificazione dei documenti vengono adottate diverse misure di conservazione con relativa attività di scarto dei documenti non validi, corrotti o incoerenti.

6.1 Oggetti conservati

Di seguito un elenco dei tipi di oggetti conservati ed ammessi nel sistema di conservazione

Oggetto	Fattura elettronica
Specifiche	Fatture di vendita, documenti ad emissione e tenuta obbligatoria con valenza tributaria
Periodo di conservazione	10 anni

Normativa	– Circolare n. 18e/2014 dell'Agenzia delle Entrate – Decreto del 17 giugno 2014 – Ministero Economia e Finanze – Decreto legge 24 aprile 2014, n. 66 – DPCM del 3 dicembre 2013 – Decreto del 3 aprile 2013, n. 55 – Ministero Economia e Finanze – DPCM del 22 febbraio 2013 – Legge di stabilità 2013 – Direttiva UE 45/2010 – Decreto del 7 marzo 2008 – Ministero Economia e Finanze – Legge 24 dicembre 2007, n. 244 – Circolare n. 45/2005 dell'Agenzia delle Entrate
Formati e visualizzatori	PDF - Acrobat Reader *Vers. 11.0* TIFF - Gimp , Adobe Photoshop Express V2.7 BMP - Gimp , Adobe Photoshop Express V2.7 JPG - Gimp , Adobe Photoshop Express V2.7 OOXML - LibreOffice Vers.5 XML - Mozilla Firefox- Vers.sempre aggiornata TXT – JEdit , Blocco note Windows Ver. 5.2

Oggetto	**Documento Generico**
Specifiche	Qualsiasi documento che si voglia conservare (Testi, Immagini, Codice Sorgente, Database, altro)
Periodo di conservazione	Variabile in base al tipo di file
Normativa	
Formati e visualizzatori	PDF - Acrobat Reader *dalla versione 8* TIFF - Gimp , Adobe Photoshop Express V2.7 BMP - Gimp , Adobe Photoshop Express V2.7 JPG - Gimp , Adobe Photoshop Express V2.7 OOXML - LibreOffice Vers.5 XML - Mozilla Firefox - Vers. Aggiornata TXT – JEdit , Blocco note Windows Vers.5.2

Torna al Sommario

6.2 Pacchetto di versamento

Tutti i documenti sono ricevuti dal sistema di conservazione da parte del produttore, tramite la consegna di un *pacchetto di versamento* opportunamente formattato secondo le specifiche di base.

Tramite apposita applicazione, all'interno del documento, viene creato un IdV strutturato seguendo l'apposito standard nazionale dall'UNI 11386:2010 Standard SInCRO, contenente un nodo denominato "MoreInformation" con il quale il produttore può inserire dei metadati aggiuntivi caratteristici del documento da conservare.

Il generico record "MoreInformation" fa riferimento alle informazioni aggiuntive rispetto al tracciato di metadati minimale previste dall'UNI 11386:2010 Standard SInCRO.

Il pacchetto di archiviazione è costituito da uno o più file ai quali è applicato il processo di conservazione. Per i pacchetto di archiviazione viene creato un IdC (Indice di Conservazione) corredato da: riferimento temporale, firma digitale dei soggetti intitolati ad effettuare il processo di conservazione ed elementi di aggregazione di più file contenuti in un PdV (FileGruppo). L'IdC coincide con lo schema XML descritto nello standard, istanziato secondo le specifiche esigenze di contesto e provvisto di riferimento temporale e firma digitale.

Torna al Sommario

Tipologie di pacchetto di versamento gestite :

Esempio:

SPESE DEL PERSONALE

- *Spese del personale*
    - *Stipendi*
    - *Contributi Inps*
    - *Imposta Irpef*
    - *Contributi Inail*
    - *Accantonamento TFR*
- *Rimborsi spese*

Struttura dati del PdV :

Esempio:

Struttura Generica del pacchetto di versamento :

Gruppo 1

Titolo 1.1

Sottotitolo 1.1.1

Sottotitolo 1.1.2

Etc

Titolo 1.2

Sottotitolo 1.2.1

Sottotitolo 1.2.2

Etc ...

Etc

6.3 Pacchetto di archiviazione

Il Pacchetto di Archiviazione, mette in collegamento l'*Indice del Pacchetto di Archiviazione* con l'insieme di tutti i documenti da conservare nell'ambito di un singolo contratto.

L' *Indice del Pacchetto di Archiviazione* viene generato automaticamente dal sistema all'atto del salvataggio del *Pacchetto di Versamento,* sempre nel rispetto dello standard "SInCRO".

Si presenta di seguito la struttura dati del pacchetto di archiviazione completa delle ulteriori strutture collegate ai diversi elementi "MoreInfo" previsti dallo standard SInCRO .

