Manuale di Conservazione

di Enerj S.r.l.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	24/09/2015	Ferdinando Auletta	*Responsabile del Servizio di Conservazione*
Verifica	24/09/2015	Silvano Artioli	*Responsabile della Sicurezza del Sistema di Conservazione*
Approvazione	24/09/2015	Giovanni Auletta	*Direzione*

REGISTRO DELLE VERSIONI

Num. versione	Data emissione	Modifiche apportate
1	Settembre 2005	Stesura
2	Febbraio 2006	Aggiornamento
3	Ottobre 2006	Aggiornamento
4	Marzo 2007	Aggiornamento
5	Novembre 2008	Aggiornamento
6	Marzo 2009	Aggiornamento
7	Marzo 2010	Aggiornamento
8	Marzo 2013	Aggiornamento
9	Novembre 2014	Aggiornamento
10	Febbraio 2015	Aggiornamento
11	Settembre 2015	Aggiornamento per accreditamento AGID

INDICE DEL DOCUMENTO

1 INTRODUZIONE

Enerj, società operante nel settore informatico dal 2005, progetta, sviluppa e distribuisce piattaforme software per la gestione degli archivi informatici, l'archiviazione documentale e la conservazione digitale a norma di legge.

Nell'ambito della gestione delle proprie attività peculiari, Enerj eroga un servizio di conservazione digitale rivolto alle organizzazione pubbliche e private.

Allo scopo di garantire il livello massimo di qualità dei servizi e dei prodotti distribuiti, Enerj ha implementato un sistema di gestione della qualità e della sicurezza delle informazioni, ottenendo le certificazioni:

- ISO/IEC 27001:2013
- UNI EN ISO 9001:2008

dall'ente CSQA (accreditato da Accredia) per le seguenti attività:

"Progettazione, sviluppo e distribuzione di software e servizi informatici; attività di assistenza alla clientela, erogazione di archiviazione e conservazione digitale, di gestione elettronica di documenti e di fatturazione elettronica per enti pubblici e privati".

2 SCOPO E AMBITO DEL DOCUMENTO

Il Manuale di Conservazione di Enerj (di seguito MdC) è un documento informatico redatto al fine di documentare il Sistema di Conservazione (SdC):

- dei documenti informatici, prodotti dai Clienti di Enerj nel corso della gestione della propria attività e dell'erogazione dei propri servizi di gestione degli archivi informatici;
- di altri documenti informatici che, per qualsiasi altra ragione, Enerj ritenga opportuno gestire tramite il sistema documentato dal presente manuale.

Il MdC è redatto inoltre al fine di documentare le modalità e le tempistiche adottate nella gestione dei processi di conservazione dei documenti informatici che ne consentono il mantenimento del valore legale (civile e fiscale) in base a quanto previsto dal panorama normativo vigente.

Il sistema assicura la conservazione dei documenti informatici garantendone il mantenimento delle caratteristiche di autenticità, integrità, intelligibilità, affidabilità, reperibilità e interoperabilità.

Il presente documento sostituisce le versioni precedenti.

2.1 Specificità di contratto

Il MdC descrive il funzionamento delle componenti generali del Sistema di Conservazione (SdC) implementato e gestito da Enerj. Il MdC non ha al suo interno componenti personalizzate o specifiche per singolo cliente. Ogni aspetto particolare del servizio di conservazione quale ad esempio, i documenti coinvolti, metadati scelti per l'archiviazione dei documenti, formati dei documenti, modalità di trasferimento e riferimenti presso il cliente, viene concordato e descritto nel Contratto di Servizio di Conservazione e nello Schema di conservazione (MCD01).

Torna al sommario

3 TERMINOLOGIA

3.1 GLOSSARIO

Preliminarmente si conviene di attribuire, ai termini tecnici utilizzati nel testo che segue, il significato di cui:

- all’art. 1, comma 1 del Decreto Legislativo n. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale) e successive modifiche;
- all'art. 1 del Decreto del Presidente del Consiglio dei Ministri del 30 marzo 2009.
- all'Allegato: Regole tecniche in materia di documento informatico e gestione documentale, protocollo informatico e conservazione di documenti informatici: "Glossario e Definizioni" del Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013.

L'intera struttura e tutti i contenuti del manuale sono redatti sulla base dei modelli, della terminologia e delle indicazioni fornite dall'Agenzia per l'Italia Digitale.

Di seguito si riporta in ordine alfabetico il Glossario dei termini e Acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata.

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro

certificatore accreditato	soggetto, pubblico o privato, riconosciuti dall' Agenzia per l'Italia Digitale che emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Contratto di Servizio	Documento contrattuale stipulato tra il Cliente (Produttore) ed Enerj (Conservatore) che contiene la descrizione analitica del servizio. Gli accordi di dettaglio sono riportati negli specifici allegati
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
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 CAD.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Hardware Security Module	dispositivi per la gestione sicura delle firme digitali che ne velocizzano l'apposizione e ne permettono la completa gestione in remoto
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione

immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash*
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
integrità	insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
JDoc	Software proprietario di Enerj di gestione elettronica dell'archivio informatico
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati

Manuale della Sicurezza del Sistema Informativo	documento interno che descrive le attività, le caratteristiche tecniche e procedurali del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio
marca temporale	Riferimento temporale rilasciato da un certificatore accreditato che garantisce data e ora certa
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3 dicembre 2013
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel Manuale di Conservazione

pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici
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 il responsabile della gestione documentale
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Schema di Conservazione	modulo interno personalizzato per ogni Cliente contenente la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione
sistema di conservazione	sistema di conservazione dei documenti informatici
sistema di gestione informatica dei documenti	sistema che consente la tenuta di un documento informatico come ad esempio il software di Enerj JDoc

staticità	caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
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

3.2 ACRONIMI

ACRONIMO	DEFINIZIONE
AGID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
DIR	Direzione aziendale
DPCM	Decreto del Presidente del Consiglio dei Ministri del 03 dicembre 2013
FTP (e FTPS)	File Transfer Protocol - Protocollo informatico di trasmissione di informazioni tra mittenti e destinatari, FTPS è il medesimo protocollo ulteriormente implementato con appositi criteri informatici allo scopo di aumentarne il livello sicurezza.
HSM	Hardware Security Module
IPdA	Indice del pacchetto di archiviazione
ISMS	Information Security Management System - Sistema di gestione della qualità e della sicurezza delle informazioni di Enerj

MdC	Manuale di Conservazione
MSI	Manuale della Sicurezza del Sistema Informativo
OAIS	Open Archival Information System
PBK	Piano di Backup
PCO	Piano di Continuità Operativa del Business e Disaster Recovery
PCD	Procedura di Gestione della Conservazione
PGC	Procedura di Gestione Clienti e Assistenza
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
RCM	Responsabile gestione Commerciale, Comunicazione e Marketing
RDA	Responsabile Direzione Amministrativa e contabile
RDT	Responsabile Direzione Tecnica
RFA	Responsabile della Funzione Archivistica
RGC	Responsabile Gestione dei Clienti e assistenza
RGP	Responsabile Gestione del Personale

RQS	Responsabile della sicurezza dei sistemi per la conservazione
RSC	Responsabile Servizio di Conservazione
RSI	Responsabile dei sistemi informativi per la conservazione
RSM	Responsabile sviluppo Software e Manutenzione
SdC	Sistema di Conservazione
SLA	Service Level Agreement

4 NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito è riportata la principale normativa di riferimento per l'attività di conservazione a livello nazionale.

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è riportato di seguito.

4.1 Normativa inerente per la conservazione - Legislazione Italiana

- **Codice Civile –** "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 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 11 febbraio 2005 n. 68** . Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del 2 novembre 2005** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (Gazzetta Ufficiale n. 266 del 15-11-2005) del Ministro per l'Innovazione e le Tecnologie;
- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009** - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- **Deliberazione Cnipa del 21 maggio 2009, n. 45** (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;

- **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 21 marzo 2013** - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- **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.
- **Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

4.2 Altre normative

- **Decreto Legislativo 1 settembre 1993 n.385** - "Testo unico delle leggi in materia bancaria e creditizia";
- **Decreto Legislativo 6 settembre 2005, n. 206** - Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229;
- **Decreto Legislativo 9 aprile 2008, n. 81** - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;
- **Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i.** – Codice in materia di protezione dei dati personali;

- **Legge 22.04.1941 n° 633 , G.U. 16.07.1941 e s.m.i.** - Legge sul diritto d'autore.

4.3 Standard tecnici internazionali di riferimento

4.3.1 ISO/IEC

- **UNI EN ISO 9000:2005** - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- **UNI EN ISO 9001:2008 -** Sistemi di gestione per la qualità - Requisiti;
- **UNI EN ISO 9004:2009 -** Gestire un'organizzazione per il successo durevole: L'approccio della gestione per la qualità;
- **UNI EN ISO 19011:2012 -** Linee guida per audit di sistemi di gestione;
- **ISO 14721:2012 -** Space data and information transfer systems - Open archival information system (OAIS) - Reference model; Sistema informativo aperto per l'archiviazione;
- **UNI ISO 31000:2010 -** Gestione del rischio - Principi e linee guida;
- **ISO/IEC 27000:2012 -** Overview and vocabulary;
- **ISO/IEC 27001:2013 -** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27002:2013 -** Code of practice for information security controls;
- **ISO/IEC 27005:2011 -** Information technology -- Security techniques -- Information security risk management;
- **UNI ISO 15489-1:2006** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- **UNI ISO 15489-2:2007** - Informazione e documentazione - Gestione dei documenti di archivio - Linee Guida sul record management;
- **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.

