Manuale di Conservazione

Redatto ai sensi dell'art. 34 comma 1 CAD e del paragrafo 4.7 delle Linee Guida AGID 2020 sulla formazione, gestione e conservazione dei documenti informatici.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	21/03/25	Carlo Benvenuti	*Consulente esterno incaricato*
Verifica	13/05/25	Angela Catania	*Resp. Servizio Affari Istituzionali, Amministrazione del Personale, Segreteria del Direttore Generale e Politiche Giovanili*
Approvazione	28/05/25	Michele Scarrone	*Responsabile della Conservazione*

REGISTRO DELLE VERSIONI

Num. Versione	Data emissione	Modifiche apportate
1	28/05/25	Prima stesura

Introduzione

Il percorso normativo tracciato dal legislatore nel corso degli ultimi anni in materia di semplificazione ed innovazione dei procedimenti amministrativi riconosce alla dematerializzazione documentale un ruolo di primo piano. In tale contesto, la conservazione dei documenti nativi digitali e/o digitalizzati diviene fattore imprescindibile per la sostenibilità del processo di dematerializzazione stesso: è fondamentale, infatti, garantire la conservazione documentale nel lungo periodo, così come avviene tradizionalmente per i documenti analogici.

La conservazione è l'attività volta a proteggere nel tempo gli archivi di documenti informatici ed i dati. Ha l'obiettivo di impedire la perdita o la distruzione dei documenti e di garantirne autenticità, integrità e accesso controllato ai fini amministrativi e di ricerca.

L'art. 71 comma 1 del Codice dell'amministrazione digitale – CAD e le regole tecniche per la conservazione dei documenti informatici, adottate con DPCM 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione" - oggi modificate dalle *Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici* - ampliano il concetto di memorizzazione dei documenti informatici introducendo il concetto di "sistema di conservazione", ovvero, oltre ad assicurare la conservazione a normadei documenti elettronici e la disponibilità dei fascicoli informatici, è necessario definire regole, procedure, tecnologie e modelli organizzativi da adottare per la gestione di tali processi, con indicazioni di dettaglio.

Le Linee Guida Agid, emanate nel 2020, sono articolate in un documento principale e sei allegati tecnici ed hanno il duplice scopo di:

- *aggiornare le regole tecniche attualmente in vigore sulla formazione, protocollazione, gestione e conservazione dei documenti informatici, già precedentemente regolate nei DPCM del 2013 e 2014;*
- *fornire una cornice unica di regolamentazione per le regole tecniche e le circolari in materia, in coerenza con le discipline dei Beni culturali.*

Il Manuale di Conservazione, come previsto dall'art. 4.7 delle Linee guida AGID, è un documento informatico che illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate,le misure di sicurezza adottate ed ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Esso illustra nel dettaglio l'organizzazione del processo di conservazione di Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO definendo:

- i soggetti coinvolti
- i ruoli svolti dagli stessi
- il modello organizzativo di funzionamento dell'attività di conservazione
- la descrizione delle architetture e delle infrastrutture utilizzate
- le misure di sicurezza adottate
- ogni altra informazione utile alla gestione ed alla verifica del funzionamento nel tempo del sistema di conservazione.

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO è il soggetto Titolare dell'oggetto della conservazione, il quale intende sottoporre a conservazione i propri documenti digitali, affidando il processo di conservazione ad un conservatore accreditato presso AGID.

La redazione del Manuale di Conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete del Titolare dell'oggetto della conservazione.

La pubblicazione dello stesso è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del D.lgs. 33/2013.

Il Manuale costituisce una guida per gli attori coinvolti nel processo di gestione e di conservazione, per il cittadino e per le imprese. Ai primi, per attuare le corrette operazioni di gestione e conservazione documentale, agli ultimi due per comprendere le caratteristiche del Sistema di conservazione documentale e dei processi erogati.

Il Manuale di Conservazione è un documento informatico che riporta, nello specifico utilizzando talvolta rinvii al manuale di conservazione del fornitore, al quale l'Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO non ha apportato alcuna modifica relativamente a specifiche tecnico informatiche:

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

Il presente Manuale descrive il SdC di Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO rimandando tuttavia per gli specifici dettagli operativi al manuale di conservazione del fornitore nonché alla documentazione amministrativa descrittiva degli accordi intercorsi e delle varie fasi che si sono succedute nel tempo.

1 Terminologia (Glossario e acronimi)

All'interno del presente Manuale si fa riferimento alle definizioni riportate nella tabella che segue:

Termine	Significato
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristicheomogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività. In questo contesto si colloca anche il concetto di "Archivio informatico" che è costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Area Organizzativa Omogenea	Un insieme di funzioni e di strutture, individuate dall'amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
Classificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione al quale sia stato riconosciuto, dall'AGID il possesso dei requisiti del livello più elevato in termini di qualità e di sicurezza.
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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti.
Copia informatica di documento analogico	Il documento informatico avente contenuto identico a quello del documento analogico da cui ètratto.
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico dacui è tratto.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto susupporto informatico con diversa sequenza di valori binari.
Documento	Viene definito documento una rappresentazione di atti, fatti e dati su un supporto sia esso cartaceoo informatico. La rappresentazione può avvenire direttamente o mediante un processo di elaborazione elettronica. La disposizione di questi dati sul supporto e le relazioni che sussistono traquesti oggetti determinano rispettivamente forma e sostanza del documento.
Documento analogico	La rappresentazione non informatica di atti, fatti, o dati giuridicamente rilevanti. Il "documento analogico originale" può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi; un tipico caso di documento analogico originale non unico è la fattura: viene emessa da un soggetto mittente che è tenuto alla conservazione di una copia e viene, successivamente, ricevuta da un destinatario che è tenuto alla conservazione del documento stesso come originale.
Documento Amministrativo Informatico - DAI	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie,del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa. Il Doc. informatico è il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento statico non modificabile	Documento informatico redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione nonché immutabile nel tempo; a tal fine il documento informaticonon deve contenere macroistruzioni o codice eseguibile, tali da

	attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.
Evidenza informatica	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti,documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
Firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altridati elettronici, utilizzati come metodo di identificazione informatica. Vedi art.li 3 e 26 del regolamento EIDAS.
Firma elettronica avanzata - FEA	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. Vedi art. 3 e 26 del regolamento EIDAS.
Firma elettronicaqualificata - FEQ	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma" e non più "ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario. Vedi art.3 del regolamento EIDAS.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistemadi chiavi crittografiche, una pubblica e una privata, correlate tra loro che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il doc informatico; comunemente è identificato attraverso l'estensione dei file.
Funzione di Hash	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittograficao digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Impronta	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.
Insieme minimo di metadati del documento informatico	Complesso di metadati, la cui struttura è descritta nell'allegato 5 delle Linee Guida Agid 2020, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Metadati	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti aglioggetti da conservare.Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in: a) pacchetti di versamento; b) pacchetti di archiviazione; c) pacchetti di distribuzione.
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione

Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
Pacchetto di distribuzione	Il pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte aproteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quantoconforme alle modalità previste dal manuale di conservazione.
Processo di conservazione	L'insieme delle attività finalizzate alla conservazione dei documenti informatici
Rapporto di versamento	Il documento informatico che attesta l'avvenuta presa in carico da parte del sistema diconservazione dei pacchetti di versamento inviati dal produttore.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti idocumenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare (Repertorio)	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Responsabile del Servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso deirequisiti professionali individuati da AGID.
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governala gestione con piena responsabilità ed autonomia.
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi. Garantisce l'origine e l'integrità dei documenti digitali. Si riferisce ad una persona giuridica (un organismo unitario composto da una pluralità di individui o un complesso di beni, al quale vengono riconosciuti diritti e doveri).
Sistema di conservazione	Un sistema che dalla presa in carico fino all'eventuale scarto assicura la conservazione dei documenti e dei fascicoli informatici con i metadati a essi associati, tramite l'adozione di regole, procedure e tecnologie idonee a garantirne le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

ACRONIMI:

AOO	Area organizzativa omogenea
AgID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale e s.m.i.
ISMS	Information Security Management System – Sistema di gestione della qualità e della sicurezza delle informazioni di EnerJ
GDPR	Regolamento (UE) No 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardoal trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
OAIS	Open Archival Information System
PdA/AiP	Pacchetto di Archiviazione
PdD/DiP	Pacchetto di Distribuzione
PdV/SiP	Pacchetto di Versamento
SdC	Sistema di Conservazione
RGD	Responsabile della Gestione Documentale
RdC	Responsabile della Conservazione

2 Normativa di riferimento

Il presente Manuale della Conservazione è stato redatto tenendo conto di quanto prescritto dalle seguenti normative:

- 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;
- D.P.R. 28 dicembre 2000, n. 445 e s.m.i. - Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - TUDA;
- D.Lgs. 196/2003, Codice in materia di protezione dei dati personali;
- D.Lgs. 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio
- D.Lgs. 7 marzo 2005 n. 82 Codice Amministrazione Digitale e s.m.i;
- Deliberazione CNIPA n. 45 del 21 maggio 2009 modificata dalla emanazione della Determinazione Commissariale DigitPA n.69 del 28 luglio 2010 (oggi AgID) Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;
- D.P.C.M. 3 dicembre 2013 Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, comma 4,43 commi 1e 3,44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- D.P.C.M. 22 febbraio 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- D.P.C.M. 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 sostitutiva, 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;
- D.M.E.F. (Decreto del Ministero dell'economia e delle finanze) 3 aprile 2013, n. 55 Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche;
- 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;
- D.M.E.F. (Decreto del Ministero dell'economia e delle finanze) 17 giugno 2014 Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ad alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n.82/2005;
- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (eIDAS), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- D.P.C.M. 13 novembre 2014 Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Regolamento (UE) 2016/679 (General Data Protection Regulation o GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;

- Circolare Accredia 5/2017 - Schema di accreditamento degli Organismi di Certificazione per il processo di certificazione dei Conservatori a Norma, secondo le disposizioni dell'Agenzia per l'Italia Digitale.
- Circolare n. 2 del 9 aprile 2018, recante i criteri per la qualificazione dei Cloud Service Provider per la PA;
- Circolare n. 3 del 9 aprile 2018, recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;
- DECRETO-LEGGE 16 luglio 2020, n. 76 - Misure urgenti per la semplificazione e l'innovazione digitale. (G.U. Serie Generale n.178 del 16/07/2020 - S.O. n. 24)
- Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici, 2020.
- Determinazione n. 455/2021 del 25 giugno 2021 - Adozione del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lett. b). Il Regolamento è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 ed entrerà in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la circolare n. 65/2014.

Standard Internazionali

ISO/IEC

- UNI EN ISO 9000:2015 - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualità - Requisiti;
- UNI EN ISO 9004:2018 - Gestione per la qualità - Qualità di un'organizzazione - Linee guida per conseguire il successo durevole
- UNI EN ISO 19011:2018 - 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 31000:2018 - Gestione del rischio - Principi e linee guida;
- UNI CEI EN ISO/IEC 27000:2017 - Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Descrizione e vocabolario;
- UNI CEI EN ISO/IEC 27001:2017 - Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti;
- UNI CEI EN ISO/IEC 27002:2017 - Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni;
- ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management;
- UNI ISO 15489-1:2016 - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- UNI ISO/TR 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 metadati del Dublin Core.
- ISO 15836-1:2017 - Information and documentation -- The Dublin Core metadata element set -- Part 1: Core elements
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- UNI ISO 31000 Gestione del rischio - Principi e linee guida.

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 (2015-06) - Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture;
- ETSI GS ISI 001-2 V1.1.1 (2015-06) - 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 (2015-11) - Information Security Indicators (ISI); Event Model A security event classification model and taxonomy;
- ETSI GS ISI 003 V1.1.2 (2018-01) – 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.
- 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) – Recommended Practice – CCSDS 650.0-M-2 - 2012;
- ETSI TS 119 511 V1.1.1 (2019-06) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- ETSI TS 119 512 V1.1.1 (2020-01) - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services;
- ISAD (G) - General International Standard Archival Description.

3 Modello Organizzativo dell'Ente

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO è costituito da unico codice:

CODICE UNIVOCO	**UFQ4JO**
DOMICILIO DIGITALE	direzione@pec.aliseo.liguria.it
INDIRIZZO	Via San Vincenzo 4, 16124 Genova

La struttura, in continuo aggiornamento ed evoluzione può essere consultata all'indirizzo *www.indicepa.gov.it*

L'Agenzia è organizzata in unica Unità Organizzativa; l'organigramma aggiornato dell'Ente può essere consultato nell'apposita sezione di "Amministrazione trasparente".

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO è il soggetto "Produttore" ed in quanto tale è il Titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità ed autonomia; in relazione al modello organizzativo di seguito adottato affida a Conservatori accreditati la gestione del Servizio di Conservazione secondo quanto previsto dalla normativa in materia.