Torna al Sommario

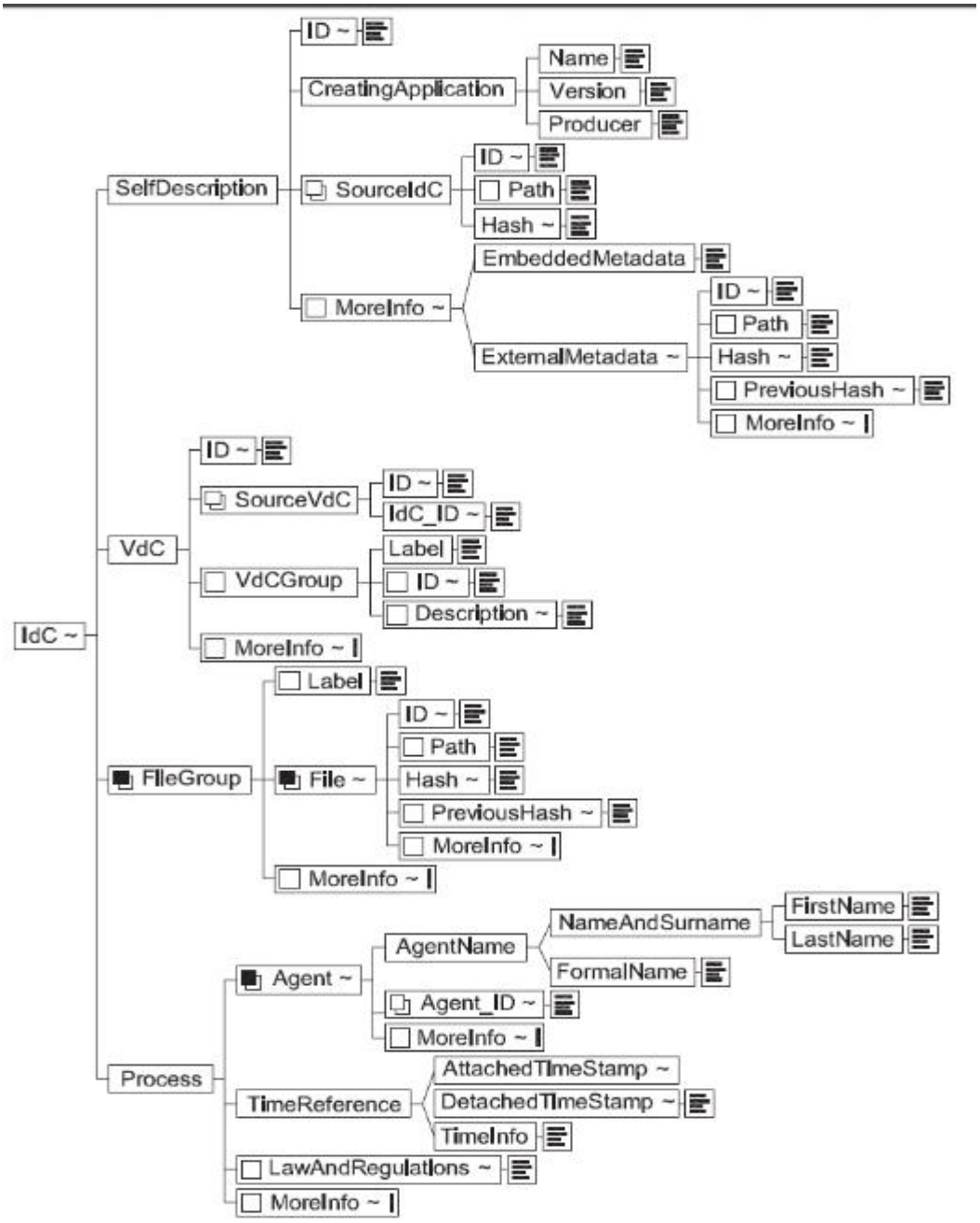

Figura 2 – Struttura dell' Indice di Conservazione (IPdA)

6.4 Pacchetto di distribuzione

Per il *Pacchetto di Distribuzione* si adottano le stesse specifiche del *Pacchetto di Archiviazione*, seguendo le indicazioni tecniche del DPCM del 3 Dicembre 2013 all'art.9, comma 1, lettera h.

Torna al Sommario

7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si compone di passi definiti con lo scopo di agevolare l'utente finale nel caricamento dei documenti digitali ed allo stesso tempo abbattere eventuali errori umani.

La prima fase è l'atto della deposizione del documento e la gestione dei *Pacchetti di Versamento* con relativi controlli. Il versamento dei pacchetti avviene tramite applicazione online con accesso protetto e criptazione dei dati.

Al termine del controllo, il processo termina con l'invio automatico di un Ricevuta di Versamento di tutti i pacchetti coinvolti (*Pacchetti di Archiviazione e di Distribuzione*).

Completata la fase di caricamento e versamento del documento, i *Pacchetti di Archiviazione* ed il *Pacchetto di Distribuzione* saranno visionati e firmati dal Responsabile del servizio di Conservazione che attuerà il processo di firma per completare il processo di conservazione, sulla base della delega del Responsabile della Conservazione.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato. Tale delega può essere affidata al Responsabile del servizio di conservazione

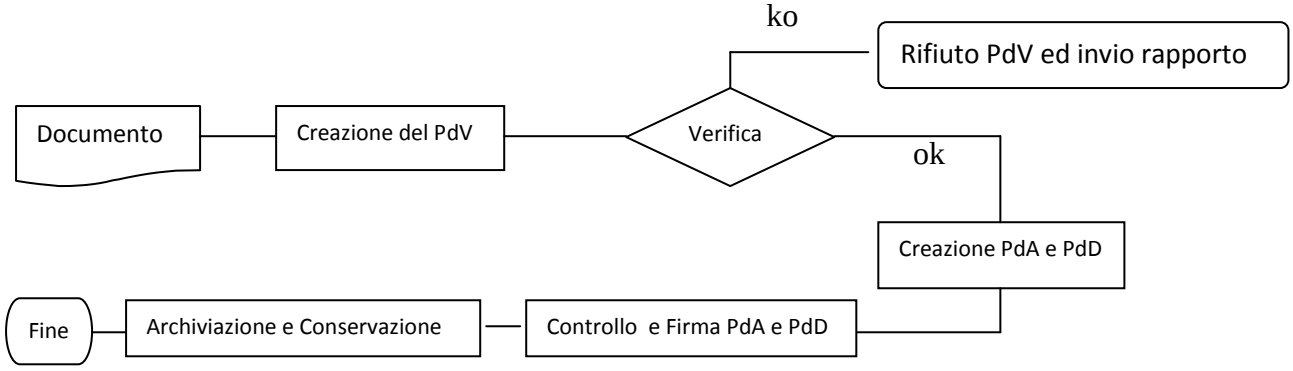

Figura 3 – Dettaglio grafico del processo di conservazione

Il *Pacchetto di Archiviazione* ed il *Pacchetto di Distribuzione* sarà copiato ulteriormente su dispositivi ridondanti di memorizzazione (sistema di backup su dischi in Raid 1). L'intera procedura verrà inoltre storicizzata tramite l'utilizzo di un file di Log specifico per ogni Pacchetto coinvolto nella procedura di conservazione. Il file di Log memorizza tutte le operazioni effettuate sul singolo pacchetto indicandone lo stato egli eventuali errori.

E' prevista la possibilità di effettuare una copia istantanea per eventuali controlli o richieste del cliente.

Le attività di gestione dei pacchetti di versamento seguono le *regole tecniche Art. 9, 1, lettera a.*
I controlli formali sul *Pacchetto di Versamento* ricevuto seguono le *regole tecniche Art. 9, comma 1, lettera b*
La generazione automatica della *Ricevuta di Versamento segue le regole tecniche Art. 9, comma 1, lettera),* dei
Pacchetti di Archiviazione (regole tecniche Art. 9, comma 1, lettera f) e del *Pacchetto di Distribuzione (regole tecniche Art. 9, comma 1, lettera g).*

Torna al Sommario

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

Per l'acquisizione dei *Pacchetti di Versamento,* il sistema utilizza un'architettura di tipo client-server basata sul protocollo *http.*

Per garantire una maggiore sicurezza nella comunicazione è opzionalmente possibile veicolare la chiamata tramite il protocollo HTTP su un Secure Socket Layer (SSL), anche detto *HTTPS.*

L' *HTTPS* utilizza un canale di comunicazione criptato tra il client
ed il server tramite la porta 443 anziché la porta 80 come avviene nel protocollo http –
Il livello di sicurezza è basato su Secure Socket Layer (SSL) o Transport Layer
Security (TLS).