4.3.2 ETSI (European Telecommunications Standards Institute)

- **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) -** Electronic Signatures and

Infrastructures (ESI); Data Preservation Systems Security; Part 2: Guidelines for Assessors; Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni

- **ETSI GS ISI 001-1 V1.1.1 (2013-04) -** Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operation al indicators for organizations to use to benchmark their security posture;
- **ETSI GS ISI 001-2 V1.1.1 (2013-04) -** Information Security Indicators (ISI);Indicators (INC); Part 2: Guide to select operational indicators based on the full set given in part 1;
- **ETSI GS ISI 002 V1.1.1 (2013-04) -** Information Security Indicators (ISI); Event Model A security event classification model and taxonomy;
- **ETSI GS ISI 003 V1.1.2 (2014-06) –** Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection;
- **ETSI GS ISI 004 V1.1.1 (2013-12) -** Information Security Indicators (ISI); Guidelines for event detection implementation.

4.3.3 OAIS (Open Archival Information System)

- Consultative Committee for Space Data Systems (CCSDS – Audit and Certification of Trustworthy Digital Repositories – Recommended Practice – CCSDS 652.0-M-2 - 2012;
- Consultative Committee for Space Data Systems (CCSDS – Reference Model for an Open Archival Information System (OAIS).

Torna al sommario

5 RUOLI E RESPONSABILITÀ

5.1 Ruoli esterni al SdC

5.1.1 Produttore

È il Cliente che, avvalendosi dei servizi di gestione degli archivi informatici erogati da Enerj, conferisce al SdC i documenti informatici (di cui è titolare) da conservare elettronicamente.

5.1.2 Fruitore

Il ruolo del Fruitore del SdC è ricoperto dai soggetti che, opportunamente autorizzati, accedono al SdC ottenendo uno o più Pacchetti di Distribuzione (PdD).

5.1.3 Certification Authority e fornitori di servizi di Firma Digitale

I certificati crittografici utilizzati nel processo di firma sono certificati rilasciati da Certificatori accreditati dall'AGID.

Il dispositivo HSM deputato alle operazioni di firma è conforme al D.P.C.M. 22 febbraio 2013 e viene mantenuto in un Data Center, sito presso il Certificatore Accreditato, con certificazioni ISO 27001:2005, ISO 9001:2008, ISO 14001:2004, OHSAS 18001:2007.

5.1.4 Time Stamping Authority

Le marche temporali utilizzate nel processo di apposizione del riferimento temporale sono rilasciate da Certificatori accreditati dall'AGID.

5.2 Ruoli interni al SdC

Per motivi di riservatezza il nominativo ed i riferimenti dei soggetti riportati nelle sezioni che seguono sono omessi dal presente manuale e sono esclusivamente indicati nel Contratto di Servizio nel quale sono anche presenti le attività affidate al Responsabile del Servizio di Conservazione, i periodi di permanenza negli incarichi riferiti ai diversi profili e le eventuali deleghe.

5.2.1 Responsabile del Servizio di Conservazione (RSC)

Il RSC è individuato, all'interno dell'organigramma di Enerj, come Responsabile dei Servizi di gestione dell'archivio informatico e conservazione ed è incaricato delle seguenti funzioni:

- Definisce e attua le politiche complessive del sistema di conservazione, nonché il governo della gestione del sistema di conservazione;

- Definisce le caratteristiche e i requisiti del sistema di conservazione in conformità alla normativa vigente;
- Assicura la corretta erogazione del servizio di conservazione all'ente produttore;
- Gestisce le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

5.2.2 Responsabile della sicurezza dei sistemi per la conservazione (RQS)

- Definisce le politiche di rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza;
- Segnala le eventuali difformità a RSC, individua e pianifica le necessarie azioni correttive.

5.2.3 Responsabile funzione archivistica di conservazione (RFA)

- Definisce e gestisce il 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;
- Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici;
- Monitora il processo di conservazione e attua analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- Collabora 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.

5.2.4 Responsabile del Trattamento dei Dati personali (DIR)

- Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
- Garantisce 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

5.2.5 Responsabile sistemi informatici per la conservazione (RSI)

- Gestisce l'esercizio delle componenti hardware e software del sistema di conservazione;
- Monitora il mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;
- Segnala le eventuali difformità degli SLA al RSC e individua e pianifica le necessarie azioni correttive;
- Pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione;
- Controlla e verifica i livelli di servizio erogati da terzi e segnala le eventuali difformità al RSC.

5.2.6 Responsabile sviluppo e manutenzione del sistema (RSM)

- Coordina lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione;
- Pianifica e monitora i progetti di sviluppo del sistema di conservazione;
- Monitora gli SLA relativi alla manutenzione del sistema di conservazione;
- Si interfaccia con il produttore in relazione 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;
- Gestisce lo sviluppo degli applicativi software connessi al servizio di conservazione.

Di seguito vengono riportati i nominativi attualmente in carica.

Ruolo	**Nominativo in carica**
Responsabile del Servizio di Conservazione (RSC)	Auletta Ferdinando
Responsabile della sicurezza dei sistemi per la conservazione (RQS)	Artioli Silvano
Responsabile funzione archivistica di conservazione (RFA)	Auletta Ferdinando
Responsabile del Trattamento dei Dati personali (DIR)	Auletta Giovanni

Ruolo	Nominativo in carica
Responsabile sistemi informatici per la conservazione (RSI)	Recchia Mauro
Responsabile sviluppo e manutenzione del sistema (RSM)	Zanella Stefano

Torna al sommario

6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 Organigramma

Le strutture organizzative coinvolte nel servizio di conservazione sono illustrate nell'organigramma (ALL01) allegato.

6.2 Strutture organizzative

Di seguito si descrivono le strutture organizzative che intervengono nelle principali funzioni che riguardano il servizio di conservazione, in particolare si specificano, per ogni attività svolta dalle strutture, le relative figure di riferimento.

6.2.1 Attività proprie di ciascun contratto di servizio di conservazione

Attività	Figura di riferimento	Strutture organizzative interagenti
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	RGC	Gestione commerciale, comunicazione e marketing Gestione clienti e assistenza Gestione della funzione archivistica Servizi di gestione dell'archivio informatico e conservazione
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione clienti e assistenza
Preparazione e gestione del pacchetto di archiviazione	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione della funzione archivistica
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	RSC	Servizi di gestione dell'archivio informatico e conservazione Gestione clienti e assistenza Gestione sistemi informativi

Attività	Figura di riferimento	Strutture organizzative interagenti
Scarto dei pacchetti di archiviazione	RSC	Gestione della funzione archivistica Servizi di gestione dell'archivio informatico e conservazione
Chiusura del servizio di conservazione (al termine di un contratto)	RSC	Gestione clienti e assistenza Gestione commerciale, comunicazione e marketing Gestione della funzione archivistica Direzione amministrativa e contabile

6.2.2 Attività proprie di gestione dei sistemi informativi

Attività	Figura di riferimento	Strutture organizzative interagenti
Conduzione e manutenzione del sistema di conservazione	RSM	Gestione sviluppo software e manutenzione Gestione sistemi informativi Gestione della qualità e della sicurezza delle informazioni e dei sistemi
Monitoraggio del sistema di conservazione	RQS	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Servizi di gestione dell'archivio informatico e conservazione Gestione della funzione archivistica Presidenza (Responsabile del trattamento dei dati personali)

Attività	Figura di riferimento	Strutture organizzative interagenti
Change management	RFA	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Gestione della funzione archivistica Gestione clienti e assistenza Gestione commerciale, comunicazione e marketing Direzione tecnica
Verifica periodica di conformità a normativa e standard di riferimento	RQS	Gestione della qualità e della sicurezza delle informazioni e dei sistemi Gestione della funzione archivistica Direzione tecnica Presidenza (Responsabile del trattamento dei dati personali)

Torna al sommario

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE

Nella presente sezione si descrivono le tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione.

7.1 Oggetti conservati

Il SdC acquisisce pacchetti informativi trasformandoli in PdA e conservandoli in linea con i requisiti della normativa.

Un pacchetto informativo può contenere qualsiasi tipologia di documento informatico, nonché una o più aggregazioni documentali informatiche. Di seguito si descrivono le principali aggregazioni gestite:

Tipologia documentale	Descrizione
Fatture elettroniche (in formato XML FatturaPA)	Fatture commerciali emesse e/o ricevute dalle Amministrazioni Pubbliche in formato FatturaPA.
Fatture clienti	Fatture commerciali attive (elettroniche ed analogiche) emesse da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Fatture fornitori	Fatture commerciali passive (elettroniche ed analogiche) ricevute da organizzazioni private e pubbliche fruitrici del servizio di conservazione.
Documenti di trasporto	Documenti emessi per giustificare il trasferimento di un materiale da cedente a cessionario attraverso il trasporto dello stesso, in base a quanto sancito dal Testo del D.P.R. 14 agosto 1996 n. 472. ("Regolamento di attuazione delle disposizioni contenute nell'art. 3, comma 147, lettera d), della legge 28 dicembre 1995, n. 549, relativamente alla soppressione dell'obbligo della bolla di accompagnamento delle merci viaggianti")
Libri contabili	Libri, registri, documenti e altre scritture contabili obbligatorie e/o richieste dalla natura e dalle dimensioni dell'impresa, quali (a titolo esemplificativo): libro giornale, libro inventari, piano dei conti, libro mastro, libro magazzino, registri iva, ecc....

Documenti di protocollo	Documenti afferenti al sistema di gestione del protocollo informatico nella Pubblica Amministrazione quali (a titolo esemplificativo): mail PEC, registro di protocollo.
Atti amministrativi	Documenti formati dalla Pubblica Amministrazione nella gestione ordinaria delle sua attività istituzionale, quali (a titolo esemplificativo): delibere di giunta, delibere di consiglio, determine, ordinanze, albo pretorio, contratti, ecc...
Mandati di pagamento e reversali informatici	Documenti di interscambio tra la Pubblica Amministrazione e l'Istituto Bancario gestore del Servizio di Tesoreria.