Dati Ente:

Descrizione dell'Amministrazione	Agenzia Ligure per gli Studenti e l'Orientamento - ALiSEO
Codice Fiscale	02575860990
Codice IPA	Aliseo
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale.	Via San Vincenzo 4, 16124 Genova
Casella di posta elettronica istituzionale della AOO	direzione@pec.aliseo.liguria.it

Nomine:

Nominativo del **Responsabile della Conservazione documentale;** definisce le politiche del sistema di conservazione e predispone il manuale di conservazione, è il soggetto cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione.	**Dott. Michele Scarrone** Decreto del Direttore Generale nr. 87 Del 11/03/25

3.1 Conservazione in outsourcing

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO (soggetto titolare dell'oggetto della conservazione) realizza i processi di conservazione all'interno della propria struttura organizzativa affidandoli ad conservatori accreditati Agid di cui all'art. 44-bis, comma 1, del Codice, fatte salve le competenze del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.

Il Produttore è il titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce ed attua le politiche complessive del Sistema di conservazione governandone la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato affida ai Conservatori la gestione del servizio di conservazione secondo quanto previsto dalla normativa in materia.

Il modello in Outsourcing prevede: un Responsabile della Conservazione interno al produttore ed un Responsabile del Servizio di Conservazione interno a ciascun conservatore.

In ogni caso, modello in house o in outsourcing, il sistema di conservazione deve rispettare le linee previste dalla normativa in vigore.

4 Ruoli e responsabilità

Nel Sistema di Conservazione si individuano almeno i seguenti ruoli:

- *Titolare dell'oggetto della conservazione e Produttore dei PdV*
- *Utente abilitato*
- *Responsabile della Conservazione (lato produttore)*
- *Responsabile del Servizio di Conservazione (RSC)/Conservatore*

4.1 Titolare dell'oggetto della conservazione e Produttore PdV

Il Titolare dell'oggetto della conservazione e Produttore PdV si identifica con l'Agenzia, ovvero si tratta della struttura organizzativa che ha la titolarità dei documenti da conservare.

L'Ente affida la conservazione dei propri documenti a ciascun Conservatore in outsourcing attraverso la sottoscrizione di un contratto di servizio.

Il Produttore del PdV è quindi persona giuridica che, avvalendosi dei servizi di conservazione degli archivi informatici erogati dal Conservatore, produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.

4.2 Utente Abilitato

L'Utente del SdC è il ruolo svolto da soggetti (pubblici o privati) oppure da un sistema di gestione documentale che interagisce con i servizi del sistema di conservazione al fine di trovare e acquisire le informazioni di interesse (PdD).

Le Autorità incaricate di effettuare i controlli (quali l'Agenzia delle entrate, la Guardia di Finanza, etc.) hanno diritto di accedere in qualsiasi momento al sistema di conservazione; inoltre godono dello stesso diritto anche le Autorità di controllo diversificate in base alla natura giuridica e alla mission del produttore.

L'Agid, in qualità di Autorità che ha rilasciato la certificazione, dichiarando valido il sistema di conservazione, può effettuare l'accesso al sistema per compiere l'attività di controllo.

Di seguito sono elencati gli utenti abilitati all'accesso ai servizi di conservazione in base alle corrispondenti Aree organizzative corrispondenti:

Area organizzativa	Nominativo
Servizio Affari Istituzionali, Amministrazione del Personale, Segreteria del Direttore Generale e Politiche Giovanili	Dott.ssa Angela Catania
Servizio Gestione Risorse Economiche e Finanziarie	Sig.ra Carmela Censuales

4.3 Responsabile della Conservazione

Il Responsabile della Conservazione è la figura cardine che governa il processo della conservazione digitale: è la persona fisica normalmente inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce ed attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilitàe autonomia, in relazione al modello organizzativo adottato. Il RdC opera secondo quanto previsto dall'art. 44 comma 1-quater, del CAD.

Nella Pubblica Amministrazione, il Responsabile della Conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenzegiuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.
d) Non può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione, come previsto dalle attuali Linee Guida in materia (par. 4.7).

L'ente ha deciso di nominare il Direttore Generale Responsabile della conservazione, affiancato da un professionista esterno.

Il RdC definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. Il RdC, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse ad uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze.

In particolare, il **Responsabile della Conservazione**:

a) definisce le politiche di conservazione ed i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
l) predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui, come per Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO, il Servizio di Conservazione venga affidato a più Conservatori esterni, le attività suddette o alcune di esse, ad esclusione della lettera l), potranno essere affidate al Responsabile del Servizio di Conservazione (interno al soggetto Conservatore), rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing.

4.4 Responsabile del Servizio di Conservazione

Il Responsabile del Servizio di Conservazione è il soggetto conservatore nominato dal produttore a svolgereil servizio di conservazione in relazione alla normativa vigente ed alle condizioni sottoscritte nel contratto diServizio. Il RSC è individuato, all'interno dell'organigramma dei Conservatori accreditati, come Responsabile dei Servizi di gestione dell'archivio informatico e conservazione ed è incaricato delle seguenti funzioni:

a. definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con pienaresponsabilità ed autonomia;
b. definisce le caratteristiche ed i requisiti del sistema di conservazione in conformità alla normativa vigente;
c. assicura la corretta erogazione del servizio di conservazione all'ente produttore;

d. 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.

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO gestisce il SdC attraverso più Conservatori accreditati che dispongono di un processo tecnico e organizzativo certificato e validato da strutture esterne qualificate nel settore.

Profilo dei Conservatori	**Enerj Srl** Via Diaz, 4 Centro direzionale Diamante 2 Sant' Ambrogio di Valpolicella 37015, Verona, ITALY Partita IVA 03466010232 Tel. [+39] 045 878 04 50 Email info@enerj.it PEC: enerj@actalispec.it
	InfoCert S.p.A. Società Soggetta alla Direzione e al Coordinamento di Tinexta S.p.A. Piazzale Flaminio 1/B 00196 – Roma, ITALY Partita IVA 07945211006 Tel. [+39] 049 78 49 350 Email infocert@legalmail.it PEC: notifiche.pec@mail.infocert.it

5 Formati e Metadati

Il formato è l'insieme di informazioni che determinano la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto. Un oggetto digitale è una sequenza di bit fissati con una certa organizzazione fisica su di una memoria. Tale contenuto digitale viene memorizzato e definito file.

La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore.
La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a talescopo, infatti, un problema di cui è necessario tener presente, è costituito dall'obsolescenza dei formati. Attualmente la soluzione più sicura è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine.
I formati da utilizzare nell'ambito delle Linee guida AGID sono quelli previsti dall'Allegato 2 denominato "Formati di file e riversamento". Nello scegliere i formati di file da utilizzare per i propri documenti informatici, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: *formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo*.

Le pubbliche amministrazioni garantiscono sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici. Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), le pubbliche amministrazioni, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori. È possibile

utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento", effettuando una valutazione di interoperabilità.

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine. I metadati vengono esplicitamente citati come oggetti da sottoporre a conservazione associati ai documenti informatici, ai documenti amministrativiinformatici e ai fascicoli informatici aggregazioni documentali.

I Metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono,spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione. Sonoinfatti un insieme di dati associati ad 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.

Ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc.

I metadati sono descritti all'interno dell'allegato tecnico del presente Manuale (MCD01 Accordo di versamento).

6 Oggetti sottoposti a conservazione

Il modello adottato per la conservazione digitale garantisce la conservazione di oggetti digitali a lungo termine, nel rispetto della normativa vigente.

Ai fini della corretta conservazione nel medio e lungo periodo è indispensabile conoscere la natura di oggettiinformativi complessi sia dei documenti che delle loro aggregazioni.

Il Sdc acquisisce, gestisce, organizza e conserva documenti informatici, in particolare documenti amministrativi informatici - DAI, e le loro aggregazioni documentali informatiche sotto forma di fascicoli e serie. Il DAI è prodotto e memorizzato su di un supporto elettronico durante lo svolgimento di un'attività di carattere amministrativo e, grazie al sistema di gestione in cui è stato inserito al momento dell'acquisizione,possiede le opportune caratteristiche di *immodificabilità, integrità e staticità*, come previsto dalla normativavigente.

Durante la vita nel Sistema di gestione corrente, il documento è sottoposto ad una serie di azioni (es. *protocollazione o registrazione a sistema, classificazione, assegnazione al Responsabile del procedimento, attribuzione al fascicolo, etc.*) che ne determinano la posizione logica all'interno dell'archivio così come l'identità: la particolarità e unicità del documento è caratterizzata proprio dalla specifica funzione che esso riveste nello svolgimento dell'attività del Produttore.

Le caratteristiche proprie del documento vengono tradotte in ambito elettronico in *metadati*: informazioni connesse al documento che consentono all'interno del Sistema l'identificazione, la descrizione, la gestione ela conservazione. La normativa prescrive un pacchetto minimo di metadati da associare al documento informatico immodificabile. In tal senso risulta importante l'appartenenza del documento al fascicolo.

La fascicolazione è un requisito importante per la corretta gestione del documento all'interno del contesto relazionale che ne determina il significato e l'identità. "Fascicolare" significa esplicitare la posizione logica e fisica del singolo documento all'interno dell'archivio e quindi stabilire esattamente la funzione che il documento svolge. Le azioni a cui il documento è soggetto nel corso della propria esistenza sono strettamente determinate dall'appartenenza al fascicolo.

6.1 Tipologie documentali da inviare in conservazione

I documenti da portare in conservazione secondo la normativa sono: documenti amministrativi, fiscali e contabili, i fascicoli, i registri e i repertori informatici predisposti secondo le seguenti possibili forme:

- Documenti di testo, fogli di calcolo, schemi XML redatti tramite l'utilizzo di appositi strumenti software;
- Documenti acquisiti per via telematica o su supporto informatico, e-mail, documenti acquisiti come copia per immagine di un documento analogico;
- Registrazioni informatiche di transazioni o processi informatici, dati forniti dall'utente attraverso la compilazione di moduli o formulari elettronici;
- Insiemi di dati, provenienti da una o più basi dati, raggruppati secondo una struttura logica determinata (visite).

Nel Manuale del Conservatore sono indicate le tipologie documentali contrattualizzate. Per questo motivo, a fronte di un invio di un documento che non rientra nelle tipologie contrattualizzate, il web service del SDC restituisce un codice di errore specifico.

Assieme alle tipologie documentali, vengono contrattualizzati anche i tempi di conservazione, per cui lo scarto dei documenti lato SDC viene gestito in autonomia dallo stesso software.

Viene comunque data discrezionalità all'Ente, in quanto è necessaria un'autorizzazione da parte della Sovrintendenza per poter procedere con l'eliminazione fisica dei documenti.

L'Ente si riserva di inviare nel tempo ulteriori tipologie documentali.

Il Sistema di conservazione acquisisce pacchetti informativi trasformandoli in PdA (pacchetti di archiviazione) 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. I metadati di ogni tipologia documentale sono definiti in modo parametrico attraverso il SdC e formalizzati nel Contratto di Servizio.

Di seguito si riportano le principali tipologie di documenti amministrativi informatici ed il relativo tempo di conservazione, la periodicità di versamento ed il formato che l'Agenzia riversa in conservazione dalla Piattaforma Gestionale in uso:

Tipologia documento Conservazione	**Tempo di conservazione**	**Versamento – periodicità**	**Formato doc.**
Allegati firmati di Protocollo	illimitata	Versamento periodico da Civilia Next	Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades), EML
Registro giornaliero di protocollo	illimitata	Versamento giornaliero da Civilia Next	Pdf/A
Atti Amministrativi	illimitata	Versamento periodico da Civilia Next	Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades)
Fatturazione attiva e passiva	10 anni	Versamento periodico da Eusis GPI	.xml, Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades)

L'ente si riserva per il futuro di inviare in conservazione ulteriori tipologie documentali di rilevanza per lo stesso.

Di seguito si riporta la cronologia dei Conservatori accreditati AGID a cui si è rivolto Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO per i servizi di conservazione documentale:

Conservatori	Tipologie documentali riversate	Periodo di riferimento
ENERJ S.r.l.	RgP - Protocollo – Atti amm.vi	11/02/2019 - attualmente
INFOCERT S.p.A.	Fatture attive - passive	01/01/2019 - attualmente

7. Processo di Conservazione

Il processo di conservazione è realizzato sulla base del modello funzionale OAIS (Open Archival Information System) normato dallo standard ISO 14721:2003. 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.

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati in conformità con le Linee Guida AGID.