L'utilizzo del protocollo HTTPS prevede la creazione di un certificato digitale che associ l'identità di una persona ad una chiave pubblica utilizzata per cifrare il traffico.

Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore (i browser web sono creati in modo da poter verificare la loro validità tramite una lista preimpostata).

Segue un diagramma generale dell'operazione

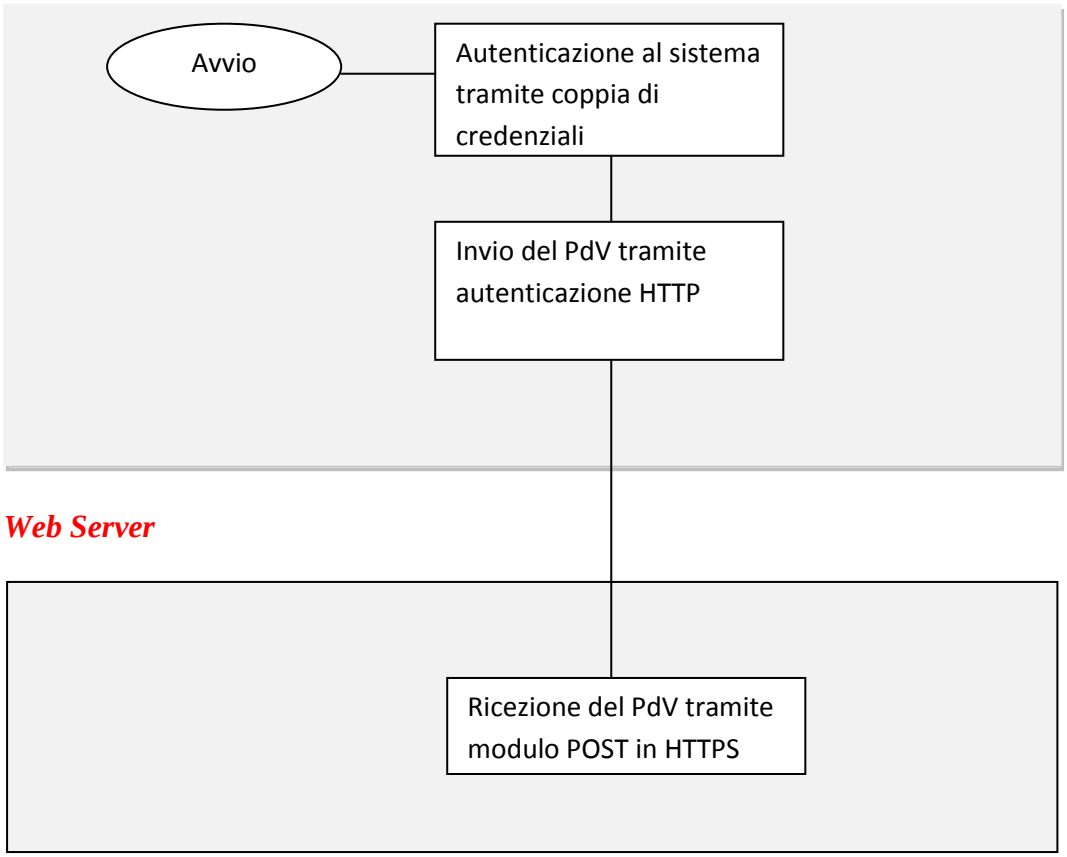

Figura 4 – Acquisizione generico pacchetto di Versamento

Gli header richiesti sono Authentication e RepositoryName che permettono al sistema invocante di specificare una propria chiave di autenticazione ed il nome del proprio repository di conservazione.
Questi due parametri vengono definiti in fase di attivazione del servizio di conservazione: il *"RepositoryName"* è un nome liberamente scelto dal produttore per identificare il proprio repository, mentre la *"Authentication"* è una chiave di autenticazione casuale erogante un coefficiente di univocità pari a 62 fattoriale combinazioni fornita direttamente al produttore.

A termine dell'acquisizione si genera automaticamente un file log con il dettaglio dell'esito della transazione.

In dettaglio, ogni *Log* indica nel nome file, la data e l'ora della ricezione in formato Timestamp.
Il contenuto del *Log* prevede le seguenti informazioni relative al singolo processo di versamento.

- Indirizzo IP del Produttore
- Repository scelta dal Produttore per il deposito del pacchetto di versamento
- Dettaglio sul tipo di documento
- Data ed ora di ricezione della chiamata (formato Unix Timestamp con precisione al secondo)
- Esito del processo di versamento

Il log inoltre notifica le seguenti informazioni :

- Tracciatura delle attività effettuate dal produttore verso il sistema di Conservazione
- Controllo di eventuali attacchi al repository cliente con immediato Alert al Responsabile della sicurezza del sistema come previsto nel manuale della ISO/EIC 27001:2013

Sarà cura e responsabilità del *Responsabile della Sicurezza del Sistema di Conservazione,* adottare soluzioni idonee

Torna al Sommario

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

Gestita la fase di ricezione del Pacchetto di Versamento, la successiva verifica consiste nel controllo sui contenuti.
Nel dettaglio le verifiche sono le seguenti :

• Verifica della corrispondenza del *PdV* con il formato *XML* atteso tramite un *XSD Validator.*
• Verifica dell'univocità del produttore tramite *identificativo* associato al repository di conservazione in cui si sta effettuando il versamento.
• Verifica della corrispondenza tra l'identificativo del tipo di oggetto associato al repository di conservazione e lo schema del *PdV* ricevuto (vedi capitolo 6 del presente documento).
• Verifica della corrispondenza tra il formato del documento informatico contenuto nel *PdV* e le tipologie di documenti informatici accettati per il tipo di oggetto e per il repository in cui si sta eseguendo il versamento.

Come ulteriore verifica si aggiungono ulteriori verifiche correlate alla validità contrattuale del produttore con Digitaly srl.

Le procedure di monitoraggio sui pacchetti di versamento sono eseguite automaticamente dal server tramite il software opensource **logalyze** per la gestione degli eventi sul server e la registrazione dei log.

La verifica avviene dapprima per tentativo di accesso all'applicazione web da parte dell'utente che intende tentare il caricamento di un pacchetto in conservazione
Come ulteriore verifica si verifica che il dato versato sia compatibile con quanto definito nelle specifiche del PdV .