I metadati di ogni tipologia documentale sono definiti in modo parametrico attraverso il SdC per ogni singolo cliente e formalizzati nel Contratto di Servizio. Nella definizione dei metadati dei documenti aventi rilevanza fiscale si fa riferimento all'art. 3 del DMEF 17 giugno 2014.

Il set di metadati minimi associati ai documenti informatici è allineato con quanto definito dall'allegato 5 del DPCM.

7.2 Formati

Il SdC, in linea con quanto indicato nell'allegato 2 del DPCM, gestisce i documenti informatici mediante diversi formati di file tra i quali si indicano, di seguito, i principali:

Formato del file	Visualizzatore	Standard	Versione del formato	Sistema Operativo
PDF - PDF/A	Adobe Reader	ISO 32000-1 ISO 19005-1:2005 ISO 19005-1:2011	1.4 -1.7	Qualsiasi
XML	Browser internet o text editor	ISO 26300:2006	ND	Qualsiasi
EML	MS Outlook o Mozilla Thunderbird	RFC 5322	ND	Qualsiasi
Documento con firma digitale	Dike, ArubaSign.	CADES, XADES, PADES	ND	Qualsiasi

7.3 Pacchetto di versamento

Il PdV è il pacchetto informativo, inviato dal produttore al SdC, il cui formato e contenuto sono concordati con il soggetto produttore.

I PdV contengono insiemi informativi da sottoporre a conservazione e sono generati tramite:

- procedura automatizzata messa a disposizione dalla piattaforma JDoc;
- appositi web-services che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- altri software sviluppati da partner di Enerj

Il PdV, eventualmente integrato da ulteriori informazioni concordate con il cliente, viene trasferito dal produttore al soggetto conservatore Enerj tramite una apposita procedura informatica automatizzata che consente l'identificazione certa del soggetto, dell'ente o dell'amministrazione che ha formato e trasmesso il documento.

Le informazioni relative alle diverse tipologie di pacchetti di versamento trattati, sono descritte nel Contratto di Servizio e sono concordate specificamente con ciascun soggetto produttore.

A titolo di esempio riportiamo, di seguito, un tracciato XML di un PdV.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" p3:version="-" p3:url=""
p3:schemaLocation="-" xmlns:p3="http://www.uni.com/U3011/sincro/"
xmlns="http://www.uni.com/U3011/sincro/">
<p3:SelfDescription>
    <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
    <p3:CreatingApplication>
      <p3:Name>JDoc</p3:Name>
      <p3:Version>6.0.0.0</p3:Version>
      <p3:Producer>enerj s.r.l.</p3:Producer>
    </p3:CreatingApplication>
  </p3:SelfDescription>
  <p3:VdC>
    <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
  </p3:VdC>
  <p3:FileGroup>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
      <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b410a</p3:Has
h>
      <p3:MoreInfo p3:XMLScheme="">
```

```
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-
b87f413b29d4</p3:ID>
               <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-
b87f413b29d4.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
      <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-
f85fc1b5e114</p3:ID>
               <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-
f85fc1b5e114.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
          <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
      <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
               <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-
5cda0b64e0a7</p3:ID>
               <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-
5cda0b64e0a7.xml</p3:Path>
               <p3:Hash p3:function="SHA-
256">b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
  </p3:FileGroup>
  <p3:Process>
    <p3:Agent p3:type="organization" p3:role="OtherRole"
p3:otherRole="Producer">
      <p3:AgentName>
        <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
```

```
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
    </p3:Agent>
    <p3:TimeReference>
      <p3:AttachedTimeStamp>2015-06-
03T14:04:01.444+02:00</p3:AttachedTimeStamp>
    </p3:TimeReference>
  </p3:Process>
</IdC>
```

7.4 Pacchetto di archiviazione

Il PdA viene formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali).

Le informazioni più rilevanti che il sistema di conservazione gestisce, in relazione ad ogni PdA prodotto, sono:

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale , Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'IPdA generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdA (Produttore, nome e versione);
- Informazioni sui PdA contenuti nell'indice;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- Informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso;

La norma definisce il contenuto del PdA in base alla tassonomia specificamente determinata dal DPCM e schematizzata come segue:

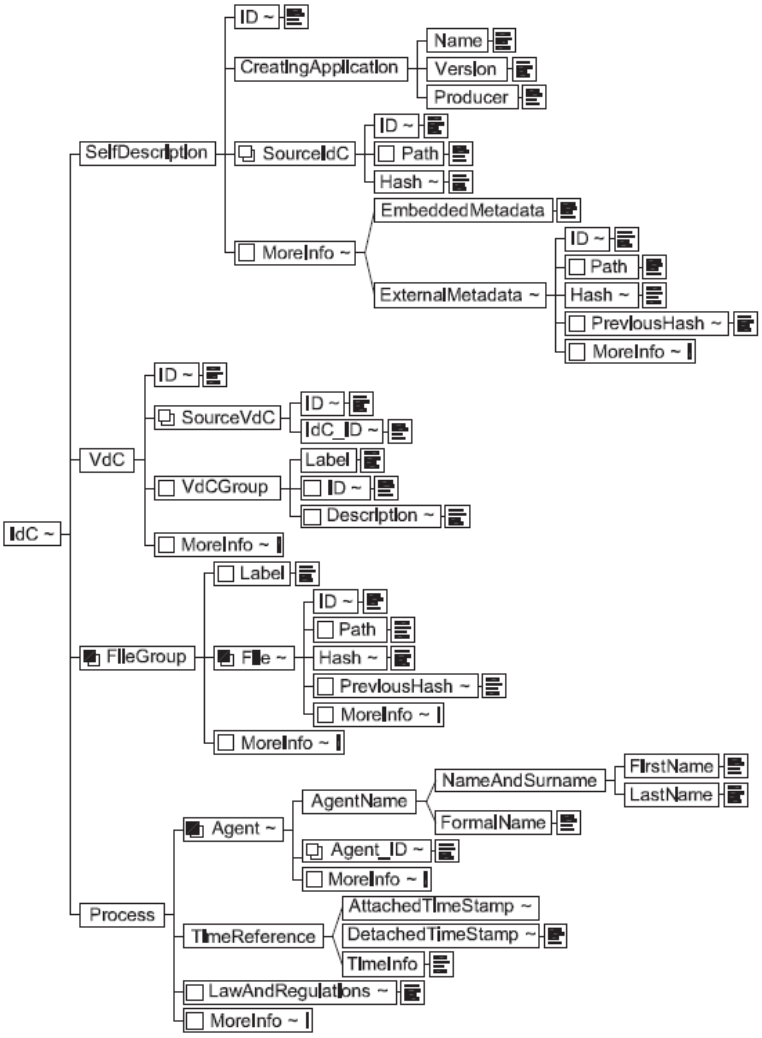


Figura 1 - Rappresentazione UML del contenuto del PdA

A titolo esemplificativo riportiamo, di seguito, un tracciato XML di un PdA.

```
<?xml version="1.0" encoding="utf-8"?>
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" p3:version="-" p3:url=""
p3:schemaLocation="-" xmlns:p3="http://www.uni.com/U3011/sincro/"
xmlns="http://www.uni.com/U3011/sincro/">
  <p3:SelfDescription>
    <p3:ID p3:scheme="local">d170cb44-62b3-4084-87b2-d63642202588</p3:ID>
    <p3:CreatingApplication>
      <p3:Name>JDoc</p3:Name>
      <p3:Version>6.0.0.0</p3:Version>
      <p3:Producer>enerj s.r.l.</p3:Producer>
    </p3:CreatingApplication>
  </p3:SelfDescription>
  <p3:VdC>
```

```
    <p3:ID p3:scheme="local">36cfc425-d08e-4fc9-8bdc-5b3811c3de71</p3:ID>
  </p3:VdC>
  <p3:FileGroup>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">210b033f-e467-4289-8055-77f94a7c29a2</p3:ID>
      <p3:Path>./File/210b033f-e467-4289-8055-77f94a7c29a2.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">4826a0a7634c2b96b4cfb1d6e1fc1aef21394791f46338d16d356aa1a9b2410a</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">0d3c702d-9e25-4b87-a7ce-
b87f413b29d4</p3:ID>
            <p3:Path>./Meta/0d3c702d-9e25-4b87-a7ce-
b87f413b29d4.xml</p3:Path>
            <p3:Hash p3:function="SHA-
256">48b849509eb8994cee42a233bf19063ecfec6a88b11c91517ff8d86663ba3809</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
    <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">

      <p3:ID p3:scheme="local">d001c351-b862-440e-a5dc-490574244c98</p3:ID>
      <p3:Path>./File/d001c351-b862-440e-a5dc-490574244c98.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">69eb58664b83234a804d231a117629673bbeb0b3f767e9b03897d1459e7fc758</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">a477ebf5-df4f-4df9-adbc-
f85fc1b5e114</p3:ID>
            <p3:Path>./Meta/a477ebf5-df4f-4df9-adbc-
f85fc1b5e114.xml</p3:Path>
            <p3:Hash p3:function="SHA-
256">e3ee0413622956a9ccdeb9ef3e8edfc90808a4d2cae1d09e4a4de66f503c0a7d</p3:Ha
sh>
         </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
          <p3:File p3:encoding="binary" p3:extension="p7m"
p3:format="application/p7m">
      <p3:ID p3:scheme="local">a50e8671-fa15-47b6-b1d1-97a34a8a8316</p3:ID>
      <p3:Path>./File/a50e8671-fa15-47b6-b1d1-97a34a8a8316.p7m</p3:Path>
      <p3:Hash p3:function="SHA-
256">c2b1e05b9f7999fb00060cfe5adb371ec8844b65b923253834fbb040418f4203</p3:Ha
sh>
      <p3:MoreInfo p3:XMLScheme="">
         <p3:ExternalMetadata p3:format="application/xml"
p3:encoding="binary">
            <p3:ID p3:scheme="local">1b32e85b-58e2-432d-bd06-
5cda0b64e0a7</p3:ID>
            <p3:Path>./Meta/1b32e85b-58e2-432d-bd06-
5cda0b64e0a7.xml</p3:Path>
```