7.1 Tipologie di pacchetti informativi

Di seguito vengono descritti 3 principali tipi di pacchetti informativi:

Pacchetto di versamento (SIP-*Submission Information Package* o PdV): il pacchetto inviato ad un sistema di conservazione dal produttore, ovvero Pacchetto informativo inviato dal produttore al Sistema di conservazione secondo un formato predefinito e concordato. Questo strumento di gestione e conservazionedocumentale indentifica, in maniera univoca, l'insieme dei dati che vengono inviati al sistema di conservazione

Pacchetto di archiviazione (AIP-*Archival Information Package* o PdA): il pacchetto conservato in un sistema di conservazione, ovvero pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato Specifiche tecniche del pacchetto di conservazionedel CAD D.Lgs. 82/2005 e s.m.i.. Il pacchetto di archiviazione è un "derivato" del pacchetto di versamento e ha la funzione di archiviare i dati in esso contenuti.

Pacchetto di distribuzione (DIP-*Dissemination Information Package* o PdD): il pacchetto inviato ad un Utente da un sistema di conservazione, ovvero pacchetto informativo inviato dal Sistema di conservazione all'utentein risposta ad una sua richiesta. E' un pacchetto informativo che viene ricevuto da un utente come risposta auna richiesta di esibizione del contenuto conservato inoltrata a un sistema di conservazione.

7.2 Pacchetto di versamento

Il PdV è il pacchetto informativo, inviato dal produttore al SdC, il cui formato e contenuto sono concordati tra il soggetto produttore ed il consumatore. Il PdV eventualmente integrato da ulteriori informazioni concordate con il cliente, viene trasferito dal produttore al soggetto conservatore tramite una apposita procedura informatica automatizzata (Web services) 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.

7.3 Pacchetto di archiviazione

Il PdA viene formato secondo le regole tecniche definite nella norma UNI 11386:2020 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, CF, Partita IVA, etc.);
- 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;

7.4 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 dagli Utenti Abilitat dall'ente

7.5 Modalità di acquisizione dei PdV per la loro presa in carico

La modalità di trasmissione dei pacchetti di versamento (PdV) avviene tramite l'utilizzo di appositi web-services che ne consentono l'inserimento nel SdC. Tutti i canali di comunicazione instaurati tra cliente e conservatore sono cifrati per la protezione dei dati oggetto di transazione.

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) del Conservatore.

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).

7.6 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, per determinare la correttezza delle caratteristiche formali e dei documenti informatici e/o delle aggregazioni documentali informatiche afferenti al pacchetto stesso. 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 modalità 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:** il SdC verifica 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 sottoporreal 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, etc.).
- **Verifica dell'omogeneità dei documenti**: dove previsto dagli accordi contrattuali viene verificata la coerenza nella progressione numerica e temporale nonché la progressività rispetto all'ultima operazione di conservazione.
- **Verifica dei metadati minimi obbligatori**: il sistema verifica la presenza dei metadati minimi obbligatori per ogni cliente e per ogni tipologia documentale, così come definito negli accordi specifici del Contratto di Servizio.

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

L'accettazione del PdV dà luogo alla generazione automatica del rapporto di versamento relativo ad uno o più pacchetti di versamento. Il rapporto di versamento è comprensivo dell'elenco dei pacchetti di versamento accettati. Il SdC attribuisce un identificatore univoco a ciascun rapporto di versamento generato e lo segna temporalmente. 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. 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 Titolare dell'oggetto della conservazione (Ente) secondo diverse modalità in base a quanto espresso nel Contratto di Servizio.
L' interfaccia web consente all'Ente di monitorare lo stato di tutti i PdV inviati al SdC e pertanto gestire anche eventuali errori risultanti dai controlli.

Tutte 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.

7.8 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 segnata temporalmente e trasmessa al Titolare dell'oggetto della conservazione. 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.

Tutte le informazioni inerenti alle operazioni eseguite dagli utenti e dai processi informatici relative ai PdV rifiutati dal SdC vengono storicizzate su appositi log.
Maggiori informazioni relative al rifiuto dei Pacchetti di Versamento e comunicazione delle anomalie sono contenute nei Manuali di conservazione redatto dai Conservatori nonché procedure operative disponibili dai Conservatori.

7.9 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. 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.

7.10 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 PdA. I PdA 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, etc. I supporti fisici sono trasportati a cura e responsabilità dell'Ente conservatore sulla base di specifici requisiti definiti dal RdC.
I dati richiesti sono crittografati con il certificato del destinatario prima della loro spedizione/trasmissione allo stesso. Tutte le informazioni relative ai PdD richiesti, generati, esportati dal SdC vengono storicizzate su appositi log.

Fasi del Processo di esibizione del PdD

1) Richiesta di accesso al sistema di selezione
2) Verifica soggetto autorizzato
3) Accesso al sistema di selezione (se la verifica da esito positivo, altrimenti rifiuto della richiesta)
4) Selezione dei documenti informatici da esibire e Formazione della richiesta di esibizione
5) Generazione del PdD (documenti selezionati + relativo IPdA)
6) Messa a disposizione al soggetto fruitore

7.11 Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale

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

7.11.1 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 idocumenti informatici di interesse;
- in occasione dei backup e delle repliche perpetrate sui PdA allo scopo di garantirne la permanenza deirequisiti essenziali di fruibilità e verificabilità.

7.11.2 Produzione di copie informatiche ed estratti di documenti informatici

Il procedimento di produzione di copie informatiche ed estratti di documenti informatici consente di ottenieredocumenti 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.

7.11.3 Produzione di copie informatiche di documenti analogici

Il procedimento di produzione di copie informatiche di documenti analogici consente di generare documentiinformatici 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 prevede espressamente la possibilità di conservare dette fattispecie documentali. Il procedimento di produzione di copie informatiche di documenti analogici viene attivato quando il soggetto fruitore conferisce al SdC documenti espressi su supporti analogici.

7.12 Scarto dei pacchetti di archiviazione

Il SdC effettua lo scarto dei pacchetti di archiviazione sulla base di quanto espresso nel Contratto 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. 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 Produttore.

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

Al fine di garantire l'interoperabilità del proprio sistema di conservazione e la trasferibilità di archivi informatici ad altri eventuali soggetti conservatori i conservatori predispongono 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 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 espressadal 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.

Il SdC dell'Agenzia tende ad 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, i conservatori si impegnano 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.

7.14 Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del SdC

Tutte le comunicazioni prodotte durante le transazioni di pacchetti informativi (log applicativi, log di sistema, etc.) sono conservate mediante il SdC stesso.

8. 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 i conservatori e presso l'ente produttore,
- 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 suamanutenzione, procedure di conservazione, procedure di Audit, Riesame della Direzione.

9. Monitoraggio e controlli

Il SdC 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.

9.1 Procedure di monitoraggio applicativo

Gli applicativi software del SdC producono i log delle transazioni dei pacchetti informativi, 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.

9.2 Procedure di monitoraggio infrastrutturale

L'infrastruttura tecnologica dei conservatori è descritta nel Manuale della Sicurezza dei Sistemi Informativi (MSI) e relativi allegati.

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

9.3 Verifica dell'integrità degli archivi

Il SdC 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 Piano della Sicurezza del SdC;
- 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;
- nel Manuale di conservazione dei Conservatori (MDC).

Qualora si renda necessario, i conservatori sono in grado attivare metodi adeguati alle 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 test sui sistemi;
- modalità di sviluppo sicuro previste nelle procedure del Sistema della Qualità ISMS.

Tutte 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 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. 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, irisultati 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 tuttele 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.

9.3.1 Verifiche a cura del Responsabile della Conservazione

In aggiunta alle verifiche sull'integrità e leggibilità degli archivi, operate dal conservatore esterno, il Responsabile della Conservazione predispone un piano di ulteriori verifiche e monitoraggi, ai sensi dell'art. 4.5 (Attività proprie del RdC) punti e) ed f) delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici di AgID (maggio 2021, entrati in vigore il 1 gennaio 2022): le stesse verifiche sono documentate e annotate nel relativo allegato 4 al presente manuale.

Nello stesso allegato sono presenti le annotazioni dei relativi esiti delle verifiche effettuate.

9.4 Soluzioni adottate in caso di anomalie

In caso di anomalie sono previste soluzioni commisurate all'entità ed alle caratteristiche dell'incidente. Nello specifico, la trattazione degli incidenti di sicurezza è documentata nel Manuale della Sicurezza del Sistema Informativo afferente al sistema ISMS. La gestione delle segnalazioni di anomalia relative al SdC pervenute ai conservatori dai Clienti sono documentate nella Procedura Gestione Clienti e Assistenza (PGC).

9.5 Sicurezza del SdC

Il RSC approva il piano della sicurezza del SdC e il RQS ne cura l'aggiornamento. In relazione a quanto previsto nella procedura di analisi dei rischi vengono periodicamente condotte le analisi dei rischi inerenti al Sistema di conservazione.

La continuità operativa del SdC è garantita dall'infrastruttura di backup e disaster recovery del datacenter dei Conservatori così come dettagliato nei loro Piani della Continuità Operativa del Business e Disaster Recovery (PCO) e nei relativi Piani di Backup (PBK).

10. Allegati

Il presente MdC (manuale della conservazione) è concepito e redatto definendo un corpo centrale (il presente documento), snello e schematico ma esaustivo, e una serie di allegati che ne caratterizzano il contesto temporale e lo scenario operativo del momento in cui è stato redatto.

L'insieme degli allegati, elencati nel paragrafo successivo, si rende necessario al fine di integrare il documento con informazioni provenienti da procedure interne o soggetti esterni all'organizzazione, come ad esempio il manuale del Conservatori esterni.

Attraverso il versionamento del documento è possibile tenere traccia nel tempo degli aggiornamenti intervenuti e procedere con le modifiche e integrazioni necessarie.

10.1 Elenco degli allegati al presente manuale

Questa sezione del manuale contiene il dettaglio dei documenti allegati, numerati progressivamente e con la descrizione della natura e contenuto degli stessi. È possibile poi avere traccia delle integrazioni,

modifiche o sostituzione degli allegati, attraverso l'esame della tabella delle versioni presente sul frontespizio del presente manuale.

NR.	Allegato	Descrizione
1	Elenco documenti conservati	Tabella riepilogativa che elenca tutte le tipologie attualmente portate in conservazione.
2	Manuale della conservazione Enerj	Manuale del conservatore esterno Enerj Srl nella versione ultima disponibile
3	Manuale della conservazione Infocert	Manuale del conservatore esterno Infocert Spa nella versione ultima disponibile
4	Registro delle verifiche effettuate	Elenco cronologico delle operazioni di verifica operate a cura del RdC o di personale delegato

11. Approvazione e aggiornamento del Manuale

Agenzia Ligure per gli Studenti e l'Orientamento – ALiSEO adotta il presente Manuale su proposta del Responsabile della Conservazione.
Il Manuale potrà essere aggiornato a seguito di:

- Normativa sopravvenuta
- Introduzione, nell'Ente, di nuove pratiche finalizzate al miglioramento dell'attività amministrativa in termini di efficacia, efficienza e trasparenza
- Sostituzione del conservatore accreditato
- Altri motivi di natura tecnica

Il presente Manuale è operativo dal 29 maggio 2025

Con l'entrata in vigore del presente Manuale sono abrogati tutti i regolamenti dell'Ente nelle parti contrastanti con lo stesso.

Il Manuale è pubblicato sul sito istituzionale dell'Ente nella sezione "Amministrazione trasparente" sottosezione "Altri Contenuti".

Lista dei tipi di documenti in conservazione

Allegato 1

Ente: ALISEO - Agenzia Ligure per gli Studenti e l'Orientamento

Tipo documento	Conservatore	Inizio conservaz.	Durata conserv.	Chiusura pacchetti	Formati
Registro giornaliero di Protocollo (RGP)	Enerj	01/01/19	Tempo illimitato	Giornaliero	.pdf .xml .P7M
Documenti di Protocollo (PROTO)	Enerj	01/01/19	Tempo illimitato	Mensile	.pdf .xml .P7M .eml
Atti Amministrativi (ATTI)	Enerj	01/01/19	Tempo illimitato	Mensile	.pdf .xml .P7M .eml
Fattura Attiva PA (FATCPA)	Infocert	01/01/19	10 anni	Mensile	.pdf .xml .P7M .eml
Fattura Passiva PA (FATFPA)	Infocert	01/01/19	10 anni	Mensile	.pdf .xml .P7M .eml

Manuale del servizio di conservazione (MDC)

Servizio di conservazione a norma degli archivi informatici di ENERJ SRL.

Rev. 14 del 30/05/2022

ENERJ Srl - P.IVA 03466010232 - Via Diaz 4 Sant'Ambrogio di Valpolicella 37015, Verona [ITALY]

Sommario

1 Introduzione

ENERJ è una società di servizi specializzata nella consulenza e nella realizzazione di soluzioni dedicate alla gestione elettronica documentale e nella conservazione a norma di legge degli archivi informatici per clienti privati e PA.

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

Allo scopo di garantire il livello massimo di qualità e sicurezza 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 (con relative estensioni ISO/IEC 27017 e ISO/IEC 27018)
- UNI EN ISO 9001

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".