Il log di monitoraggio sui pacchetti di versamento, è strutturato come di seguito:

- Colonna Data in formato TIMESTAMP
- Identificativo univoco del PdV
- IP pubblico mittente del PdV
- Nome utente dell'utenza che tenta l'invio del pacchetto di versamento
- Formato del PdV
- Nome e descrizione del pacchetto di versamento
- Status , che può assumere il valore di ERROR, OK, ALERT
  Lo stato avviene nel caso in cui il pacchetto di conservazione sia stato correttamente inviato ma non risulta leggibile per problemi legati alla protezione del file da parte del mittente o un formato non valido.

Produttore del documento

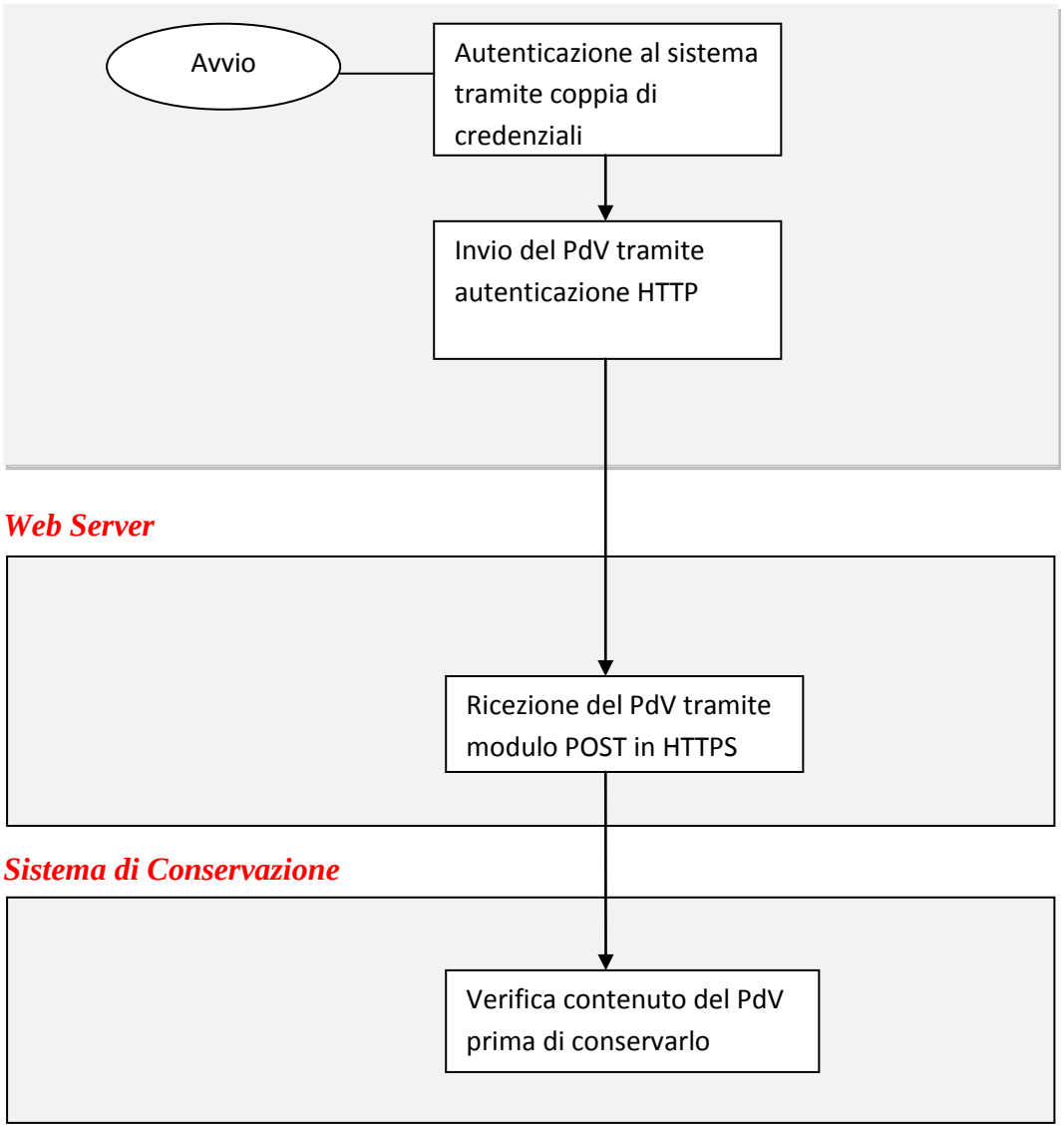

Figura 5 – Acquisizione generale pacchetto di Versamento

Torna al Sommario

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

Se le verifiche effettuate nel precedente paragrafo diano esito positivo, il sistema procederà con la generazione del Rapporto di Versamento, inviato allo stesso tempo al Produttore.
Avverrà allo stesso istante un log di pacchetto di versamento accettato.
Il log sarà strutturato come segue :

- Colonna Data in formato TIMESTAMP
- Identificativo univoco del PdV
- IP pubblico mittente del PdV
- Nome utente dell'utenza che tenta l'invio del pacchetto di versamento
- Formato del PdV
- Nome e descrizione del pacchetto di versamento
- Status , che può assumere il valore di ACCETTATO/NON ACCETTATO

Il *Rapporto di Versamento*, così come indicato dalle regole tecniche (Art. 9, comma 1, lettera d), contiene un hash del *Pacchetto di Versamento* che è stato preso in carico dal sistema di conservazione e dall'apposizione di un riferimento temporale UTC del momento in cui sia avvenuta la presa in carico.

I Rapporti di Versamento sono salvati all'interno del repository di conservazione dell'utente che potrà quindi accedervi in qualsiasi momento, seguendo le stesse politiche attuate per i *Pacchetti di Versamento*

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

Il non superare una delle condizione imposte per l'invio ed il contenuto dei Pacchetti di Versamento, comporta un rifiuto automatico dal Sistema di Conservazione

Tra le possibili cause del rifiuto di presa in carico del documento vi sono:
• Problemi tecnici relativi al formato del file inviato in relazione alla relativa classe documentale;
• Problemi tecnici con il salvataggio del file in fase di presa in carico;
• Problemi amministrativi relativi alla validità del contratto commerciale tra il produttore ed il conservatore.
Tutta la procedura di rifiuto dei Pacchetti di Versamento sarà memorizzata su dei log di sistema del servizio di conservazione, In ogni caso il produttore può contattare, se necessario, l'Help Desk

del servizio di conservazione o il Responsabile del servizio della Conservazione, per chiarimenti in merito alla natura del rifiuto da parte del sistema di conservazione, con riferimento alla presa in carico del documento stesso.