```
            <p3:Hash p3:function="SHA-
256">b16495efe3ad36832146bd18179d036d6129830c2988e78367e035c50ed26863</p3:Ha
sh>
       </p3:ExternalMetadata>
      </p3:MoreInfo>
    </p3:File>
  </p3:FileGroup>
  <p3:Process>
    <p3:Agent p3:type="organization" p3:role="PreservationManager">
      <p3:AgentName>
        <p3:FormalName>enerj s.r.l.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
    </p3:Agent>
    <p3:Agent p3:type="organization" p3:role="Delegate">
      <p3:AgentName>
        <p3:FormalName>enerj s.r.l.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">03466010232</p3:Agent_ID>
    </p3:Agent>
    <p3:Agent p3:type="organization" p3:role="OtherRole"
p3:otherRole="Producer">
      <p3:AgentName>
        <p3:FormalName>ESEMPIO S.p.A.</p3:FormalName>
      </p3:AgentName>
      <p3:Agent_ID
p3:scheme="VATRegistrationNumber">12345678910</p3:Agent_ID>
    </p3:Agent>
    <p3:TimeReference>
      <p3:AttachedTimeStamp>2015-06-
03T14:04:01.444+02:00</p3:AttachedTimeStamp>
    </p3:TimeReference>
  </p3:Process>
</IdC>
```

Alla struttura del PdA citata in precedenza sono collegate ulteriori strutture, in formato XML, contenenti i metadati del documento, tramite i diversi elementi “MoreInfo” previsti nello standard SInCRO. Di seguito riportiamo un esempio di una struttura implementata per la conservazione delle fatture elettroniche alla PA.

```
<?xml version="1.0" encoding="utf-8"?>
<documento IDDocumento="210b033f-e467-4289-8055-77f94a7c29a2">
  <datachiusura>2015-01-13</datachiusura>
  <oggettodocumento>esempio</oggettodocumento>
  <soggettoproduttore>
    <nome>Mario</nome>
    <cognome>Rossi</cognome>
    <codicefiscale>esempioesempioes</codicefiscale>
  </soggettoproduttore>
  <destinatario>
    <nome>Nome responsabile PA destinataria</nome>
    <cognome>Cognome responsabile PA destinataria</cognome>
    <codicefiscale>esempioesempioes</codicefiscale>
  </destinatario>
    <ProgressivoInvio>0000069284</ProgressivoInvio>
```