ENERJ dal 13 febbraio 2022 è iscritta ed è stata inserita nel marketplace dei Conservatori AGID dal 2022 e dal 2015 al 2021 è stata Conservatore accreditato AGID.

ENERJ ha adottato un sistema di gestione per la qualità e per la sicurezza delle informazioni in modo da:

- Preservare la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un adeguato processo di gestione dei rischi che dà fiducia alle parti interessate
- Dimostrare la capacità di gestire processi e fornire con regolarità prodotti che rispettino i requisiti dei clienti e quelli cogenti stabiliti da leggi, direttive, regolamenti e prescrizioni obbligatorie in genere;
- Accrescere la soddisfazione delle parti interessate con l'efficace applicazione del sistema di gestione, ivi inclusi i processi per il miglioramento continuo e l'assicurazione della conformità ai requisiti dei clienti ed a quelli cogenti applicabili.

Tale sistema di gestione per la qualità e per la sicurezza delle informazioni è stato conformato alle prescrizioni della norma UNI EN ISO 9001: "Sistemi di gestione per la qualità" e alla norma UNI CEI ISO/IEC 27001: "Sistemi di gestione per la sicurezza delle informazioni" con estensioni: 27017: " Codice di condotta per i controlli di sicurezza delle informazioni basato su ISO/IEC 27002 per i servizi cloud" e 27018: "Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei cloud pubblici che agiscono in qualità di responsabili del trattamento delle PII".

Inoltre, ENERJ, per finalità etiche e in considerazione della rilevanza dei propri processi informatici e della volontà di allineamento con le previsioni di legge, ha integrato il modello di organizzazione, gestione e controllo (MOGC) conforme al Decreto Legislativo 8 giugno 2001 n. 231 che prevede:

- un Codice Etico quale codice comportamentale che elenca i principi etici che vincolano l'azione della Società;
- un Sistema disciplinare volto a tutelare l'azienda e a sanzionare i comportamenti che la danneggiano nei suoi asset materiali e immateriali;
- un Organigramma aziendale che individua la Direzione e i soggetti in posizione apicale, risultando gli altri sottoposti all'altrui direzione (dipendenti e collaboratori);
- un'analisi del rischio (mediante mappatura dei processi e analisi delle singole aree di rischio) con l'indicazione delle figure responsabili e dei controlli attivati;
- un quadro di deleghe e di direttive aziendali vincolanti
- l'individuazione di un Organismo di Vigilanza (OdV) garante dell'applicazione del MOGC;
- l'individuazione e pianificazione delle modalità di controllo preventivo (piani di audit);
- un programma di miglioramento continuo.

ENERJ, come premesso, eroga servizi di conservazione a norma degli archivi informatici a clienti privati e PA tramite il proprio sistema di conservazione (JSDC) che garantisce la gestione ed il mantenimento delle caratteristiche di autenticità, integrità, intelligibilità, affidabilità, reperibilità e interoperabilità dei documenti informatici.

È necessario premettere che il contesto normativo che regola la formazione, gestione e conservazione dei documenti informatici è stato recentemente aggiornato dalle importanti modifiche apportate al Codice dell'amministrazione digitale (CAD) dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020, in relazione ai sistemi di conservazione.

Si considera di particolare importanza il superamento del meccanismo di accreditamento dei conservatori dei documenti informatici per conto delle pubbliche amministrazioni e la gestione dei sistemi di conservazione da parte di soggetti esterni che si uniforma alla disciplina europea in materia e alle nuove disposizioni dell'Agenzia per l'Italia digitale (AGID).

Dette disposizioni sono contenute nel Regolamento oggetto della Determinazione n. 455/2021 ed è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020.

L'entrata in vigore del Regolamento è il 1° gennaio 2022, data a partire dalla quale è abrogata la circolare n. 65/2014 e di conseguenza l'intero meccanismo di accreditamento.

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 e nell'accordo di versamento (MCD01).

2.1.1 Accordo di versamento (MCD01)

Quest'ultimo in particolare costituisce un allegato contrattuale e contiene tutte le informazioni relative allo specifico rapporto contrattuale e di servizio, in particolare in relazione a:

- i dati identificativi del soggetto titolare,
- le informazioni relative ai soggetti responsabili coinvolti nella gestione dei processi di conservazione (produttore del PDV, responsabile della conservazione e utente),
- i parametri relativi all'organizzazione temporale del processo e alle modalità di conservazione,
- le caratteristiche relative al tipo di oggetto conservato,
- le informazioni relative ai formati e metadati utilizzati per rappresentare gli oggetti conservati,
- i controlli applicati agli oggetti da conservare.

Il modulo MCD01 viene comunque generato e reso disponibile tramite PEC con frequenza annuale in base alla scadenza contrattuale o a fronte di variazioni e modifiche al contenuto in relazione alle informazioni citate ai punti che precedono.

2.1.2 Portale servizi

Con l'attivazione dei servizi, ENERJ fornisce ai propri clienti l'accesso al "portale servizi" che costituisce uno strumento sia informativo che di controllo dello stato dei propri servizi.

L'area informativa del portale contiene:

- istruzioni operative dettagliate in relazione ai processi di gestione delle funzionalità di JSDC,
- informazioni tecniche per l'integrazione di JSDC nei sistemi dei clienti,
- manuali e guide d'uso delle interfacce utente delle applicazioni utilizzate dai clienti nella gestione dei servizi,
- Informazioni in merito ai formati utilizzati dal sistema per rappresentare i documenti informatici e ai set minimi di metadati per l'ingresso di questi in JSDC (come approfondito nella sez. 8.3.1 Metadati,
- Le versioni più recenti del presente manuale e del piano di cessazione.

L'accesso sicuro al portale servizi è gestito tramite profili (utente/password) definiti nel sistema e indicati dal cliente (titolare degli oggetti conservati) tramite l'apposito modulo.

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;
- al Capo I, Art. 3 del Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014;
- 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.
- all'Allegato 1 al documento "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" di AGID denominato "Glossario dei termini e degli acronimi";
- All'art. 4 del GDPR (General Data Protection Regulation) EU Regulation 679/2016.

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.

3.2 Acronimi

Di seguito un elenco degli acronimi utilizzati nel testo.

Acronimo	Descrizione
AGID	Agenzia per l'Italia Digitale
CAD	Codice dell'Amministrazione Digitale
DIR	Direzione (Presidenza)
ISMS	Information Security Management System - Sistema di Gestione per la Qualità e la Sicurezza delle Informazioni
JCRM	Modulo di amministrazione dei servizi e di gestione degli utenti afferente a JSDC
JSDC	Sistema Di Conservazione di ENERJ
LLGG	Linee guida sulla formazione, gestione e conservazione dei documenti informatici
MAR	Modulo di Analisi dei Rischi
MOGC	Modello di Organizzazione, Gestione e Controllo conforme al D.Lgs. 231/2001

Acronimo	Descrizione
ODV	Organismo di Vigilanza della Società ai sensi D.Lgs. 231/2001
PAR	Procedura di Analisi dei Rischi
PCD	Procedura di gestione della Conservazione Digitale
PCE	Piano di Cessazione
PDS	Piano della Sicurezza
PEC	La casella di posta elettronica certificata: enerj@actalispec.it
PGA	Procedura di Gestione degli Audit
PGC	Procedura di Gestione dei Clienti
PM	Privacy Manager (responsabile interno della protezione dei dati)
PSS	Procedura di Sviluppo Software
RDA	Responsabile della Direzione Amministrativa e Contabile
RDP	Privacy manager (Responsabile del trattamento dei Dati Personali)
RDT	Responsabile della Direzione Tecnica
RFA	Responsabile della Funzione Archivistica
RGC	Responsabile della Gestione dei Clienti
RQS	Responsabile della gestione della Qualità e della Sicurezza delle informazioni
RSC	Responsabile del Servizio di Conservazione
RSI	Responsabile della gestione dei Sistemi Informativi
RSM	Responsabile della gestione dello Sviluppo software e Manutenzione
SDC	Sistema Di Conservazione
PDV	Pacchetto di versamento
PDA	Pacchetto di archiviazione
Pindex	Indice del pacchetto di archiviazione
PCO	Piano di Continuità Operativa
MDC	Manuale della Conservazione
MSI	Manuale della Sicurezza del Sistema Informativo

Schema 1 - Acronimi

4 NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito è riportata la normativa nazionale di riferimento ed i principali standard utilizzati nella gestione del sistema di conservazione.

4.1 Normativa nazionale

- 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 23 gennaio 2004 del Ministero delle Finanze e s.m.i. - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto;
- 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 (G.U. 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, comma 3, 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.
- Circolare Accredia 5/2017 - Schema di accreditamento degli Organismi di Certificazione per il processo di certificazione dei Conservatori a Norma, secondo le disposizioni dell'Agenzia per l'Italia Digitale.
- DECRETO-LEGGE 16 luglio 2020, n. 76 - Misure urgenti per la semplificazione e l'innovazione digitale. (G.U. Serie Generale n.178 del 16/07/2020 - S.O. n. 24)
- Determinazione n. 455/2021 del 25 giugno 2021 - Adozione del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lett. b).
- Linee guida sulla formazione, gestione e conservazione dei documenti informatici.

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 10 agosto 2018, n. 101 e s.m.i. - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- Legge 22.04.1941 n. 633, G.U. 16.07.1941 e s.m.i. - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

- Decreto Legislativo 3 aprile 2006, n. 152, G.U. n. 96 del 14/04/2006 - S.O. - Norme in materia ambientale.

4.2 Normativa europea

- Regolamento (UE) 2016/679 (General Data Protection Regulation o GDPR) del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).
- Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (eIDAS), in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

4.3 Standard internazionali

ISO/IEC

- UNI EN ISO 9000:2015 - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- UNI EN ISO 9001:2015 - Sistemi di gestione per la qualità - Requisiti;
- UNI EN ISO 9004:2018 - Gestione per la qualità - Qualità di un'organizzazione - Linee guida per conseguire il successo durevole;
- UNI EN ISO 19011:2018 - 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 31000:2018 - Gestione del rischio - Principi e linee guida;
- UNI CEI EN ISO/IEC 27000:2017 - Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Descrizione e vocabolario;
- UNI CEI EN ISO/IEC 27001:2017 - Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione – Requisiti,
    - Estensione ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services,
    - ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- UNI CEI EN ISO/IEC 27002:2017 - Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni;
- ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management;
- UNI ISO 15489-1:2016 - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- UNI ISO/TR 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 metadati del Dublin Core;
- ISO 15836-1:2017 - Information and documentation -- The Dublin Core metadata element set -- Part 1: Core elements;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;

- UNI ISO 31000 Gestione del rischio - Principi e linee guida.

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 (2015-06) - Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of operational indicators for organizations to use to benchmark their security posture;
- ETSI GS ISI 001-2 V1.1.1 (2015-06) - 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 (2015-11) - Information Security Indicators (ISI); Event Model A security event classification model and taxonomy;
- ETSI GS ISI 003 V1.1.2 (2018-01) – 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.
- 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) – Recommended Practice – CCSDS 650.0-M-2 - 2012;
- ETSI TS 119 511 V1.1.1 (2019-06) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- ETSI TS 119 512 V1.1.1 (2020-01) - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services;
- ISAD (G) - General International Standard Archival Description.

5 RUOLI E RESPONSABILITÀ

Di seguito si descrivono i ruoli aziendali principali coinvolti nel processo di conservazione: gli ulteriori ruoli presenti nell'organizzazione e i nominativi dei relativi responsabili sono specificati e mantenuti costantemente aggiornati nel modulo "Ruoli e responsabilità" (ALL04) disponibile alle parti interessati dietro richiesta.

5.1 Titolare dell'oggetto della conservazione

Il titolare dell'oggetto della conservazione è il soggetto produttore degli oggetti di conservazione. Il SDC garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dello stesso e, in ogni caso, per il tempo di attività del servizio, sulla base degli accordi contrattuali intercorrenti con il conservatore e dalla normativa vigente

Gli oggetti possono essere conservati per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

5.2 Produttore dei PDV

Il soggetto produttore dei PDV è il soggetto, di norma diversa da quello 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.

Nelle Pubbliche Amministrazioni il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PDV e assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

5.3 Utente abilitato

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 nei limiti previsti dalla legge e nelle modalità previste dal presente manuale e dagli accordi contrattuali.

5.4 Responsabile della conservazione

Il responsabile della conservazione è il soggetto che effettua la conservazione dei documenti informatici, definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia e può affidare la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali.

In ottemperanza a quanto previsto dal secondo quanto previsto dall'art. 44, comma 1-quater, del CAD, il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali e con il responsabile della sicurezza e con il responsabile dei sistemi informativi; nella PA anche con il responsabile della gestione documentale.

Nella PA, il responsabile della conservazione:

a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla PA, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

Il responsabile della conservazione:

- Definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

- provvede per le amministrazioni statali centrali e periferiche a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sul servizi affidati in outsourcing dalle PA.