I pacchetti di versamento devono includere:

- elementi e attributi per ciascuna tipologia di oggetti (identificati secondo standard internazionali)
- definizione sulla base di accordi scritti con i soggetti produttori che depositano/versano i documenti/archivi delle procedure e delle modalità di gestione e accesso
- linee guida per l'acquisizione
- requisiti per un controllo fisico degli oggetti depositati
- verifica della completezza e accuratezza degli elementi informativi
- documentazione delle responsabilità per la conservazione
- utilizzo di sistemi che garantiscano l'identificazione univoca degli oggetti e i legami con le informazioni di rappresentazione
- utilizzo di meccanismi di verifica dell'integrità dei contenuti del deposito

la comunicazione di eventuali anomalie conterrà l'indicazione di quelle caratteristiche che non corrispondono al modello richiesto.
I riferimenti temporali saranno ottenuti tramite:

La trasmissione di una richiesta contenente l'impronta e si ottiene in risposta la marca temporale: un documento firmato dal certificatore contenente un insieme formato dall'impronta del documento per il quale si richiede la marcatura e da una informazione di data ed ora precisa e affidabile

Torna al Sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Durante la preparazione del Pacchetto di Archiviazione, si genera un logo di sistema contenente all'interno le seguenti informazioni :

• Riferimento temporale dell'operazione;
• Repository di conservazione di riferimento (con indicazione dell'utenza del Produttore);
• Identificativo interno al sistema di conservazione (c.d. *fileKey*) di salvataggio del *Pacchetto di Versamento;*
• Hash del *Pacchetto di Versamento*: hash (SHA256) del documento contenuto nel PdV, MD5 e SHA256 del *Pacchetto di Versamento* nella sua interezza;
• Identificativo interno al sistema di conservazione (c.d. fileKey) di salvataggio del Pacchetto di Archiviazione;

• Hash MD5 e SHA256 del *Pacchetto di Versamento* nella sua interezza.

Il *Pacchetto di Archiviazione* viene a questo punto inserito in uno pila FIFO (**First In First Out** - primo ad entrare, primo ad uscire) del Responsabile del servizio di Conservazione che provvede ad apporre la propria firma digitale secondo la
seguente procedura:

• Il Responsabile del servizio di Conservazione accede al pannello web di amministrazione del sistema di conservazione da cui ha evidenza di tutti i documenti (IPdA ed IPdD) in attesa della sua firma;
• Il Responsabile del servizio di Conservazione scarica sulla propria postazione locale i documenti da firmare.
• Il Responsabile del servizio di Conservazione appone la propria firma digitale sui documenti da firmare;
• Il Responsabile del servizio di Conservazione accede nuovamente al pannello web e carica sul sistema i documenti firmati.
• Il sistema di conservazione provvede ad apporre la Marca Temporale al documento controfirmato salvato interrogando la Time Stamping Autorithy.

Ad intervalli pianificati di 6 mesi rispetto alla data di presa in
carico, il sistema di conservazione provvederà ad effettuare un controllo automatizzato sui Pacchetti di Archiviazione conservati. Il controllo si articolerà sui seguenti punti:
• Verifica a livello base dell'integrità del file su filesystem effettuata calcolando l'MD5 e lo SHA256 del file memorizzato e confrontandoli con quelli memorizzati nel sistema di conservazione in fase di creazione del PdA
• Verifica del contenuto del PdA calcolando l'hash SHA256 del documento contenuto all'interno del Pacchetto di Versamento e confrontandolo con i valori riportati all'interno del Pacchetto di Archiviazione
Tale tipo di verifica, accedendo fisicamente al file in esame, può fornire adeguate garanzie sia in termini di disponibilità che di leggibilità del file.

Torna al Sommario

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

Il sistema di conservazione distingue in due modalità di accesso separate, una basata su *Autenticazione http* protetta, per permettere l'accesso al Produttore ai propri documenti conservati è disponibile una coppia di credenziali di accesso HTTP

Gli Header HTTP "Authentication" e "RepositoryName" permettono al sistema invocante di specificare una propria chiave di autenticazione ed il nome del proprio repository di conservazione.

Per l'accesso ai documenti in conservazione da parte di soggetti terzi rispetto al produttore, è richiesto l'intervento del Responsabile del servizio di Conservazione che, a partire da una determinata e specifica richiesta di accesso ai documenti, e se necessario con il supporto del *Responsabile della Funzione Archivistica di Conservazione*, valutata la legittimità della richiesta, può effettuare la ricerca del dato richiesto all'interno del sistema di conservazione tramite delle apposite interfacce.

Il soggetto produttore richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.
Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva secondo le modalità descritte nel manuale di conservazione

Una volta identificato il documento ricercato dall'interfaccia web, è possibile scaricare tutta la catena dei file relativi al documento ricercato, quindi: *Pacchetto di Distribuzione*. In particolare per quel che concerne il *Pacchetto di Distribuzione* è anche possibile scaricare la versione dei documenti controfirmati dal *Responsabile del servizio di Conservazione* e le relative marche temporali.

In questo secondo caso, qualora i documenti debbano essere trasferiti presso un'altra locazione, si applicheranno tutte le linee guida per la sicurezza dei dati in uscita dal perimetro dell'azienda previsti dalla certificazione ISO/EIC 27001:2013 in particolar modo per quel che riguarda le procedure di cifratura dei dati in uscita, dell'anonimizzazione dei volumi che li contengono e le politiche di distruzione dei volumi una volta completate le operazioni. A tal proposito si rimanda alla *PS03 "Procedura di classificazione delle informazioni, gestione e smaltimento dei supporti removibili e cartacei"* delle procedure ISO/EIC 27001:2013.

Torna al Sommario

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

Il sistema di conservazione permette agli utenti, che vogliano avere una copia dei documenti conservati, di accedere in autonomia agli stessi, purché dispongano delle opportune autorizzazioni, tramite le opportune procedure di sicurezza.
Tali procedure permettono di accedere sia ai documenti originali, sia alle versioni controfirmate dal *Responsabile del servizio di Conservazione*
Il sistema di conservazione prevede inoltre una procedura precisa finalizzata ad effettuare l'adeguamento dei formati all'evoluzione tecnologica, generalmente gestita come procedura di riversamento, che può essere di tipo diretto o di copia informatica.

Il procedimento di *riversamento diretto* consiste nel trasferimento di un documento (già conservato), da un supporto di memorizzazione ad un altro, senza alterarne la rappresentazione digitale (ad esempio, la generazione di copie di sicurezza), e non è soggetto a prescrizioni formali specifiche.

La *copia di un documento informatico*, è un processo che trasferisce un documento, già conservato, da un supporto di memorizzazione ad un altro, modificando la rappresentazione informatica del suo contenuto. Esso richiede, l'apposizione della firma elettronica qualificata e della marca temporale sull'insieme dei documenti (ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti o di insiemi di essi), da parte Responsabile del servizio di Conservazione

Per il perfezionamento della *copia di un documenti informatici*, occorre, altresì, l'apposizione del riferimento temporale e della firma elettronica qualificata da parte di un *Pubblico Ufficiale* (necessaria anche per il riversamento di documenti analogici originali unici conservati).