```
        <NomeFile>IT03466010232_00I1U.xml</NomeFile>
        <DatiGeneraliDocumento>
         <TipoDocumento>TD01</TipoDocumento>
         <Data>2015-09-02</Data>
         <Numero>2015110727</Numero>
    </DatiGeneraliDocumento>
        <CessionarioCommittente>
         <CodiceFiscale>xxxxxx00988</CodiceFiscale>
         <PartitaIVA>ITxxxxxx00988</PartitaIVA>
         <Denominazione>Nome Pubblica Amministrazione</Denominazione>
        </CessionarioCommittente>
</documento>
```

7.5 Pacchetto di distribuzione

La richiesta di esibizione da parte del Cliente dei documenti conservati viene soddisfatta attraverso la generazione di un PdD.

Il PdD viene formato secondo le regole tecniche definite nello Standard SInCRO.

Il PdD ha una struttura analoga a quella del PdA ed include i riferimenti univoci ai PdA che sono stati estratti dal SdC.

Il PdD è corredato da ulteriori informazioni quali:

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale , Codice Fiscale, Partita IVA, ...);
- Identificativo univoco dell'PdD generato automaticamente dal SdC;
- Informazioni sull'applicazione che ha generato il PdD (Produttore, nome e versione);
- Informazioni sui PdA contenuti nel PdD;
- Informazioni sui documenti (ID, Impronta di hash, formato, percorso);
- le immagini in formato originale estratte dai PdA;
- Informazioni relative al processo di conservazione (elementi identificativi del RSC);
- Informazioni relative alla data di produzione del pacchetto stesso (marca temporale);
- Informazioni relative alla firma digitale.
- eventuali informazioni relative ai metadati dei documenti previste negli accordi specifici del Contratto del Servizio;
- Informazioni necessarie per il controllo ed il log delle operazioni relative al pacchetto stesso;

Le richieste di esibizione dei PdD sono accettate solamente se provenienti dai

soggetti autorizzati dal Cliente.

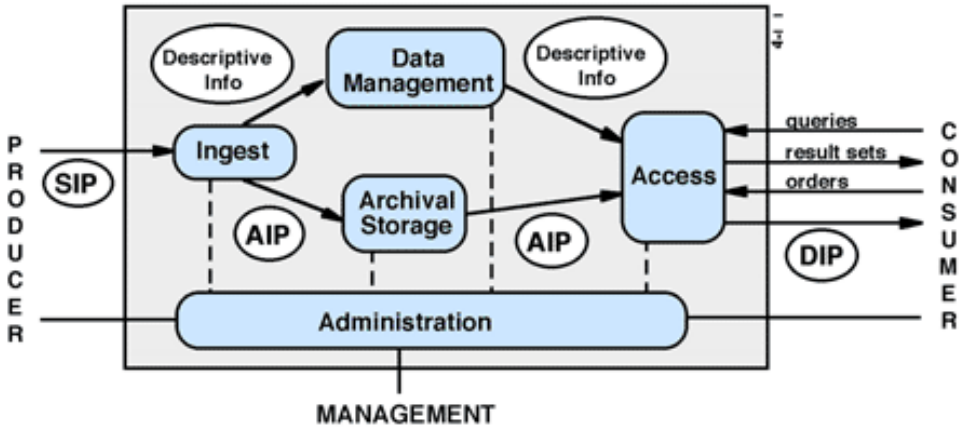
Torna al sommario

8 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione si esegue sulla base delle modalità previste dall' art. 9 del DPCM, e delle specifiche contenute nella Procedura di gestione della Conservazione Digitale (PCD) afferente al ISMS e dalle peculiarità presenti nei Contratti di Servizio.

Il processo di conservazione è realizzato sulla base del modello funzionale OAIS (Open Archival Information System) normato dallo standard ISO 14721:2003 a cui si è fatto riferimento. Il modello OAIS ha introdotto nella gestione degli archivi informatici i concetti fondamentali relativi alle modalità di transazione dei pacchetti informativi (PdV, PdA, PdD) contemplati e descritti nel presente manuale.

Nello schema che segue si evidenziano le modalità che regolano il flusso informativo di pacchetti informativi generati da un soggetto produttore (nello schema: *Producer*) sotto forma di PdV (nello schema: *SIP*) ad un SdC (nello schema: *management*) che lo trasforma in PdA (nello schema: *AIP*) e ne cura la conservazione ed il mantenimento nel tempo. Il SdC provvede anche a mettere a disposizione del soggetto fruitore (nello schema: *consumer*) il contenuto del PdA tramite opportune modalità di accesso (nello schema: *Access*) e sotto forma di PdD (nello schema *DIP*)



Schema 1 **- Modello funzionale OAIS**

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

Le principali modalità di trasmissione del pacchetto di versamento sono:

- procedura automatizzata messa a disposizione dalla piattaforma JDoc;
- appositi web-services che consentono l'inserimento nel SdC;
- trasmissione telematica tramite canale sicuro;
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- altri software sviluppati da partner di Enerj

E' prevista anche l'integrazione con il servizio di fatturazione elettronica alla pubblica amministrazione di Enerj, qualora il fruitore sia anche utente di tale servizio. Tali documenti informatici da conservare sono già presenti nel sistema informativo Enerj, vengono pertanto generati dei pacchetti di versamento suddivisi per singolo cliente e periodo di competenza ed inviati al SdC.

Come dettagliato nel Manuale della Sicurezza del Sistema Informativo (MSI), tutti i canali FTP/HTTP di comunicazione instaurati con i Clienti sono cifrati per la protezione dei dati oggetto di transazione con il cliente. Il ripristino delle funzionalità del sistema in caso di corruzione o perdita dei dati è implementato e descritto nel Piano di Continuità Operativa del Business e Disaster Recovery (PCO). Per l'intero processo di acquisizione dei PdV, il SdC produce i log di sistema necessari alla tracciatura delle attività e delle operazioni svolte, così come descritto nella sezione dedicata al *Log Management* del Manuale della Sicurezza del Sistema Informativo (MSI).

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

Il SdC, opera uno o più controlli sul contenuto del pacchetto di versamento ricevuto dal fruitore del servizio, per determinare la correttezza delle caratteristiche formali e dei documenti informatici e/o delle aggregazioni documentali informatiche afferenti al pacchetto stesso. Nelle sezioni successive, detti controlli sono ulteriormente approfonditi dal punto di vista procedurale.

Di seguito sono riportati alcuni tra gli automatismi più consueti implementati per il controllo e la verifica delle caratteristiche dei documenti relativi alle diverse aggregazioni documentali informatiche appartenenti all'archivio informatico del fruitore.

- **Identificazione certa del Produttore:** il sistema verifica l'identità del Produttore attraverso diverse modalita' in relazione alla disponibilità tecnica del cliente.
  Vengono verificate: le credenziali fornite ad esso, lo specifico canale sicuro di comunicazione messo a disposizione, il filtro sugli indirizzi internet, la codifica specifica del codice cliente attribuita ai dati che il Produttore invia in fase di Versamento.
- **Controlli di corretto trasferimento via rete internet:** dove previsto dalla parametrizzazione del SdC il trasferimento via rete internet il SdC verificata l'integrità dei documenti contenuti nei pacchetti di versamento, attraverso il confronto delle impronte di hash.
- **Controlli di formato:** il SdC verifica se i formati inviati dal produttore sono censiti e contrattualizzati nel periodo di competenza del servizio. I formati vengono verificati attraverso librerie e procedure software automatiche che effettuano un log completo delle operazioni effettuate. Per alcuni formati, dove possibile, viene anche controllata la correttezza dei dati.
- **Automatismi per la verifica della consistenza dei documenti presenti nel flusso:** il sistema verifica la presenza di tutti i dati e/o dei metadati dei documenti informatici che compongono l'archivio da sottoporre al procedimento di conservazione. L'utente del servizio ha a disposizione un insieme completo di informazioni e di riscontri utilizzabili in relazione ai dati di origine del flusso (sistema gestionali contabile, ERP, CRM, ecc…).
- **Verifica dell'omogeneità dei documenti:** dove previsto viene verificata la coerenza nella progressione numerica e temporale dei protocolli nonché la progressività dei protocolli rispetto all'ultima operazione di conservazione.
- **Verifica dei metadati minimi obbligatori:** il sistema verifica la presenza dei metadati minimi obbligatori per ogni specifici per ogni cliente e per ogni tipologia documentale, così come definito negli accordi specifici del Contratto di Servizio.

Ulteriori automatismi possono essere implementati su richiesta dell'organizzazione fruitrice ed in base alle esigenze delle stessa e sulla base degli accordi specifici del Contratto di Servizio.

I controlli e le verifiche implementabili sono descritti nella procedura di Gestione della Conservazione Digitale (PCD).

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

L'accettazione del PdV da luogo alla generazione automatica del rapporto di versamento relativo ad uno o più pacchetti di versamento.

Il rapporto di versamento è strutturato secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettere d) ed e) del DPCM ed è comprensivo dell'elenco dei pacchetti di versamento accettati.

Il SdC attribuisce un identificatore univoco a ciascun rapporto di versamento generato e la riferisce temporalmente (con riferimento al Tempo universale coordinato - UTC -).

Il rapporto di versamento include, a titolo non esaustivo, le seguenti informazioni:

- dati del Produttore
- dati dell'utente richiedente il versamento
- tipologie dei documenti
- formati dei documenti
- impronte dei documenti
- esiti dei controlli
- metadati del PdV
- riferimenti temporali

L'accettazione del PdV è subordinata ai controlli previsti dal SdC per il Cliente, le tipologie di documento oggetto di conservazione, i formati e quanto previsto al paragrafo 8.2. Tali controlli sono parametrizzati nel SdC stesso e sono parte integrante del Contratto di Servizio.

Nel rapporto di versamento sono elaborate e specificate le impronte, una o più, calcolate sull'intero contenuto del pacchetto di versamento, mediante procedura automatizzata.

Il SdC inoltra i rapporti di versamento al Produttore secondo diverse modalità in base a quanto espresso nel Contratto di Servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

L' interfaccia web consente al Produttore di monitorare lo stato di tutti i PdV inviati al SdC e pertanto gestire anche eventuali errori risultanti dai controlli (vedasi paragrafo 8.4).

Tutti le informazioni inerenti alle operazioni eseguite dagli utenti e dai processi informatici relative ai PdV accettati dal Produttore al SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola

operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

8.4 Rifiuto dei PdV e modalità di comunicazione delle anomalie

In caso di esito negativo dei controlli e delle verifiche applicati sul PdV, il SdC genera una comunicazione di rifiuto, che viene riferita temporalmente e trasmessa al produttore.

Nella comunicazione sono indicate le anomalie presenti nel PdV che ne determinano il rifiuto, quali (a titolo esemplificativo e non esaustivo):

- Presenza di documenti informatici non integri o corrotti in fase di trasmissione;
- Incongruenze relative a errata numerazione di protocollo;
- Incongruenze relative alla consecutività temporale dei documenti informatici;
- Assenza dal PdV dei dati essenziali specificati nel Contratto di Servizio;
- Anomalie relative alla sicurezza dei dati.

La comunicazione viene inoltrata al produttore secondo diverse modalità in base a quanto espresso nel Contratto di Servizio. Le modalità utilizzate sono:

- trasmissione a mezzo mail,
- trasmissione a mezzo PEC,
- messa a disposizione tramite interfaccia web.

Tutti le informazioni inerenti le operazioni eseguite dagli utenti e dai processi informatici relative ai PdV rifiutati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente, processo informatico, codice cliente, tipo di operazione, metadati completi, identificativo univoco del PdV, informazioni di sicurezza.

8.5 Preparazione e gestione del PdA

Mediante apposite procedure software del SdC, i PdV, opportunamente verificati e validati come descritto nelle sezioni precedenti, vengono trasformati in PdA e corredati delle ulteriori caratteristiche necessarie a soddisfare i requisiti previsti dalla normativa.

Qualora si rendano necessari interventi manuali da parte degli operatori del SdC di rettifica, integrazione di dati e metadati nei PdA, tali operazioni sono tracciate su appositi log che includono, a titolo non esaustivo, le seguenti informazioni: data e

ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi precedenti e successivi all'operazione, informazioni di sicurezza.

Le modalità di gestione degli interventi manuali da parte degli operatori del SdC sono documentati nella procedura PCD e prevedono l'utilizzo di apposita modulistica.

I PdA sono sottoscritti dal RSC e, ad essi, sono associate le relative marche temporali.

I PdA, così sottoposti al processo di conservazione digitale, sono custoditi, per i tempi previsti dalla normativa e dai Contratti di Servizio, nell'archivio informatico facente parte del SdC. Il sistema è implementato e sviluppato allo scopo di garantire e mantenere la disponibilità, la fruibilità, l'immodificabilità e l'autenticità dei documenti informatici in esso contenuti.

Le ulteriori informazioni peculiari contenute nel PdA, eventualmente concordate con il soggetto Produttore, sono definite nei Contratti di Servizio.

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

Il processo di preparazione del PdD è attivato dalla ricezione di una richiesta di esibizione da parte dell'utente. Il SdC si occupa di verificare che il profilo dell'utente che accede abbia le necessarie autorizzazioni per effettuare l'estrazione.

L'utente, guidato dal sistema, opera la selezione dei documenti informatici da estrarre. Il sistema, sulla base della selezione, compone la richiesta di esibizione che specifica quali documenti informatici comporranno il PdD.

Il sistema provvede quindi a confezionare il PdD contenente i documenti informatici oggetto della selezione ed i relativi IPdA.

I IPdA contengono le impronte dei documenti richiesti per consentire al fruitore la verifica autonoma e completa delle caratteristiche che determinano la corretta conservazione dei documenti.

Nel caso in cui si preveda l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, si fa riferimento a quanto previsto nel Contratto di Servizio.

I supporti fisici non presentano riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.

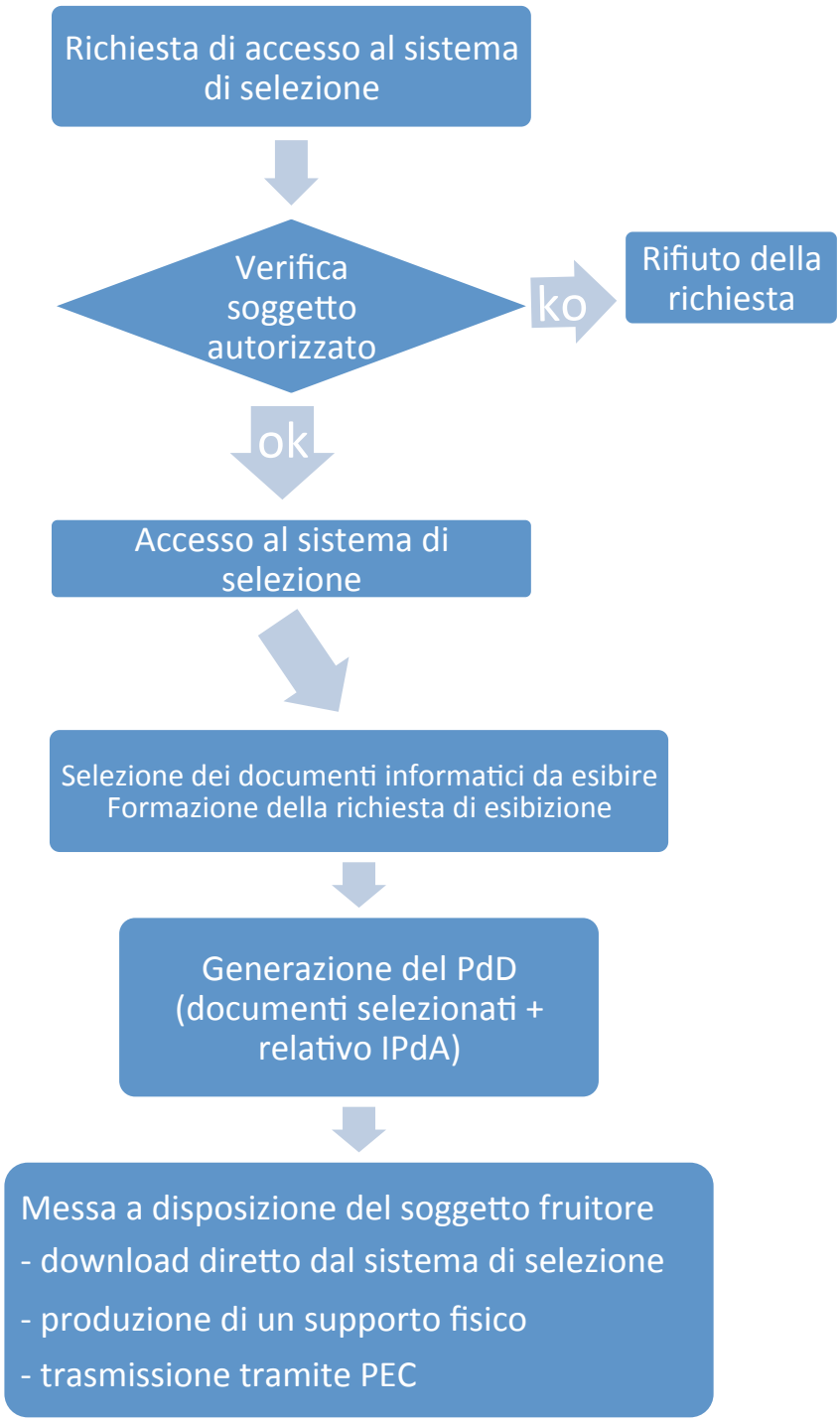
I supporti fisici sono trasportati a cura e responsabilità di personale Enerj o

incaricato da Enerj sulla base di specifici requisiti definiti dal RdC nella procedura PCD.

I dati richiesti sono crittografati con il certificato del destinatario prima della loro spedizione/trasmissione allo stesso.

Nel caso in cui i contratti di servizio implichino la consegna dei PdD via email, viene utilizzata la posta certificata per permettere di tracciare l'intera trasmissione e sono conservate le sole ricevute di invio e consegna.

Tutti le informazioni relative ai PdD richiesti, generati, esportati dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, metadati completi, informazioni di sicurezza.



Schema 2 - Processo di preparazione e gestione del PdD

8.7 Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale nei casi previsti

Il SdC di Enerj prevede specifiche procedure per la generazione e produzione di duplicati informatici e copie informatiche sulla base delle modalità definite dall'art. 22 del CAD.

8.7.1 Produzione di duplicati informatici

Il procedimento di produzione di duplicati informatici consente di ottenere dal SdC i duplicati informatici aventi il medesimo valore giuridico, ad ogni effetto di legge, dei documenti informatici dai quali sono tratti in conformità con le regole tecniche vigenti. I duplicati di documenti informatici hanno il medesimo contenuto e la medesima rappresentazione informatica degli originali dai quali sono tratti.

Il procedimento di produzione di duplicati si attiva automaticamente:

- ogni volta che il soggetto fruitore accede al sistema di selezione per ottenere uno o più PdD contenenti i documenti informatici di interesse;
- in occasione dei backup e delle repliche perpetrate sui PdA allo scopo di garantirne la permanenza dei requisiti essenziali di fruibilità e verificabilità;

8.7.2 Produzione di copie informatiche/analogiche ed estratti di documenti informatici

Il procedimento di produzione di copie informatiche ed estratti di documenti informatici consente di ottenere documenti aventi la stessa efficacia probatoria dei documenti informatici dai quali sono tratte. Le copie e gli estratti di documenti informatici hanno il medesimo contenuto degli originali da cui sono tratte ma diversa rappresentazione informatica.

Il procedimento di generazione di copie informatiche ed estratti viene di norma attivato:

- ogni qual volta sia richiesto dai soggetti fruitori e specificamente previsto dal Contratto di Servizio in relazione agli accordi;
- quando, per motivi legati all'evoluzione tecnologica e/o normativa, la rappresentazione informatica dei documenti originali non sia più fruibile dai sistemi di consultazione utilizzati e sia necessario adeguarne il formato.

Il procedimento di generazione di copie informatiche prevede la possibilità di richiedere l'intervento di un pubblico ufficiale allo scopo di attestare la conformità di queste con gli originali.

8.7.3 Produzione di copie informatiche di documenti analogici