5.5 Conservatore

Nelle sottosezioni che seguono si citano i ruoli interni al perimetro di JSDC, 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:

- nell'organigramma aziendale completo (ALL01)
- nel modulo Ruoli e Responsabilità. (ALL04) nel quale sono anche descritte le attività affidate ai responsabili coinvolti nella gestione del sistema di conservazione, la durata degli incarichi riferiti ai diversi profili e i riferimenti alle eventuali deleghe.

Come successivamente definito nella sezione 7.1 "Organigramma" si allega in calce al presente documento la versione anonimizzata dello stesso, il documento completo è disponibile alle parti interessate dietro motivata richiesta.

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.5.4 Privacy manager (PM)

- 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

5.5.5 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.

5.5.6 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.

6 Terze parti coinvolte

Nella presente sezione sono indicate le terze parti coinvolte nella gestione del SDC. I soggetti di cui ENERJ eventualmente si avvale per compiere operazioni che comportano il trattamento di dati personali, sono individuati come Responsabili del trattamento, nel rispetto dei requisiti previsti dall'art. 28 del Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Parti interessate	Ruolo ed ambito di competenza
Clienti privati e PA	Affidano i propri archivi informatici ai servizi di conservazione fruibili tramite il SDC.
Rivenditori/Partners	Integrano JSDC nei propri sistemi e nei sistemi proposti ai propri clienti o collaborano, a diversi livelli, alla diffusione del servizio.
Fornitori	Erogano ad ENERJ i servizi necessari per lo svolgimento dell'attività di conservatore. Il fornitore dei servizi di QTSA e' quello maggiormente coinvolto nel processo.
Autorità e Enti di controllo • Agenzia per l'Italia Digitale • Garante per la Protezione dei Dati Personali • CSQA Certificazioni • ODV (Organismo di Vigilanza) ex 231/2001 - MOGC • DPO (Responsabile della protezione dei dati)	Presidiano (anche a livello politico e legislativo) tematiche chiave o importanti sull'attività di conservatore. Svolgono attività di verifica e controllo dell'attività di ENERJ nelle tematiche della sicurezza delle informazioni, della qualità dei processi aziendali e della protezione dei dati. Certificano la compatibilità dell'attività e dei processi di ENERJ in relazione agli standard normativi necessari per l'attività di conservatore.

Schema 2 - Terze parti coinvolte

7 Struttura organizzativa per il servizio di conservazione

7.1 Organigramma

Le strutture organizzative coinvolte nel servizio di conservazione sono illustrate nell'organigramma quale appendice al MDC allegata alla specifica documentazione contrattuale.

7.2 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.

7.2.1 Attività proprie dello specifico contratto di servizio

Strutture organizzative interagenti	Attività	Figura di riferimento
• **Gestione commerciale, comunicazione e marketing** • **Gestione clienti e assistenza** • **Gestione della funzione archivistica** • **Servizi di gestione dell'archivio informatico e conservazione**	Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	RGC
• **Servizi di gestione dell'archivio informatico e conservazione** • **Gestione clienti e assistenza**	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 della funzione archivistica**	Preparazione e gestione del pacchetto di archiviazione	RSC
• **Servizi di gestione dell'archivio informatico e conservazione** • **Gestione clienti e assistenza** • **Gestione sistemi informativi**	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	RSC
• **Gestione della funzione archivistica** • **Servizi di gestione dell'archivio informatico e conservazione**	Scarto dei pacchetti di archiviazione	RSC
• **Gestione clienti e assistenza** • **Gestione commerciale, comunicazione e marketing** • **Gestione della funzione archivistica** • **Direzione amministrativa e contabile**	Chiusura del servizio di conservazione (al termine di un contratto)	RSC

Schema 3 - Attività proprie dello specifico contratto

7.2.2 Attività proprie di gestione dei sistemi informativi

Strutture organizzative interagenti	Attività	Figura di riferimento
• **Gestione sviluppo software e manutenzione** • **Gestione sistemi informativi** • **Gestione della qualità e della sicurezza delle informazioni e dei sistemi**	Conduzione e manutenzione del sistema di conservazione	RSM

Strutture organizzative interagenti	Attività	Figura di riferimento
• **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)**	Monitoraggio del sistema di conservazione	RQS
• **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**	Change management	RFA
• **Gestione della qualità e della sicurezza delle informazioni e dei sistemi** • **Gestione della funzione archivistica** • **Direzione tecnica** • **Presidenza (Responsabile del trattamento dei dati personali)**	Verifica periodica di conformità a normativa e standard di riferimento	RQS

Schema 4 - Attività proprie di gestione dei sistemi informativi

8 Oggetti sottoposti a conservazione

8.1 Premessa sulla gestione documentale e sulla formazione dei documenti informatici

Le fasi antecedenti alla conservazione sono la formazione e la gestione (cd. gestione documentale). Come descritto nelle LLGG, la conservazione dei documenti informatici rappresenta l'ultima fase del ciclo di vita dei documenti perché si limita a conferire ad essi una serie di caratteristiche tecnologiche utili alla preservazione delle caratteristiche di disponibilità, integrità e autenticità per il tempo previsto dalla normativa vigente ed in base ai rapporti contrattuali legati alla fornitura del servizio di conservazione.

ENERJ, in qualità di conservatore, non può influenzare in alcun modo la rappresentazione informatica degli oggetti formati e gestiti dal produttore: la scelta dei formati degli oggetti informatici e dei metadati da associare agli stessi è infatti vincolata dalle caratteristiche tecnologiche del sistema di gestione informatica dei documenti adottato dal produttore.

Il documento informatico è formato mediante le modalità descritte nella tabella che segue;

	Modalità di formazione	**Caratteristiche di immodificabilità e integrità**
A	creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle LLGG	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9 delle LLGG; • il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale; • versamento ad un sistema di conservazione.
B	acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9 delle LLGG; • versamento ad un sistema di conservazione.
C	memorizzazione su supporto informatico informato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;	• apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata; • registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle

	Modalità di formazione	Caratteristiche di immodificabilità e integrità
D	generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti inter-operanti, secondo una struttura logica predeterminata e memorizzata in forma statica.	basi di dati e per la produzione e conservazione dei log di sistema; • produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Schema 5 - Modalità di formazione del documento informatico

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" delle LLGG. In ogni caso è sempre possibile individuare ulteriori metadati da associare a particolari tipologie di documenti informatici.

8.2 Documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto qui di seguito specificato.

La PA forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui ai seguenti articoli del CAD:

- Art. 5 -bis "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese";
- Art. 40-bis le comunicazioni che provengono da o sono inviate a domicili digitali;
- Art. 65 Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità indicate al punto 8.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

8.3 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 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...
Registro giornaliero di Protocollo	Documenti afferenti ai registri periodici gestiti dalla PA.
Documenti di protocollo	Documenti afferenti al sistema di gestione del protocollo informatico nella PA quali (a titolo esemplificativo): mail PEC, registro di protocollo, repertori, ecc...
Atti amministrativi	Documenti formati dalla PA nella gestione ordinaria delle sue 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 PA e l'Istituto Bancario gestore del Servizio di Tesoreria.

Schema 6 - Tipologie documentali

8.3.1 Metadati

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 alle LLGG ed è definito nel contratto di servizio e negli accordi di versamento.

8.3.2 Formati

Con l'allegato 2 alle LLGG: "Formati di file e riversamento", AGID fornisce le indicazioni iniziali sui formati dei file con cui vengono rappresentati i documenti informatici oggetto di conservazione.

I formati descritti sono scelti dal titolare tra quelli che possono maggiormente garantire il principio dell'interoperabilità tra i sistemi di gestione documentale e conservazione e in base alla normativa vigente riguardante specifiche tipologie di documenti.

Il SDC, in linea con quanto indicato nell'allegato 2 al documento alle LLGG, gestisce i documenti informatici rappresentati tramite diversi formati di file.

8.3.3 Classe dei Formati

Come premesso nella sezione 8.1: "Premessa sulla gestione documentale e sulla formazione dei documenti informatici", la scelta dei formati degli oggetti informatici e dei metadati da associare agli stessi è condizionata dalle caratteristiche tecnologiche del sistema di gestione informatica dei documenti adottato dal produttore. ENERJ si limita infatti ad affiancare il soggetto produttore fornendo la necessaria consulenza e gli appropriati strumenti tecnici a supporto.

Coerentemente con il contenuto dell'allegato 2 alle LLGG e allo scopo di definire correttamente i livelli ed i limiti di responsabilità di ENERJ nella garanzia di mantenimento delle caratteristiche di fruibilità ed interoperabilità degli oggetti conservati, questi ultimi sono censiti all'ingresso nel sistema di conservazione in tre categorie o "classi":

- **Classe A**

  Oggetto con formato previsto nell'Allegato 2 delle LLGG. In questo caso il CONSERVATORE garantisce la leggibilità, ma visto che, così come indicato a pag. 3 del citato documento "non tutti i formati di file nel presente documento sono leggibili da qualsivoglia elaboratore, a seconda della configurazione degli applicativi installati", rimane nella responsabilità del Titolare del documento conservare copia dei software necessari e relative licenze per corretta fruizione dell'oggetto conservato.

- **Classe B**

  Oggetto con formato previsto ma sconsigliato, nell'Allegato 2 delle LLGG oppure non presenti nell'Allegato 2 ma per i quali è stata richiesta la conservazione.

  Per gli oggetti di questa fattispecie non è assicurata la corretta conservazione, gli stessi sono comunque archiviati dal sistema in attesa di azioni di adeguamento promosse e concordate dal titolare.

- **Classe C**

  Oggetto con formato non previsto nell'Allegato 2 delle LLGG e sconosciuto al sistema di conservazione. In questo caso il CONSERVATORE non garantisce la leggibilità. Sono esempi: documenti con formato sconosciuto, dichiarato "UNKNOWN" ed estensione qualsiasi, anche se inseriti in buste crittografiche. Per gli oggetti di questa fattispecie non è assicurata la corretta

conservazione, gli stessi sono comunque archiviati dal sistema in attesa di azioni di adeguamento promosse e concordate dal titolare.

Nella tabella che segue sono elencati e descritti i principali formati specificano l'attribuzione della classe

CODIFICA	DESCRIZIONE	CLASSE	MIME TYPE	ESTENSIONI
7-ZIP	7-Zip compressed archive format	A	{application/x-7z-compressed}	{.7z}
ACCESS 2007	Microsoft Access Connectivity Engine	B	{application/msaccess}	{.accdb}
ACES	Academy Color Encoding System	A	{application/mxf,image/exr,application/mxf,image/exr,application/mxf,image/exr,application/mxf,image/exr}	{.exr,.mxf,.amf,.clf}
AIFF	Audio Interchange	B	{audio/aiff,audio/aiff,audio/aiff}	{.aiff,.aifc,.aif}
AMF	ACES Metadata	A	{application/amf+xml}	{.amf}
ARRIRAW	Aristotele Audio	B	{image/arriraw}	{.ari}
ASSERZIONE SPID	Asserzione Spid	A	{text/xml}	{.xml}
AVI	Advanced Video Interleave	B	{video/msvideo,video/avi}	{.avi,.avi}
CDA2	Clinical Document Architecture	A	{application/xml}	{.xml}
CINEMADNG	Adobe CinemaDNG	B	{video/x-adobe-dng,video/x-adobe-dng}	{.dng,.wav}
CSS	Cascaded Style Sheet	A	{text/css}	{.css}
CSV	Comma-Separated Value	A	{text/csv}	{.csv}
D.I. BASATO SU DPX	Digital Intermediate	B	{sound/wav,image/x-dpx,sound/wav,image/x-dpx}	{.wav,.dpx}
D.I. BASATO SU EXR	Digital Intermediate	A	{sound/wav,image/exr,sound/wav,image/exr}	{.exr,.exr,.wav,.wav}
DCDM	Digital Cinema Distribution Master	A	{image/tiff,sound/wav,image/tiff,sound/wav,image/tiff,sound/wav}	{.wav,.tif,.tiff}
DCP	Digital Cinema Package	B	{application/xml,application/mxf,application/xml,application/mxf}	{.mxf,.xml}
DICOM	Digital Imaging and Communications in Medicine	A	{image/dicom}	{.zip}
DMG	Apple Disk Image	B	{application/x-apple-diskimage}	{.dmg}
DNG	Adobe Digital Negative	B	{image/x-adobe-dng}	{.dng}
DPX	Digital Picture	B	{image/x-dpx}	{.dpx}
DWF	AutoCAD Design	B	{image/dwf,drawing/dwf,model/vnd.dwf,image/dwf,drawing/dwf,model/vnd.dwf}	{.dwfx,.dwf}
DWG	AutoCAD Drawing	A	{image/vnd.dwg,application/acad,image/vnd.dwg,application/acad}	{.dwg,.dwt}
DXF	AutoCAD Drawing Interchange	B	{image/vnd.dxf}	{.dxf}
EBU-TT	Timed Text	B	{application/ttml+xml}	{.xml}
EML	Electronic Mail	A	{application/email}	{.eml}
ENCAPSULATED POSTSCRIPT	Encapsulated PostScript	B	{application/eps,image/eps}	{.eps,.eps}
EPUB	Electronic Publication	B	{application/epub+zip}	{.epub}
EXCEL 2007	Microsoft Excel	A	{application/vnd.openxmlformats-officedocument.spreadsheetml.sheet,applic	{.xlsx,.xltx}