Torna al Sommario

7.8 Scarto dei pacchetti di archiviazione

Il sistema di conservazione provvederà in maniera automatizzata allo scarto dei pacchetti di archiviazione che abbiano superato i tempi di conservazione previsti per la specifica tipologia di oggetto contenuto al suo interno.
Il servizio di conservazione, con un processo automatizzato eseguito almeno 4 volte al mese, provvederà a fare una revisione dei documenti presenti nei repository di conservazione, confrontando la data di presa in carico degli stessi con la data attuale in relazione al periodo previsto di conservazione. Qualora il periodo di conservazione sia scaduto, il sistema provvederà ad effettuare una cancellazione *"logica"* dei record relativi ai *Pacchetti di Versamento* scartati.

Contemporaneamente il sistema di conservazione provvederà a notificare il produttore dell'avvenuta preparazione allo scarto dei pacchetti, tramite un canale di comunicazione, definito nell'ambito del contratto d'utilizzo del sistema di conservazione.
Qualora nel successivo mese solare il produttore non effettui comunicazioni richiedendo il ripristino dei documenti in oggetto, il sistema provvederà alla loro cancellazione fisica allo scadere del periodo di conservazione più un mese, basandosi sul principio del silenzio assenso.

Nel caso di archivi pubblici o privati, che rivestono interesse storico, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero per i beni e le attività culturali rilasciata al Produttore secondo quanto previsto dalla normativa vigente in materia (D. lgs. 42/2004)

Torna al Sommario

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

Al fine di agevolare l'interoperabilità tra i sistemi di conservazione, come richiesto in più passaggi delle regole tecniche del DPCM 3 dicembre 2013, il sistema di conservazione adotta alcune scelte tecniche di adozione di standard di formati e gestione dei tracciati dati, a cui si affiancano alcune scelte gestionali dei documenti. Nel dettaglio:

• Per l'accettazione dei file presi in carico, l'aderenza ad un subset di formati di documenti "standard", indicati all'allegato 2 delle regole tecniche del DCPM 3 dicembre 2013;
• Per la generazione dei file di Indice del Pacchetto di Archiviazione, che permettono di organizzare e catalogare i Pacchetti di Archiviazione che si stanno ricevendo, l'aderenza allo standard UNI 11386 "SInCRO";
• Per la generazione dei Pacchetti di Distribuzione, come indicato dalle regole tecniche all'Art. 9, comma 1, lettera h, la corrispondenza univoca tra Pacchetto di Versamento preso in carico, Pacchetto di Archiviazione generato, e Pacchetto di Distribuzione.
In particolare in fase di conclusione del rapporto per cessazione del servizio di conservazione, l'insieme dei documenti in conservazione sarà reso disponibile al produttore su un supporto adeguato alle dimensioni da trattare ovvero sarà reso disponibile tramite download dal sistema di conservatoria con un'apposita procedura che genera un archivio compresso. Il periodo previsto per la gestione delle procedure di rilascio dei documenti alla fine dei rapporti contrattuali è di 30 giorni, durante i quali sarà cura del Produttore richiedere l'accesso a copia dei file.

8 IL SISTEMA DI CONSERVAZIONE

Nel seguente paragrafo vengono descritte le componenti logiche, tecnologiche e fisiche coinvolte nel sistema di conservazione, con particolare risalto agli aspetti di sicurezza ed alle procedure adottate per garantire la massima qualità del servizio erogato.

Torna al Sommario

8.1 Componenti Logiche

Il sistema di conservazione si divide in due aree :

• Un'interfaccia *web* di amministrazione del sistema di conservazione con la quale interagisce sia il *Responsabile del servizio della Conservazione* (per supervisionare il processo trasversale a tutto

il sistema di conservazione ed effettuare le attività di firma dei documenti *"alla firma"* quali i *PdA* ed i *PdD* generati), sia il Produttore (per controllare e gestire il funzionamento dei propri repository di conservazione, accedere ai propri documenti conservati eccetera). L'interfaccia *web* è ospitata presso un Server in Aruba dotato di protocollo HTTPS.

• Un'interfaccia di *web services* di tipo HTTP REST dedicata all'integrazione del sistema di conservazione con altre piattaforme software (generalmente di competenza del Produttore) che gestisce la ricezione e la trasmissione di qualsiasi documento verso e dal sistema di conservazione.

Torna al Sommario

8.2 Componenti Tecnologiche

L'infrastruttura tecnologica e composta da più elementi interoperanti tra loro.
Ricalcando la divisione delle componenti logiche, le seguenti sono le tecnologie di riferimento per l'implementazione di ogni livello di servizio:
• *L'interfaccia WEB:* interfaccia HTML5 e CSS e linguaggio PHP, operante su protocollo HTTP o HTTPS all'interno del web server Apache Httpd.
La parte di autenticazione è basata sugli standard OpenID ed OAuth2.
Dialoga con la parte di Web Services tramite chiamate HTTP di tipo REST
• *L'interfaccia Web Services* è sviluppata in linguaggio PHP e dialoga secondo lo standard REST con un set di API di tipo open all'interno del web server Apache Httpd.
L' interfaccia interroga un database relazionale MySQL.
Dialoga con la parte di interfaccia Web e con i sistemi esterni tramite chiamate HTTP di tipo REST

Tutti i sistemi sono operanti dietro dei Load Balancer basati su Apache e sono responsabili delle logiche di gestione dell'integrità di sessione e delle logiche di fault tolerance e fallback in caso di problemi sui singoli server;

• I sistemi sono operanti in ambiente UNIX (FreeBSD) e Windows Server 2012 vengono monitorati tramite protocolli SNMP per verificare lo stato delle macchine ed il loro carico

• Il sistema di backup utilizza ntbackup di Windows Server ed RSync in ambiente Linux