Il procedimento di produzione di copie informatiche di documenti analogici consente di generare documenti informatici aventi la stessa efficacia probatoria degli originali analogici da cui sono tratti. Le modalità tecniche di ottenimento delle suddette copie sono costituite da procedure di digitalizzazione che avvengono tramite appositi dispositivi scanner o mediante procedure di rielaborazione delle informazioni che costituiscono i contenuti dei documenti analogici originali.

Il SdC di Enerj prevede espressamente la possibilità di conservare dette fattispecie documentali e le procedure di digitalizzazione utilizzate sono ampiamente descritte nelle procedure di Gestione della Digitalizzazione Interna (PDI) e Gestione della Digitalizzazione Esterna (PDO), afferenti al ISMS.

Le procedure di elaborazione di un documento analogico in informatico, menzionate al paragrafo precedente, sono invece gestite da un apposito modulo software del SdC.

Il procedimento di produzione di copie informatiche di documenti analogici viene attivato quando il soggetto fruitore conferisce al SdC documenti espressi su supporti analogici.

8.8 Scarto dei pacchetti di archiviazione

Il SdC di Enerj effettua lo scarto dei pacchetti di archiviazione sulla base di quanto espresso nei Contratti di Servizio. L'eliminazione dei pacchetti informativi scartati e delle eventuali relative informazioni a corredo viene eseguita tramite una procedura di distruzione sicura dei dati, in linea con la vigente normativa sulla sicurezza dei dati e privacy. Detta funzione è approfondita nella Piano della Sicurezza del Sistema di Conservazione (PDS) e nella Procedura di Conservazione Digitale (PCD).

Nel caso di archivi pubblici o privati di particolare interesse culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo. La gestione della richiesta di autorizzazione è a carico dell' Ente pubblico Produttore.

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

Enerj, al fine di garantire l'interoperabilità del proprio sistema di conservazione e la trasferibilità di archivi informatici ad altri eventuali soggetti conservatori ha predisposto le seguenti misure:

- Adozione conformemente a quanto determinato dallo standard SInCRO, di tracciati XML omogenei relativi ai PdD e PdA.
- Generazione di tracciati XML (conformi allo standard SInCRO) privi di informazioni non standardizzate e/o arbitrariamente definite da Enerj e/o ridondanti, salvo il caso in cui la presenza di esse sia espressamente richiesta dal fruitore del servizio e palesata nelle specificità contrattuali;
- Mantenimento, per i PdD, della medesima struttura di dati espressa dal DPCM per la configurazione dei PdA (vedasi paragrafi 7.4 e 7.5);
- Mantenimento di identità tra Indice IPdA del PdA ed il medesimo presente nel PdD;
- Gestione dei metadati dei documenti informatici esterna al PdA tramite la corretta valorizzazione della sezione <MoreInfo>.

Il SdC di Enerj è in grado di accettare il versamento di PdD prodotti da altri sistemi di conservazione se in formato standard SInCRO. Eventuali altri formati dovranno essere sottoposti ad analisi e valutazione tecnica prima dell'ingresso nel SdC allo scopo di programmare e svolgere le opportune attività volte all'adeguamento ai formati standard.

In caso di conclusione del Contratto di Servizio, Enerj si impegna a produrre i PdD, coincidenti con i PdA conservati per il fruitore del servizio, tramite i canali e nelle modalità definite negli specifici accordi contrattuali e previa sottoscrizione dei relativi verbali di consegna. Ove previsto dalla natura dei dati riprodotti, sarà effettuata la cifratura degli stessi e la comunicazione, con canale distinto, della relativa chiave per la decifratura e la fruizione esclusiva da parte del titolare dell'archivio.

8.10 Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del servizio di conservazione.

Tutte le comunicazioni prodotte durante le transazioni di pacchetti informativi tra Enerj e il cliente (log applicativi, log di sistema, mail, mail pec) sono conservate mediante il SdC stesso.

Torna al sommario

9 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione, di seguito descritto nelle sue modalità di accesso, utilizzo e protezione è composto da:

- Componenti Logiche e Tecnologiche: Informazioni e dati, prodotti / servizi di software installati presso Enerj e presso la Clientela
- Componenti Fisiche: architettura informatica aziendale in tutti le sue componenti hardware, reti (aziendali ed esterne),
- Procedure di gestione e di evoluzione: procedure di produzione del software aziendale e della sua manutenzione, procedure di conservazione, procedure di Audit, Riesame della Direzione.

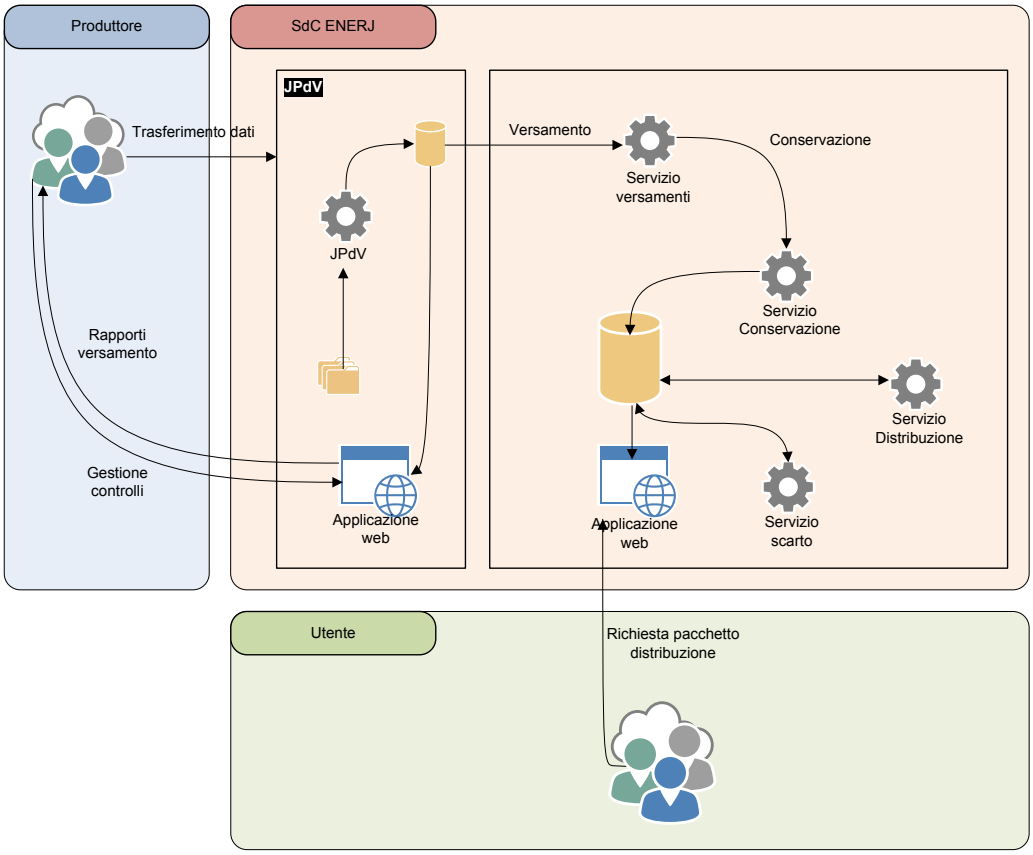
9.1 Componenti Logiche

Il SdC è composto dai seguenti oggetti:

- Produttore: effettuano il versamento dei nuovi PdV generati al SdC;
- JDoc che raccoglie e archivia i documenti inviati dal Produttore;
- JPdV: gestisce la generazione dei PdV effettuando tutte le azioni di monitoraggio e controllo previste nonché la generazione dei rapporti di versamento;
- Servizio Versamenti: prende in carico i PdV validati e gestisce l'inoltro al sistema di conservazione;
- Servizio Conservazione: gestisce la trasformazione da PdV a PdA utilizzando i servizi di firma digitale dei documenti implementati con tecnologia HSM presso una CA accreditata convenzionata con Enerj;
- Servizio Distribuzione: gestisce la ricerca dei documenti da parte degli Utenti abilitati e la generazione dei PdD è realizzata tramite JDoc;
- Servizio Scarto: gestisce lo scarto dei documenti in base a quanto previsto nelle specificità contrattuali;
- Utenti: fruiscono del SdC, accedendo alla piattaforma di front-end gestita tramite applicazioni web-based.

Tutte le funzionalità gestite dal sistema sono erogate in modalità di servizio. Un ulteriore elemento logico è costituito dall'ambiente di test e dall'ambiente di sviluppo che vengono gestiti in modo separato rispetto all'ambiente di produzione.

Lo schema riportato di seguito rappresenta l'architettura logico-funzionale del SdC.



Schema 3 - Schema delle componenti logiche del SdC

9.2 Componenti Tecnologiche

Enerj ha sviluppato una serie di moduli applicativi per l'implementazione del SdC tra cui si riportano i principali:

- **JDoc** Sistema di gestione dell'archivio informatico;
- **JCos** Sistema di gestione dei pacchetti informativi;
- **JSign** Modulo software di gestione della firma digitale e della marcatura temporale;
- **JView** Modulo software per la distribuzione e l'esibizione dei documenti informatici conservati.

L'elenco completo dei software implementati da Enerj e utilizzati nel SdC è contenuto negli inventari del software afferenti al ISMS (MCO04 - Inventario del software commerciale, MCO02 - Inventario del software proprietario).

9.3 Componenti Fisiche

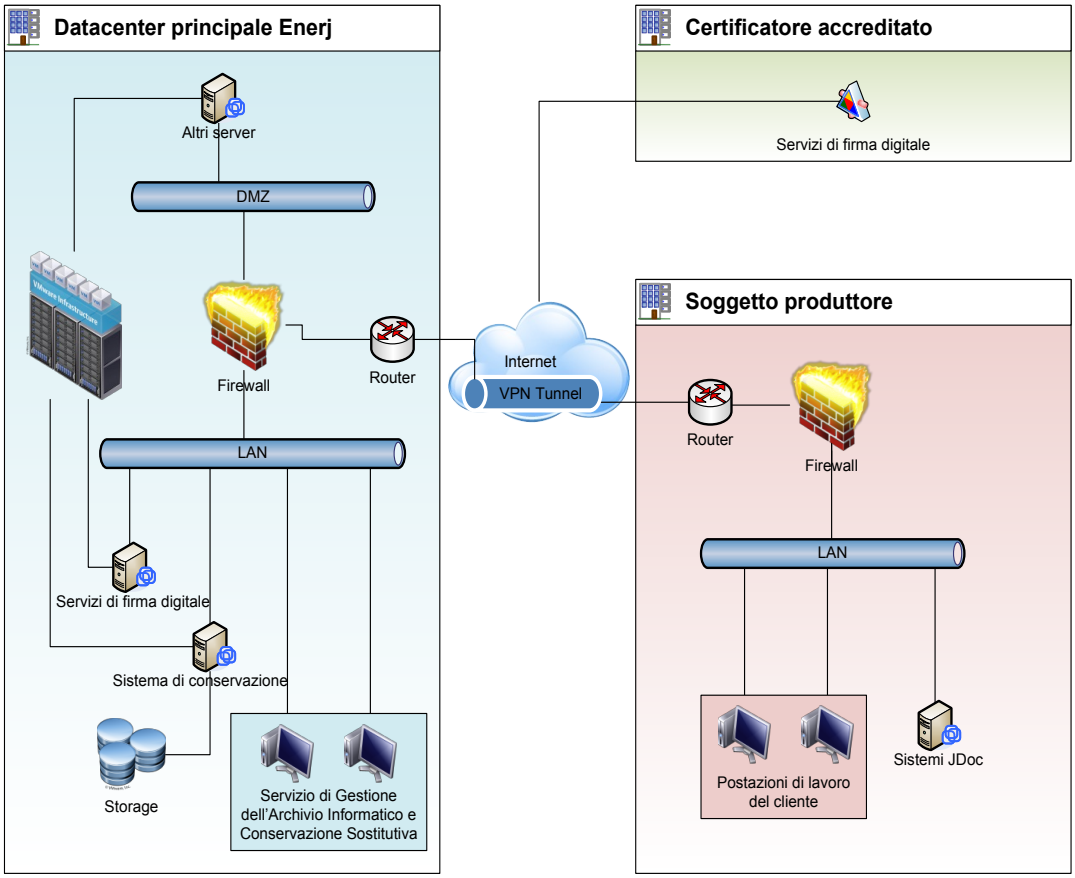
Le componenti fisiche utilizzate nell'infrastruttura di Enerj sono definite e descritte nel dettaglio nei seguenti documenti afferenti al ISMS:

- PDC - Procedura di Gestione del Datacenter
- MSI - Manuale della Sicurezza del Sistema Informativo
- MCO03 - Inventario delle attrezzature informatiche
- PCO - Piano della Continuità Operativa del business e Disaster Recovery
- PBK - Piano di Backup

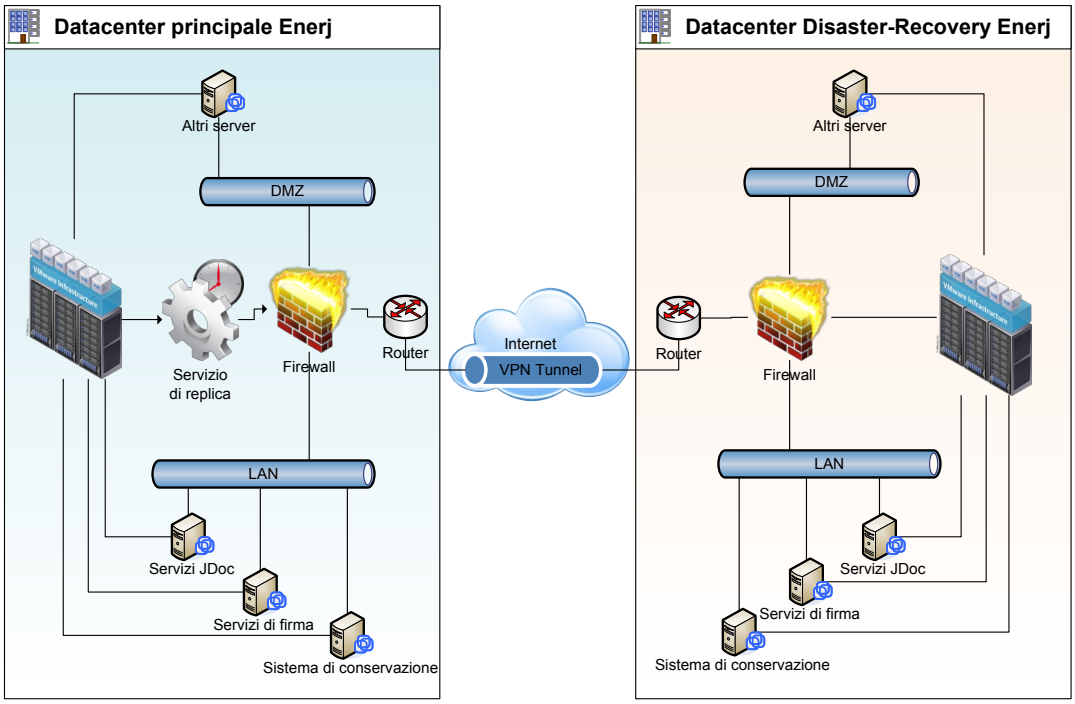
Il SdC si compone di due siti: uno primario situato presso la sede di Enerj ed uno secondario presso il sito di Disaster Recovery. I due datacenter sono connessi mediante una connessione sicura (VPN).

Gli HSM sono situati presso il datacenter del Certificatore accreditato convenzionato.

Di seguito si riporta lo schema dei siti di conservazione e delle connessioni tra i diversi siti con riferimento alle componenti fisiche e tecnologiche del SdC di Enerj.



Schema 4 - Schema e descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione.



Schema 5- Schema topologico che rappresenta del sistema di conservazione.

9.4 Procedure di gestione e di evoluzione

9.4.1 Conduzione e manutenzione del sistema di conservazione

In relazione alle componenti software di Enerj la procedura di Sviluppo e Manutenzione Software (PSS) descrive le modalità di aggiornamento degli applicativi software in relazione all'evoluzione normative, tecnologiche ed alle esigenze dei Clienti.

I componenti software implementati nel SdC sono sviluppati da una struttura aziendale dedicata.

9.4.2 Gestione e conservazione dei log