CODIFICA	DESCRIZIONE	CLASSE	MIME TYPE	ESTENSIONI
			ation/vnd.openxmlformats-officedocument.spreadsheetml.sheet}	
EXR	OpenEXR	A	{image/x-exr}	{.exr}
FATTURAPA	Fattura Elettronica	A	{application/xml}	{.xml}
FBX	Autodesk FBX	A	{model/vnd.fbx}	{.fbx}
FLAC	Free Lossless Audio Codec	A	{audio/flac}	{.flac}
GIF	Graphic Image file Format	B	{image/gif}	{.gif}
GZIP	Gnu Zip	A	{application/gzip}	{.gzip}
HTML	Hypertext Markup Language	A	{text/html,text/html}	{.html,.htm}
ILLUSTRATOR	Adobe Illustrator	B	{application/illustrator}	{.ai}
IMF	Interoperable Master	A	{application/xml,application/mxf,application/xml,application/mxf}	{.mxf,.xml}
IMSC1	Timed Text Markup Language	A	{application/ttml+xml}	{.ttml}
INDESIGNML	Adobe InDesign	B	{application/x-indesign+xml}	{.idml}
ISO	Immagine di volume	A	{application/x-iso9660-image}	{.iso}
JAR	Java Archive	A	{application/jar-archive}	{.jar}
JPEG	Joint Photographic Experts Group	A	{image/jpeg,image/jpg,image/jpeg,image/jpg}	{.jpg,.jpeg}
JPEG2000	Joint Photographic Experts Group 2000	B	{image/jp2}	{.jp2}
JSON	JavaScript Object Notation	A	{application/json}	{.json}
JSON-LD	JSON Linked Data	A	{application/ld+json}	{.jsonld}
KDM	Key Delivery Message	B	{application/kdm+xml,application/kdm+xml}	{.xml,.kdm}
LATEX	LaTex	B	{application/x-tex}	{.tex}
LOG	File di registro	B	{text/plain,text/plain}	{.log,.txt}
M7M	M7M	C	{application/pkcs7-mime}	{.m7m}
MARKDOWN	Markdown Documentation	A	{text/markdown}	{.md}
MATHML	Mathematical Markup Language	A	{text/mathml-renderer,text/mathml,text/mathml-renderer,text/mathml}	{.xml,.mml}
MATROSKA	Matroska File	B	{audio/x-matroska,video/x-matroska,audio/x-matroska,video/x-matroska,audio/x-matroska,video/x-matroska,audio/x-matroska,video/x-matroska}	{.mkv,.mka,.mks,.mk3d}
MBOX	MBox	A	{application/mbox}	{.mbox}
MIDI	Musical Instrument	A	{application/x-midi,audio/midi,application/x-midi,audio/midi}	{.mid,.midi}
MP3	MPEG-3	B	{audio/mpeg}	{.mp3}
MP4	MPEG-4	A	{audio/mp4,video/mp4,audio/mp4,video/mp4,audio/mp4,video/mp4}	{.mp4,.m4a,.m4v}

CODIFICA	DESCRIZIONE	CLASSE	MIME TYPE	ESTENSIONI
MPEG2-PS	MPEG-2 Program Stream	B	{video/MP2P,video/MP2P,video/MP2P,video/MP2P}	{.mpg,.mpeg,.vob,.m2p}
MPEG2-TS	MPEG-2 Transport Stream	B	{video/MP2T,video/MP2T}	{.ts,.m2ts}
MS-DOC	Microsoft Word Binary File Format	B	{application/msword,application/msword}	{.doc,.dot}
MS-MDB	Microsoft Access Binary file	B	{application/msaccess}	{.mdb}
MS-MSG	Microsoft Outlook Item	B	{application/vnd.ms-outlook}	{.msg}
MS-PPT	Microsoft PowerPoint Binary	B	{application/vnd.ms-powerpoint}	{.ppt}
MS-PST	Microsoft Outlook	B	{application/vnd.ms-outlook}	{.pst}
MS-XLS	Microsoft Excel Binary	B	{application/vnd.ms-excel}	{.xls}
MUSICXML	MusicXml	A	{application/vnd.recordare.musicxml}	{.musicxml}
MXF	Material Exchange	A	{application/mxf}	{.mxf}
ODB	Open Document for Database	B	{application/vnd.oasis.opendocument.database}	{.odb}
ODG	Open Document for Applications	B	{application/vnd.oasis.opendocument.graphics}	{.odg}
ODP	Open Document for Presentations	A	{application/vnd.oasis.opendocument.presentation}	{.odp}
ODS	Open Document for Office Spreadsheets	A	{application/vnd.oasis.opendocument.spreadsheet}	{.ods}
ODT	Open Document Text	A	{application/vnd.oasis.opendocument.text}	{.odt}
OGG	Ogg encapsulated	B	{application/ogg,video/ogg,audio/ogg,application/ogg,video/ogg,audio/ogg,application/ogg,video/ogg,audio/ogg}	{.ogg,.oga,.ogv}
OPENDOCUMENT	Open Document	A	{application/vnd.oasis.opendocument.formula,application/vnd.oasis.opendocument.image,application/vnd.oasis.opendocument.text,application/vnd.oasis.opendocument.spreadsheet,application/vnd.oasis.opendocument.presentation,application/vnd.oasis.opendocument.graphics,application/vnd.oasis.opendocument.database,application}	{.odb,.odg,.odp,.ods,.odt,.odi,.odf}
OPENTYPE	OpenType	A	{application/x-font-otf,font/otf}	{.otf,.otf}
P7M	P7M	C	{application/pkcs7-mime}	{.p7m}
PDF	Portable Document Format	A	{application/pdf}	{.pdf}
PNG	Portable Network Graphics	A	{image/png}	{.png}
POSTSCRIPT	Adobe PostScript	B	{application/postscript}	{.ps}
POWERPOINT 2007	Microsoft PowerPoint	A	{application/vnd.openxmlformats-officedocument.presentationml.presentation,application/vnd.openxmlformats-officedocument.presentationml.presentation,application/vnd.openxmlformats-officedocument.presentationml.presentation}	{.pptx,.ppsx,.potx}
PSD	Adobe Photoshop	B	{image/x-psd}	{.psd}
QUICKTIME	Apple Quick Time	B	{video/quicktime,video/quicktime}	{.mov,.qt}

CODIFICA	DESCRIZIONE	CLASSE	MIME TYPE	ESTENSIONI
RAR	Roshal Archive	B	{application/java-archive}	{.rar}
RAW	Raw	A	{audio/basic,audio/basic,audio/basic}	{.pcm,.raw,.sam}
RICHTEXT	Rich Text Format	B	{application/rtf,text/rtf}	{.rtf,.rtf}
SEGNATURA DI PROTOCOLLO	Segnatura di protocollo	A	{application/xml}	{.xml}
SQL	Structured Query	A	{application/sql}	{.sql}
STL	Stereolithography	B	{model/x.stl-ascii|binary,model/stl}	{.stl,.stl}
SVG	Scalable Vector Graphics	A	{image/svg+xml+zip,image/svg+xml,image/svg+xml+zip,image/svg+xml}	{.svg,.svg,.svgz,.svgz}
TAR	Tape Archive	A	{application/x-tar}	{.tar}
TEXT	Testo	B	{text/plain,text/plain}	{.txt,.text}
TIFF	Tagged Image	A	{image/tiff,image/tiff}	{.tif,.tiff}
TRUETYPE	TrueType	A	{application/x-font-ttf,font/ttf}	{.ttf}
TSD	TSD	C	{application/timestamped-data}	{.tsd}
TSR	TSR	B	{application/timestamp-resply}	{.tsr}
TST	TST	B	{application/timestamp-token}	{.tst}
TTML	Internet Media Subtitles and Captions	A	{application/ttml+xml}	{.ttml}
UNKNOWN	Formato file sconosciuto	C	{application/octet-stream}	{*}
VMDK	Virtual Machine Disk	A	{application/x-vmdk}	{.vmdk}
WAV	Waveform File	A	{audio/wave,audio/wave,audio/wave}	{.wav,.bwf,.rf64}
WEBM	WebM	B	{audio/webm,video/webm,audio/webm,video/webm}	{.webm,.weba}
WOFF	Web Open Font	A	{application/font-woff,font/woff2,application/font-woff,font/woff2}	{.woff2,.woff}
WORD 2007	WordProcessingMLOOXMLExtension	A	{application/vnd.openxmlformats-officedocument.wordprocessingml.document,application/vnd.openxmlformats-officedocument.wordprocessingml.document}	{.docx,.dotx}
XDCAM	Material Exchange	B	{application/xml,application/mxf,application/xml,application/mxf}	{.mxf,.mxf,.xml}
XHTML	Extensible Hypertext Markup Language	B	{application/xhtml+xml,application/xhtml+xml}	{.html,.xhtml}
XML	Extensible Markup Language	A	{application/xml,text/xml}	{.xml}
XSD	XML Schema Definition	A	{application/xml}	{.xsd}
XSL	Extensible Stylesheet Language	A	{text/xsl}	{.xsl}
XSLT	Extensible Stylesheet Language Transformations	A	{application/xslt+xml,text/xml}	{.xslt}
ZIP	Zip	A	{application/zip,application/zip}	{.zip,.zipx}

Schema 7 - Classificazione dei formati

8.4 Pacchetti informativi

Per attuare il processo di conservazione, gli oggetti informatici da conservare sono raggruppati all'interno di strutture denominate pacchetti informativi che prendono il nome di pacchetti di versamento nella fase in cui sono trasferiti dal soggetto produttore ad ENERJ che li sottopone quindi al processo di conservazione.

8.4.1 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:

- appositi web-services,
- trasmissione telematica tramite canale sicuro,
- interfaccia web-based e mediante una azione di "upload" dei documenti informatici,
- software e sistemi sviluppati da partner di ENERJ.

Il PDV, eventualmente integrato da ulteriori informazioni concordate con il cliente, viene trasferito dal produttore al SDC 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.

Il PDV è rappresentato da un file in formato XML contenente le informazioni iniziali attribuite al pacchetto informativo prima del trasferimento al SDC, A titolo di esempio riportiamo, di seguito, un tracciato XML di un PDV.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><sincro:PIndex xmlns:sincro="http://www.uni.com/U3011/sincro-v2/"
sincro:language="it" sincro:sincroVersion="2.0" sincro:uri="http://www.uni.com/U3011/sincrov2/PIndex.xsd">
 <sincro:SelfDescription>
  <sincro:ID sincro:scheme="local">6ee58b16-0fc5-40a1-8a7d-ba21305b1247</sincro:ID>
  <sincro:CreatingApplication>
   <sincro:Name>Enerj.CDV.ControlsService</sincro:Name>
   <sincro:Version>4.2.0.0</sincro:Version>
   <sincro:Producer>Enerj srl</sincro:Producer>
  </sincro:CreatingApplication>
 </sincro:SelfDescription>
 <sincro:PVolume>
  <sincro:ID sincro:scheme="local">f2780aca-4da5-42e2-b182-9af64a3dded6</sincro:ID>
  <sincro:Description>Indice Pacchetto di Versamento per il PDV 217894</sincro:Description>
 </sincro:PVolume>
 <sincro:FileGroup>
  <sincro:ID sincro:scheme="local">8f2da6f3-4846-45d7-a677-c7ac3a89a85b</sincro:ID>
  <sincro:Description>Elenco documenti per il PDV 217894</sincro:Description>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915777</sincro:ID>
   <sincro:Path>..\Data\0008915777.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
```