Torna al Sommario

8.3 Componenti Fisiche

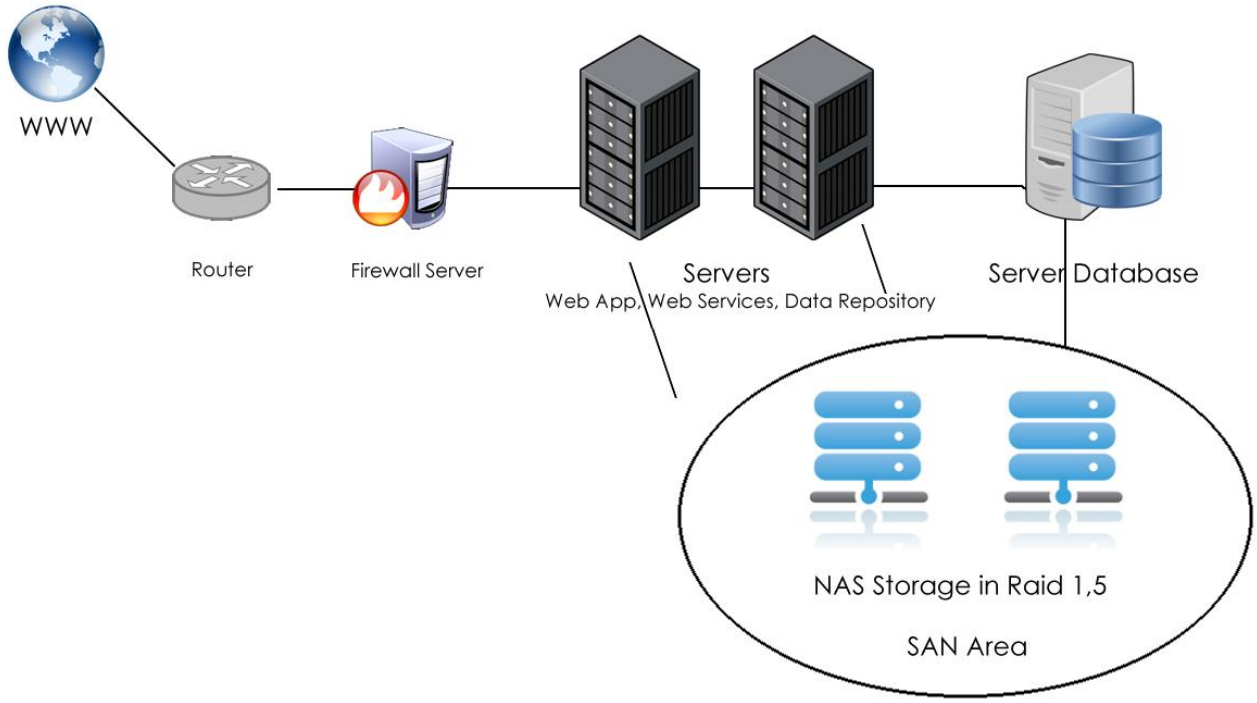

Figura 6 – Componenti Fisiche

Le componenti fisiche sono pensate e configurate per offrire maggiore ridondanza possibile sia per la connessione alla rete, servizi e backup dei dati .

Il Datacenter principale è in Digitaly Srl.

Tutte le schede di rete sono ridondanti con velocità massima di 1Gb/s

Sul Server sono poggiati tutti i principali servizi :

- Applicazioni PHP/Ajax/Javascript/html
- Procedure e Routine

Tutti i documenti archiviati, oltre alle repository nei server, sono ulteriormente conservati presso il sito Disaster Recovery in Aruba Spa . Il sistema di Backup comprende un server dotato di massima ridondanza su alimentazione,dischi in RAID 5,scheda di rete, di un server Linux per replicare il backup dei dati e di un sistema NAS con dischi in RAID 1 e per garantire ulteriore ridondanza del Backup dei dati, localizzato in un area distinta di Digitaly

Torna al Sommario

8.4 Procedure di gestione e di evoluzione

Il sistema di conservazione si attiene totalmente alle procedure previste nell'ambito della certificazione ISO/EIC 27001:2013.

Nello specifico esse riguardano:

• La conduzione e la manutenzione dei sistemi di conservazione:

Il sistema di conservazione è condotto e programmato dal Responsabile dei sistemi informativi ed il Responsabile dell'archiviazione.

L'obiettivo della manutenzione e mantenimento delle infrastrutture, è quello di garantire il corretto funzionamento degli apparati di sicurezza ambientale e perimetrali secondo le specifiche tecniche dei fornitori e quanto previsto dalla Politica per la Sicurezza, al fine di evitare perdite preventive, danni, furti o interruzioni dell'attività di DIGITALY SRL

Eventuali incidenti o interruzioni sono gestiti dal Responsabile della sicurezza il quale ne definisce la codifica preventiva e la gestione degli stessi.

• La gestione e la conservazione dei backup:

Per l'archiviazione dei dati digitali sono state messe a punto le seguenti strategie:

- Viene eseguito un back up giornaliero incrementale mentre dal venerdì alla domenica viene eseguito Full (integrale).

I back up prevedono una identificazione univoca di ogni singolo supporto.

Il data base dell'applicativo delle copie di sicurezza da indicazioni rispetto a identificativo / file del supporto dove è presente il file da ripristinare. Per ridurre al minimo la perdita di dati e consentire la continuità di funzionamento, si usa tecnologie RAID Redundant Array of Inline Disks) per il server che effettuano maggiore ridondanza del sistema anche in caso di danneggiamento di uno o più dischi. La periferica di Backup è configurata in RAID 5 denominato "Mirroring", duplica i dati archiviati su uno o più dischi aumentando la ridondanza del sistema in modo che, in caso di guasto al disco principale, i dati "Mirrorizzati" sono ancora disponibili evitando così la perdita di dati e il disservizio.

Questa configurazione è quindi dotata di fault tolerance in cui parte della capacità di archiviazione contiene informazioni ridondanti sui dati memorizzati. Le informazioni ridondanti contenute nei dischi consentono di mantenere in esecuzione il sistema in caso di malfunzionamento di un singolo

disco. La presenza di dischi di riserva consente al sistema di sopportare più rotture disco contemporaneamente. Lo storage è poi interconnesso direttamente con il produttore per cui in caso di guasto viene inviata una E-mail informativa a seguito della quale lo stesso servizio tecnico del produttore attiva le procedure per la verifica e l'eventuale intervento sul sistema in fault. Inoltre lo storage è dotato di tecnologia HOT SWAP (sostituzione a caldo) e consente di sostituire i dischi rigidi che non funzionano senza arrestare il sistema.

• La gestione e la conservazione dei log:
La gestione dei Log è seguita dal Responsabile della Sicurezza Informatica e prevede la consultazione giornaliera dei Log di ambito sistemistico e di ambito archivistico . Tutti i log sono conservati in modalità ridondante all'interno del server dati DIGITALY e in backup sia sullo storage che sul luogo del Disaster Recovery. In caso di anomalie riscontrate sui log si provvederà tempestivamente a darne comunicazione all'ente produttore.