Il Sistema di "log management" di Enerj è descritto nel Manuale di Sicurezza del Sistema Informativo (MSI).

In particolare il sistema di "log management" del SdC traccia tutte le operazioni e le transazioni informatiche inerenti a:

- versamento di pacchetti informativi;
- trasformazioni di pacchetti informativi in PdA;

- conservazione dei PdA;
- comunicazioni ed esiti relativi ai pacchetti informativi scambiati con produttori e fruitori;
- gestione della firma digitale e della marcatura temporale;
- produzione e distribuzione dei PdD;
- controllo e verifica dei PdA;
- eventi di carattere sistemistico quali: accessi a risorse informatiche, incidenti di sicurezza, interruzione dell'operatività dei servizi, ecc...;
- accessi fisici ai locali.

9.4.3 Change management

L'evoluzione del SdC segue un percorso interno ad Enerj che prevede lo svolgimento di attività specifiche di presidio costante dell'allineamento del SdC all'evoluzione del panorama normativo vigente, nonché di ricerca e sviluppo, corredandole con la stesura e l'aggiornamento di appositi documenti, così come previsto nel ISMS, tra cui:

- riesame della direzione;
- moduli relativi allo sviluppo software;
- aggiornamento del presente manuale;
- aggiornamento del manuale della sicurezza del sistema informativo;
- aggiornamento del piano della sicurezza del SdC.

9.4.4 Verifica periodica di conformità a normativa e standard di riferimento

Enerj, nell'ambito della gestione del ISMS, ha previsto una specifica procedura di gestione degli audit (PGA) interni ed esterni, che assicura la persistenza della conformità del sistema alla normativa vigente ed agli standard di riferimento.

Torna al sommario

10 MONITORAGGIO E CONTROLLI

Enerj opera con l'obiettivo di mantenere, costantemente, il livello massimo di qualità e di sicurezza delle informazioni gestite tramite i propri servizi di conservazione digitale attraverso il monitoraggio delle applicazioni e delle infrastrutture. Si unisce al predetto obiettivo, la strategia di miglioramento continuo della qualità dei servizi, sostenendolo con investimenti di carattere tecnico e nella formazione delle risorse umane nel rispetto di quanto previsto dal DPCM art. 8, comma 2, lettera h.

10.1 Procedure di monitoraggio applicativo

Gli applicativi software del SdC producono i log delle transazioni dei pacchetti informativi (di cui alla sezione 9.4.2 del presente manuale), dall'elaborazione dei quali si traggono le informazioni necessarie per valutare nel tempo il mantenimento dell'efficacia del sistema, nonché dell'efficienza e della rispondenza dello stesso ai livelli di prestazioni previsti nei Contratti di Servizio.

La direzione, in sede di riesame, individua i conseguenti interventi sullo sviluppo e la manutenzione del software, sia gli investimenti necessari nell'infrastruttura tecnologica.

10.2 Procedure di monitoraggio infrastrutturale

L'infrastruttura tecnologica di Enerj è descritta nel Manuale della Sicurezza dei Sistemi Informativi (MSI) e relativi allegati. Il monitoraggio di tutti i dispositivi hardware quali apparati server, storage e networking, è effettuato tramite un'applicazione di terze parti. Inoltre Enerj è dotata di un contratto di Service Operation Center con un'azienda leader del settore.

Il monitoraggio mette a disposizione un cruscotto gestionale, interrogabile dall'amministratore del sistema, nonché dei report automatici.

10.3 Verifica dell'integrità degli archivi

Il SdC di Enerj prevede apposite procedure periodiche di controllo dell'integrità e leggibilità dei documenti conservati e della congruenza e completezza degli archivi. Le procedure sono descritte nel ISMS, in particolare:

- nel Manuale della Sicurezza dei Sistemi Informativi (MSI)
- nel Piano della Sicurezza del SdC (PDS)
- nella Procedura di Gestione degli Audit (PGA)
- nella Procedura di Analisi dei Rischi (PAR)
- nei verbali di verifica (moduli MCD)

In base al tipo di verifica la periodicità dei controlli può essere giornaliera, annuale e comunque non superiore ai cinque anni. Ulteriori procedure aggiuntive richieste dal soggetto Produttore possono essere descritte nel Contratto di Servizio.

Lo scopo dei sistemi di gestione della sicurezza implementati in Enerj è di evidenziare le eventuali vulnerabilità del sistema di tenuta degli archivi sottoposti a conservazione di Enerj, per potere migliorare costantemente il servizio dal punto di vista organizzativo e informatico, prevenendo possibili minacce e definendo un piano di intervento, in coerenza con il Sistema della Qualità interno e la procedura aziendale di miglioramento continuo.

I criteri di analisi e valutazione si basano sull'analisi oggettiva (condivisa dal management) delle vulnerabilità riscontrate (punti deboli, criticità), valutando l'effettiva probabilità di accadimento di un evento dannoso per gli stessi che limiti o comprometta la capacità operativa corrente, la prestazione dei servizi contrattualmente erogati alla clientela, il know-how aziendale, direttamente scaturenti dalla criticità riscontrata.

Tra i criteri utilizzati particolare rilievo assume l'analisi degli scenari basata sulla previsione e costruzione dei diversi accadimenti che si potrebbero verificare stimando gli eventuali rischi.

Qualora si renda necessario, Enerj è in grado attivare metodi adeguati per le opportune attività di test tese a provare la capacità del sistema di rispondere al verificarsi di eventi dannosi o potenzialmente rischiosi. Tra i test si riportano di seguito i principali:

- verifiche sull'integrità degli archivi conservati
- verifiche sulle copie di sicurezza dei dati
- security testing and evaluation (STE): strumenti comprendenti un'ampia gamma di tests sui sistemi;
- modalita' di sviluppo sicuro previste nelle procedure del Sistema della Qualità ISMS

Tutti le informazioni relative alle verifiche periodiche effettuate dal SdC vengono storicizzate su appositi log. Tra queste, a titolo non esaustivo, citiamo: data e ora di ogni singola operazione, utente/processo, codice cliente, tipo di operazione, esiti,

informazioni di sicurezza.

Sulla base delle risultanze dei test vengono intraprese da ENERJ le azioni preventive allo scopo di eliminare cause di potenziali non conformità prima ancora che le stesse si verifichino. Sono pertanto azioni preventive anche gli interventi di miglioramento.

Le procedure di audit definite nel Sistema della Qualità interno sono implementate allo scopo di individuare le azioni idonee a prevenire le potenziali cause di pregiudizio per l'integrità dei dati. Il personale dell'Area di gestione della Qualità e della Sicurezza dei dati e delle informazioni esamina, con frequenza almeno mensile o quando le condizioni lo rendano necessario, i risultati degli audit condotti (e le relative richieste di azione correttiva) e i documenti di registrazione che rappresentano la fonte principale di informazione relativamente ai processi ed alle attività aziendali. Oltre ai succitati documenti l'Area prende in considerazione anche tutte le comunicazioni formali o informali di tutte le funzioni organizzative in merito all'evidenza di situazioni carenti, inefficienze ed a proposte di miglioramento evinte dalle analisi dei rischi condotte.

La formalizzazione di azioni preventive avviene anche attraverso l'osservazione e l'analisi statistica dei dati e delle informazioni messe a disposizione dalla piattaforma CRM.

10.4 Soluzioni adottate in caso di anomalie

In caso di anomalie sono previste diverse soluzioni commisurate all'entità e alle caratteristiche dell'incidente. Nello specifico, la trattazione degli incidenti di sicurezza è documentata nel Manuale della Sicurezza del Sistema Informativo (MSI) afferente al sistema ISMS.

La gestione delle segnalazioni di anomalia relative al SdC pervenute ad Enerj dai Clienti sono documentate nella procedura Procedura Gestione Clienti e Assistenza (PGC).

10.5 Sicurezza del SdC

Il RSC approva il piano della sicurezza del SdC (PDS) e il RQS ne cura l'aggiornamento.

In relazione a quanto previsto nella procedura di analisi dei rischi (PAR) e relativi moduli (MAR) vengono periodicamente condotte le analisi dei rischi inerenti il SdC.

La continuità operativa del SdC è garantita dall'infrastruttura di backup e disaster recovery del datacenter di Enerj così come dettagliato nel Piano della Continuità

Operativa del Business e Disaster Recovery (PCO) e nel Piano di Backup (PBK).