```
      <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
        <sincro:ID sincro:scheme="local">0008915777.xml</sincro:ID>
        <sincro:Path>..\Meta\0008915777.xml</sincro:Path>
        <sincro:Hash                                                    sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
      </sincro:ExternalMetadata>
    </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
    <sincro:ID sincro:scheme="local">8915778</sincro:ID>
    <sincro:Path>..\Data\0008915778.pdf</sincro:Path>
    <sincro:Hash                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
    <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
      <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
        <sincro:ID sincro:scheme="local">0008915778.xml</sincro:ID>
        <sincro:Path>..\Meta\0008915778.xml</sincro:Path>
        <sincro:Hash                                                    sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
      </sincro:ExternalMetadata>
    </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
    <sincro:ID sincro:scheme="local">8915779</sincro:ID>
    <sincro:Path>..\Data\0008915779.pdf</sincro:Path>
    <sincro:Hash                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
    <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
      <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
        <sincro:ID sincro:scheme="local">0008915779.xml</sincro:ID>
        <sincro:Path>..\Meta\0008915779.xml</sincro:Path>
        <sincro:Hash                                                    sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
      </sincro:ExternalMetadata>
    </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
    <sincro:ID sincro:scheme="local">8915780</sincro:ID>
    <sincro:Path>..\Data\0008915780.pdf</sincro:Path>
    <sincro:Hash                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
    <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
      <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
        <sincro:ID sincro:scheme="local">0008915780.xml</sincro:ID>
        <sincro:Path>..\Meta\0008915780.xml</sincro:Path>
        <sincro:Hash                                                    sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
      </sincro:ExternalMetadata>
    </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
    <sincro:ID sincro:scheme="local">8915781</sincro:ID>
    <sincro:Path>..\Data\0008915781.pdf</sincro:Path>
    <sincro:Hash                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
    <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
      <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
        <sincro:ID sincro:scheme="local">0008915781.xml</sincro:ID>
        <sincro:Path>..\Meta\0008915781.xml</sincro:Path>
        <sincro:Hash                                                    sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
      </sincro:ExternalMetadata>
```

```
  </sincro:MoreInfo>
 </sincro:File>
</sincro:FileGroup>
<sincro:Process>
 <sincro:Submitter sincro:agentType="natural person">
  <sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-RSSMRA80A01F205X</sincro:AgentID>
  <sincro:AgentName>
   <sincro:NameAndSurname>
    <sincro:FirstName>Mario</sincro:FirstName>
    <sincro:LastName>Rossi</sincro:LastName>
   </sincro:NameAndSurname>
  </sincro:AgentName>
  <sincro:RelevantDocument>manuale.pdf</sincro:RelevantDocument>
 </sincro:Submitter>
 <sincro:Holder sincro:agentType="legal person" sincro:holderRole="soggetto produttore">
  <sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">VATIT-61253760419</sincro:AgentID>
  <sincro:AgentName>
   <sincro:FormalName>Alfa S.P.A.</sincro:FormalName>
  </sincro:AgentName>
  <sincro:RelevantDocument>manuale.pdf</sincro:RelevantDocument>
 </sincro:Holder>
 <sincro:AuthorizedSigner sincro:agentType="natural person" sincro:signerRole="PreservationManager">
  <sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-RSSMRA80A01F205X</sincro:AgentID>
  <sincro:AgentName>
   <sincro:NameAndSurname>
    <sincro:FirstName>Giuseppe</sincro:FirstName>
    <sincro:LastName>Verdi</sincro:LastName>
   </sincro:NameAndSurname>
  </sincro:AgentName>
  <sincro:RelevantDocument>manuale_conservazione_enerj.pdf</sincro:RelevantDocument>
 </sincro:AuthorizedSigner>
 <sincro:TimeReference>
  <sincro:TimeInfo sincro:attachedTimeStamp="false">2022-03-07T17:47:43.9392206+01:00</sincro:TimeInfo>
 </sincro:TimeReference>
</sincro:Process>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signer-T-
1646671664176"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-
c14n11#WithComments"/><ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/><ds:Reference Id="r-doc-Signer-T-1646671664176" URI=""><ds:Transforms><ds:Transform
Algorithm="http://www.w3.org/2002/06/xmldsig-filter2"><XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2"
Filter="subtract">/descendant::ds:Signature</XPath></ds:Transform></ds:Transforms><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>8L+ypEBP0A4HFH9PVo3xFsiNb21JLO1F5ooOS4k851
Q=</ds:DigestValue></ds:Reference><ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties-
Signer-T-1646671664176"><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>jwpJDbj/4ZzpnogWW2JBSQQKK6XXx/EdigrqVbC5e1
M=</ds:DigestValue></ds:Reference><ds:Reference Id="r-keyinfo-Signer-T-1646671664176" URI="#KeyInfo-Signer-T-
1646671664176"><ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>O8B4KF0uZTkoYU/RQ7Hdf3RsDfAG6f34UqirfJatK5M
=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue Id="SignatureValue-Signer-T-
1646671664176">mINVsIBM8kCN/ZePUXamNPNoQo4/TqM0d5LpEyS4zR86I02ODDg25Ycw4NCvnKkrGCkZJA9ZL0s2
kZaAHS3KV+K3eoNo/kcuE4W+EtwK7/snXPhoLEjyYPe6LeSZwGMBFQb5Rk+EmdYAfxv0AEkw7HSS
BOz7/H0EhTx9+L6Xt6/2xpEtrMRXDPDNP6wVvz+YTdPKZBu64H1o93x3tlMF4pDtMJ2NJr2QhvPF
47w6y+85qxAF8TYbtGTFLVdeH5/LBUtjEU5r6Hp654c1CqT7t50DbFy/jwDMxDJCBFL6GVxybRyA
T9MzDNj5I5CP5GkJM0aXfFQe/Q+itgpj5wUgsw==</ds:SignatureValue><ds:KeyInfo Id="KeyInfo-Signer-T-
1646671664176"><ds:X509Data><ds:X509Certificate>MIIHHjCCB…Mbbj5e
lNk=</ds:X509Certificate></ds:X509Data></ds:KeyInfo><ds:Object><xades:QualifyingProperties
xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signer-T-1646671664176">
<xades:SignedProperties Id="SignedProperties-Signer-T-1646671664176">
<xades:SignedSignatureProperties>
<xades:SigningTime>2022-03-07T17:47:44+01:00</xades:SigningTime>
<xades:SigningCertificate>
<xades:Cert>
```

<xades:CertDigest>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>YtM0pQn4c2Qv0WK1u0+aHvnPsuTEilLICs32WdWSuoQ=</ds:DigestValue>
</xades:CertDigest>
<xades:IssuerSerial><ds:X509IssuerName>CN=ArubaPEC EU Qualified Certificates CA G1,OU=Qualified Trust Service Provider,2.5.4.97=#0c1156415449542d303138373930323035313 7,O=ArubaPEC S.p.A.,L=Arezzo,C=IT</ds:X509IssuerName><ds:X509SerialNumber>4751737777607465657</ds:X509SerialNumber></xades:IssuerSerial>
</xades:Cert>
</xades:SigningCertificate>
</xades:SignedSignatureProperties>
<xades:SignedDataObjectProperties>
<xades:DataObjectFormat ObjectReference="#r-doc-Signer-T-1646671664176">
<xades:MimeType>text/xml</xades:MimeType>
</xades:DataObjectFormat>
<xades:DataObjectFormat ObjectReference="#r-keyinfo-Signer-T-1646671664176">
<xades:MimeType>text/xml</xades:MimeType>
</xades:DataObjectFormat>
</xades:SignedDataObjectProperties>
</xades:SignedProperties>
</xades:QualifyingProperties></ds:Object></ds:Signature></sincro:PIndex>

Schema 8 - Esempio di contenuto del PDV

8.4.2 Pacchetto di archiviazione

Il PDA viene formato secondo le regole tecniche definite nella norma UNI 11386:2020 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali) e secondo le modalità riportate nel presente manuale.

Ad ogni PDA generato dal SDC viene associato un file denominato PIndex (Preservation Index) in formato XML che contiene gli identificatori univoci, le impronte informatiche dei documenti contenuti nel PDA e tutto l'insieme di informazioni richieste dalla norma per la rappresentazione dell'indice del pacchetto di archiviazione, tra le informazioni più rilevanti che il sistema di conservazione gestisce, in relazione ad ogni PDA prodotto, si citano a titolo esemplificativo:

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale , Codice Fiscale, Partita IVA, ...);
- Identificativo univoco del PIndex 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;

Di seguito si riporta un esempio del contenuto di un file PIndex generato dal SDC:


```
<?xml version="1.0" encoding="utf-8" standalone="no"?><sincro:PIndex xmlns:sincro="http://www.uni.com/U3011/sincro-v2/"
sincro:language="it" sincro:sincroVersion="2.0" sincro:uri="http://www.uni.com/U3011/sincrov2/PIndex.xsd">
 <sincro:SelfDescription>
  <sincro:ID sincro:scheme="local">cc0db1df-6505-457a-bc0b-9262b67b6ee0</sincro:ID>
  <sincro:CreatingApplication>
   <sincro:Name>Enerj.CDV.ControlsService</sincro:Name>
   <sincro:Version>4.2.0.0</sincro:Version>
   <sincro:Producer>Enerj srl</sincro:Producer>
  </sincro:CreatingApplication>
 </sincro:SelfDescription>
 <sincro:PVolume>
  <sincro:ID sincro:scheme="local">9977064a-0f20-4ef0-98cb-bd2e39a8906a</sincro:ID>
  <sincro:Description>Indice del Pacchetto di Archiviazione per il PDV 217894</sincro:Description>
 </sincro:PVolume>
 <sincro:FileGroup>
  <sincro:ID sincro:scheme="local">8be7067b-c44e-4c81-87d2-15041a2c441b</sincro:ID>
  <sincro:Description>Elenco documenti per il PDV 217894</sincro:Description>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915777</sincro:ID>
   <sincro:Path>.\Data\0008915777.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
    <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
     <sincro:ID sincro:scheme="local">0008915777.xml</sincro:ID>
     <sincro:Path>.\Meta\0008915777.xml</sincro:Path>
     <sincro:Hash                                                                  sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
    </sincro:ExternalMetadata>
   </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915778</sincro:ID>
   <sincro:Path>.\Data\0008915778.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
    <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
     <sincro:ID sincro:scheme="local">0008915778.xml</sincro:ID>
     <sincro:Path>.\Meta\0008915778.xml</sincro:Path>
     <sincro:Hash                                                                  sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
    </sincro:ExternalMetadata>
   </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915779</sincro:ID>
   <sincro:Path>.\Data\0008915779.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
    <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
     <sincro:ID sincro:scheme="local">0008915779.xml</sincro:ID>
     <sincro:Path>.\Meta\0008915779.xml</sincro:Path>
     <sincro:Hash                                                                  sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
    </sincro:ExternalMetadata>
   </sincro:MoreInfo>
```