• La gestione ed il monitoraggio dei sistemi fisici:
Il monitoraggio ordinario dei sistemi fisici è gestito dal Responsabile dei sistemi informativi .
I sistemi fisici controllati rientrano nell'intera Area CED e Disaster Recovery. Tutti i sistemi sono monitorati mediante avvisi email, sms e log di analisi delle prestazioni e continuità .

Consiste nel tenere aggiornata la documentazione che mappa lo stato della rete e delle configurazioni, nel verificare lo stato di funzionamento degli apparati in termini di connettività, disponibilità e verifica dei livelli di servizio.
Il referente delle infrastrutture e tecnologie di rete per ciascun cambiamento dell'infrastruttura, o della configurazione, previa analisi del rischio mutato, apporta gli aggiornamenti alla documentazione in cui è descritta l'infrastruttura e la configurazione.
Per ciascuna modifica alle connessioni di rete ciascun punto di terminazione deve essere dotato di un identificatore assegnato in maniera univoca all'interno del sistema di cablaggio. I cavi devono essere dotati di identificatori a entrambe le estremità, e la stessa dicitura riportata agli estremi dei cavi è la stessa presente sui connettori installati sulla presa di telecomunicazioni. I nuovi cavi di trasmissione dati installati devono essere inseriti nelle canaline preesistenti nel rispetto dei volumi massimi occupabili per garantire la manutenibilità (sfilabilità etc). Devono inoltre essere mantenute le proprietà di protezione da intercettazioni non autorizzate o da danni da schiacciamento e la separazione dai cavi di alimentazione elettrica.

• Change Management:

Il processo di gestione del cambiamento si articola nelle seguenti fasi:

- Fase 1: Creazione Richiesta
- Fase 2: Valutazione e Accettazione della soluzione
- Fase 3: Schedulazione/Pianificazione
- Fase 4: Implementazione
- Fase 5: User acceptance test
- Fase 6: Passaggio in produzione
- Fase 7: Chiusura

• La gestione degli accessi alle strutture fisiche dove opera il sistema di conservazione:
Gli accessi alle strutture fisiche è limitato al solo Responsabile dei sistemi informativi. Per visitatori o utenti interni a DIGITALY Srl , l'accesso alla struttura fisica (CED) è autorizzata dal Responsabile dei sistemi informativi. L'accesso alla struttura richiede il censimento dell'utente tramite apposito modulo degli accessi.

• Le problematiche di gestione degli utenti e degli accessi ai sistemi logici:
Le problematiche di gestione ed accessi degli utenti a sistemi logici (piattaforma web di conservazione, altro) richiede una verifica da parte del responsabile dei sistemi informativi per una prima fase di accertamento della problematica, una valutazione per la soluzione del problema, la risoluzione del problema e il censimento del problema sul registro degli incidenti.

• Verifica periodica di conformità e normativa standard di riferimento :

L'integrità dei files sarà verificata periodicamente ed aggiornata in base alla normativa standard di riferimento ISO 14721:2012 OAIS (Open Archival Information System)

Torna al Sommario

9 MONITORAGGIO E CONTROLLI

Sono impostati ed automatizzati degli schemi di controllo finalizzati alla verifica generale del processo di archiviazione e della corretta funzionalità delle componenti fisiche e logiche.

9.1 Procedure di monitoraggio

I controlli periodici sono posti ad interrogare tutti i server facenti parte dell'infrastruttura del sistema di conservazione, con meccanismi e procedure operanti nelle seguenti modalità:
• Interrogazione *ICMP* (ping);
• Interrogazione *SNMP* (per verifica del carico di lavoro di ogni server, degli spazi software disponibili ed altro);
• Interrogazione *HTTP/HTTPS* (per le macchine su cui è in esecuzione *Apache* per verificare il corretto funzionamento del sistema);
• Interrogazione MySQL (per le macchine su cui è in esecuzione MySQL per verificare il corretto funzionamento del sistema ed il livello di carico del sistema di RDBMS).

Tutte le interrogazioni imposte sono scansionate in un range di tempo tra i 3 e i 10 minuti in base all'effettiva priorità dell'oggetto da monitorare.

Oltre alle procedure indicate vengono notificati periodicamente gli avvisi e log sullo stato delle architetture, dall'esaurimento del disco, lo stato del sistema di dissipazione, eventuali anomalie sulle schede di rete.
Tutti i log tecnici vengono conservati nei sistemi dedicati all'interno dell'infrastruttura di Conservazione di Digitaly srl.
Torna al Sommario

9.2 Verifica dell'integrità degli archivi

Il sistema di conservazione esegue in maniera automatizzata dei controlli ad intervalli periodici sull'integrità dei file contenuti all'interno del sistema di conservazione.
Periodicamente il sistema verifica l'integrità degli archivi tramite la corrispondenza tra l'hash MD5 e l'hash SHA256 di tutti i file salvati all'interno della SAN ed i relativi valori memorizzati all'interno del database MySQL dei *web services*.

Per l'allerta preventiva la verifica effettuata sugli archivi, prevede controlli che saranno determinati sulla base di principi e criteri definiti in base alla natura dei documenti vigilato dal Responsabile dell' Archiviazione.

Prima della creazione del PdA tutti i files sono preventivamente verificati al fine di accertarne la leggibilità, escludere la presenza di software malevoli, eventuali password di protezione applicate ai files.

Torna al Sommario

9.3 Soluzioni adottate in caso di anomalie

Nel caso di anomalie si attiva un sistema di avviso automatizzato del personale responsabile e del *Responsabile del servizio della Conservazione*.

A seconda del tipo di anomalia riscontrata la situazione può essere normalizzata copiando una versione corretta da un altro nodo di servizio a quello dove è emersa l'anomalia o, qualora la versione corretta non sia più rintracciabile, ripristinando il file originale da un backup integro.
In regola con le procedure previste dalla certificazione ISO/EIC 27001:2013 e ISO 9001:2008 qualsiasi tipo di anomalia riscontrata viene tracciata all'interno del *Registro degli Incidentidi Sicurezza* o nel *Registro delle non Conformità.*

In dettaglio :

Nel caso di software malevoli : Si provvedera qualora possibile alla rimozione e lo scarto del software malevolo, nel caso impossibilitati si provvede al recupero da un backup integro

Nel caso di password: Nella ricezione del pacchetto di versamento, tutti i files saranno verificati per accerterne la leggibilità, nel caso di password applicata al file dall'ente produttore, il pacchetto di versamento viene scartato con notifica email PEC all'ente produttore con successiva richiesta del pacchetto originale senza protezione password.

Nel caso di illegibilità: Se il pacchetto di versamento ricevuto include un file illegibile, se ne richiede copia da parte dell'ente produttore altrimenti il pacchetto di archiviazione non verrà generato. Le notifiche saranno inviate mediante email PEC.

Torna al Sommario