```
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915780</sincro:ID>
   <sincro:Path>.\Data\0008915780.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
    <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
     <sincro:ID sincro:scheme="local">0008915780.xml</sincro:ID>
     <sincro:Path>.\Meta\0008915780.xml</sincro:Path>
     <sincro:Hash                                                                  sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
    </sincro:ExternalMetadata>
   </sincro:MoreInfo>
  </sincro:File>
  <sincro:File sincro:encoding="binary" sincro:extension=".pdf" sincro:format="application/pdf">
   <sincro:ID sincro:scheme="local">8915781</sincro:ID>
   <sincro:Path>.\Data\0008915781.pdf</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">8B4ED660699A7AFF0806CFBBBF78A6588C594F32C60DE5046BB0E0E83EB755B3</sincro:Hash>
   <sincro:MoreInfo sincro:xmlSchema="http://sdc-pre-app01:802/XSD/metadata_doc_info.xsd">
    <sincro:ExternalMetadata sincro:encoding="binary" sincro:format="application/xml; charset=UTF-8">
     <sincro:ID sincro:scheme="local">0008915781.xml</sincro:ID>
     <sincro:Path>.\Meta\0008915781.xml</sincro:Path>
     <sincro:Hash                                                                  sincro:hashFunction="SHA-
256">F9AB9FBD9487E9F3A50FCF75A9F7B2F1807C2DDC8C6125D11D60EF8750385368</sincro:Hash>
    </sincro:ExternalMetadata>
   </sincro:MoreInfo>
  </sincro:File>
 </sincro:FileGroup>
 <sincro:FileGroup>
  <sincro:ID sincro:scheme="local">e7f1c15d-4355-416f-9239-3f33f50cc1cd</sincro:ID>
  <sincro:Description>Indice del Pacchetto di Versamento per il PDV 217894</sincro:Description>
  <sincro:File sincro:encoding="binary" sincro:extension="xml" sincro:format="application/xml text/xml; charset=UTF-8">
   <sincro:ID sincro:scheme="local">f2780aca-4da5-42e2-b182-9af64a3dded6</sincro:ID>
   <sincro:Path>.\Versamento\f2780aca-4da5-42e2-b182-9af64a3dded6_20220307_1747_217894_IPdV.xml</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">F1668FDFF9C300C32E718A2D2B9E5943E83FF599D54C7CD74CE50023DEE5359D</sincro:Hash>
  </sincro:File>
 </sincro:FileGroup>
 <sincro:FileGroup>
  <sincro:ID sincro:scheme="local">3fbbcce6-54a0-4435-8cc7-b115b4b8f780</sincro:ID>
  <sincro:Description>Rapporto di Versamento per il PDV 217894</sincro:Description>
  <sincro:File sincro:encoding="binary" sincro:extension="xml" sincro:format="application/xml text/xml; charset=UTF-8">
   <sincro:ID sincro:scheme="local">ce5c2033-76d5-4f99-9818-00a40d643335</sincro:ID>
   <sincro:Path>.\Versamento\ce5c2033-76d5-4f99-9818-00a40d643335_20220307_1747_217894_RdV.xml</sincro:Path>
   <sincro:Hash                                                                    sincro:hashFunction="SHA-
256">76BACE9662C52FBFF5EC44537C98CF4A4FA0FA6EBCBCCA34150305544DF13728</sincro:Hash>
  </sincro:File>
 </sincro:FileGroup>
 <sincro:Process>
  <sincro:Submitter sincro:agentType="natural person">
   <sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-RSSMRA80A01F205X</sincro:AgentID>
   <sincro:AgentName>
    <sincro:NameAndSurname>
     <sincro:FirstName>Mario</sincro:FirstName>
     <sincro:LastName>Rossi</sincro:LastName>
    </sincro:NameAndSurname>
   </sincro:AgentName>
   <sincro:RelevantDocument>manuale.pdf</sincro:RelevantDocument>
  </sincro:Submitter>
  <sincro:Holder sincro:agentType="legal person" sincro:holderRole="soggetto produttore">
```

<sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">VATIT-61253760419</sincro:AgentID>
<sincro:AgentName>
<sincro:FormalName>Alfa S.P.A.</sincro:FormalName>
</sincro:AgentName>
<sincro:RelevantDocument>manuale.pdf</sincro:RelevantDocument>
</sincro:Holder>
<sincro:AuthorizedSigner sincro:agentType="natural person" sincro:signerRole="PreservationManager">
<sincro:AgentID sincro:nameRegistrationAuthority="Agenzia delle Entrate">TINIT-RSSMRA80A01F205X</sincro:AgentID>
<sincro:AgentName>
<sincro:NameAndSurname>
<sincro:FirstName>Giuseppe</sincro:FirstName>
<sincro:LastName>Verdi</sincro:LastName>
</sincro:NameAndSurname>
</sincro:AgentName>
<sincro:RelevantDocument>manuale_conservazione_enerj.pdf</sincro:RelevantDocument>
</sincro:AuthorizedSigner>
<sincro:TimeReference>
<sincro:TimeInfo sincro:attachedTimeStamp="false">2022-03-07T17:47:44.9252806+01:00</sincro:TimeInfo>
</sincro:TimeReference>
</sincro:Process>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="Signer-T-1646671665027"><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11#WithComments"/><ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference Id="r-doc-Signer-T-1646671665027" URI=""><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2"><XPath xmlns="http://www.w3.org/2002/06/xmldsig-filter2" Filter="subtract">/descendant::ds:Signature</XPath></ds:Transform></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>vLpUBf0zH3WUkSpSRJjiTEERoe+tMj42BoHaVXY+eGM=</ds:DigestValue></ds:Reference><ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#SignedProperties-Signer-T-1646671665027"><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>ZRDV680Do1v8EmE6SAXRYq+tZG8zIhLirxnldniWR10=</ds:DigestValue></ds:Reference><ds:Reference Id="r-keyinfo-Signer-T-1646671665027" URI="#KeyInfo-Signer-T-1646671665027"><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>Q/clwaY/zP26/0pExOnAdtbRUQ38s2Qf+H4SAZPbEiA=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue Id="SignatureValue-Signer-T-1646671665027">oQTOgTWCVQDydspplr62lZzBBO+v2/G3mzXiCgVJyFtZiIGqL0Zjr8cTkAFX5XcqTWLlCZz5ZPSr
pIGPTMISKaanqDt6Wmwhm4jy7Rpo2ZBWSOT2MGlmhXH+gqNLKtJ0xS8s24yUTnZFtdu9GlwSCSdD
LQOIQy6JTQGUstvSsAvXqixViQ0PgZkQtqN45acI2A1v8KE5E08lDO4LpI7QvtAsmeTviU+iJu2J
QBhgmNO96okb8WpIpcD+CA9lPrcqVh7GMVzpSfY7iBCc+S73aUkeszFIOUZ9Qnldk3YUiODhcatB
7esFXdPJXn7IE9DDdpcIVONMTBt5BZ+9yRYnGw==</ds:SignatureValue><ds:KeyInfo Id="KeyInfo-Signer-T-1646671665027"><ds:X509Data><ds:X509Certificate>MIIHHj… Mbbj5e
lNk=</ds:X509Certificate></ds:X509Data></ds:KeyInfo><ds:Object><xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" Target="#Signer-T-1646671665027">
<xades:SignedProperties Id="SignedProperties-Signer-T-1646671665027">
<xades:SignedSignatureProperties>
<xades:SigningTime>2022-03-07T17:47:45+01:00</xades:SigningTime>
<xades:SigningCertificate>
<xades:Cert>
<xades:CertDigest>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>YtM0pQn4c2Qv0WK1u0+aHvnPsuTEilLICs32WdWSuoQ=</ds:DigestValue>
</xades:CertDigest>
<xades:IssuerSerial><ds:X509IssuerName>CN=ArubaPEC EU Qualified Certificates CA G1,OU=Qualified Trust Service Provider,2.5.4.97=#0c1156415449542d303138373930230353137,O=ArubaPEC S.p.A.,L=Arezzo,C=IT</ds:X509IssuerName><ds:X509SerialNumber>4751737777607465657</ds:X509SerialNumber></xades:IssuerSerial>
</xades:Cert>
</xades:SigningCertificate>
</xades:SignedSignatureProperties>
<xades:SignedDataObjectProperties>
<xades:DataObjectFormat ObjectReference="#r-doc-Signer-T-1646671665027">
<xades:MimeType>text/xml</xades:MimeType>
</xades:DataObjectFormat>

<xades:DataObjectFormat ObjectReference="#r-keyinfo-Signer-T-1646671665027">
<xades:MimeType>text/xml</xades:MimeType>
</xades:DataObjectFormat>
</xades:SignedDataObjectProperties>
</xades:SignedProperties>
</xades:QualifyingProperties></ds:Object></ds:Signature></sincro:PIndex>

Schema 9 - Esempio del contenuto del filePindex

E' importante specificare in particolare la gestione di base che JSDC effettua sulla sezione della struttura informativa denominata: "Agent" ossia sulle seguenti caratteristiche:

- **Submitter**, ossia il soggetto che effettua il trasferimento fisico degli oggetti digitali nel sistema di conservazione: JSDC indica la ragione sociale del produttore (può essere sia persona fisica che giuridica).
- **Holder**, il soggetto produttore o proprietario, possessore o detentore degli oggetti digitali trasferiti nel sistema di conservazione. JSDC riporta in questo campo la ragione sociale del cliente del servizio come censita negli accordi contrattuali
    - Attributo HolderRole (obbligatorio), valori ammessi: "soggetto produttore", "soggetto proprietario", "soggetto possessore", "soggetto detentore", JSDC di base attribuisce a questo campo il valore: "soggetto produttore".

    NOTA: Nella norma viene raccomandato di utilizzare il valore "soggetto produttore" se il soggetto che trasferisce gli oggetti digitali in conservazione è il soggetto che ha creato, accumulato e organizzato gli stessi nello svolgimento della propria attività. Negli altri casi, utilizzare uno degli altri valori ammessi, come opportuno.
- **AuthorizedSigner** cioè il soggetto autorizzato ad apporre la firma elettronica (avanzata o qualificata) o il sigillo elettronico (avanzato o qualificato) sull'indice di conservazione, a conclusione del processo di creazione dell'indice: Nel primo caso JSDC riporta in questo campo il nome e cognome del RSC che sottoscrive il file PIndex con la propria firma digitale.
- **RelevantDocument** è una caratteristica indicata nella norma come riferimento a un documento rilevante ai fini del processo di conservazione: JSDC riporta in questo caso il nome del documento informatico relativo e il link per il download. Per gli agent che si riferiscono al produttore, l'informazione "RelevantDocument" fa riferimento al manuale della conservazione dello stesso, viceversa per gli agent che fanno riferimento al conservatore JSDC indica il presente manuale.

Qualora queste informazioni non siano rese disponibili dal soggetto produttore, JSDC ne segnala automaticamente l'assenza sia nel rapporto di versamento, sia nel contenuto del PIndex. Il produttore è in questo modo reso edotto della eventuale necessità di verificare il proprio sistema di produzione dei documenti informatici.

Una scelta tecnologica importante da evidenziare è manifestata nella valorizzazione degli elementi: "MoreInfo" che non integrano informazioni (metadati) palesemente correlabili all'oggetto conservato ed i relativi contenuti ma di memorizzarli a oggetti esterni al file PIndex e ad esso collegati tramite identificatori univoci e impronte informatiche. La scelta tecnologica consente una maggiore tutela dei contenuti degli oggetti conservati a fronte di operazioni di distribuzione e di consultazione.

8.4.3 Pacchetto di distribuzione

La richiesta di esibizione da parte del Cliente dei documenti conservati viene soddisfatta attraverso la generazione di un PDD che 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 ed è corredato da 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.

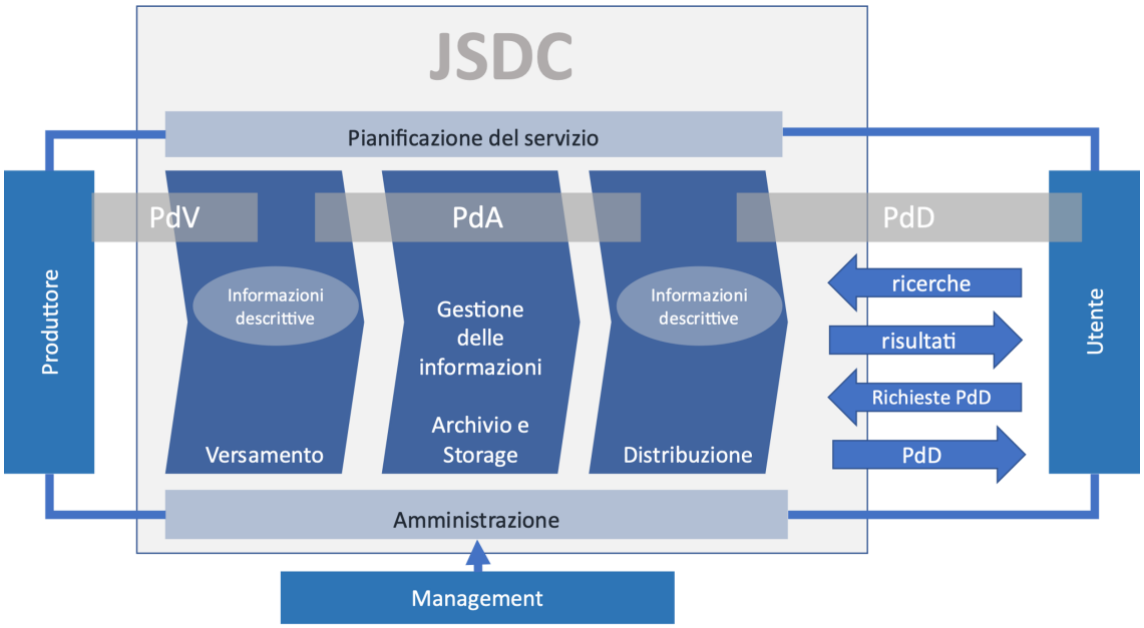
Le richieste di esibizione dei PDD sono accettate solamente se provenienti dai soggetti opportunamente profilati nel sistema e autorizzati dal Cliente.

9 Il processo di conservazione

Il processo di conservazione si esegue sulla base delle modalità previste dal paragrafo 4.7 delle LLGG, e delle specifiche contenute nella 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 sotto forma di PDV a JSDC che lo trasforma in PDA e ne cura la conservazione ed il mantenimento nel tempo. Il SDC provvede anche a mettere a disposizione del soggetto fruitore (nello schema: utente) il contenuto del PDA tramite opportune modalità di accesso per ricerche e richieste di PDD.



Schema 10 - Modello gestionale archivistico OAIS

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

Le principali modalità di trasmissione del pacchetto di versamento sono:

- 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 e sistemi sviluppati da partner di ENERJ

E' prevista anche l'integrazione con il servizio di fatturazione elettronica alla PA di ENERJ, qualora il fruitore sia anche utente di tale servizio. I relativi documenti informatici da conservare sono già presenti nel sistema informativo ENERJ, vengono pertanto generati i 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).

9.2 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 sulla base delle specifiche contenute nel contratto di servizio e nell'accordo di versamento (MCD01), 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 modalità 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 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 della stessa e sulla base degli accordi specifici del Contratto di Servizio.

I controlli e le verifiche implementabili sono descritti nella PCD.

9.3 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 MCD14 relativo ad un pacchetto di versamento.

Il rapporto di versamento è strutturato secondo quanto previsto dalle LLGG sulla formazione, gestione e conservazione dei documenti informatici 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 9.2. 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. L' interfaccia web del JSDC consente comunque sempre al Produttore di monitorare lo stato di tutti i PDV inviati al SDC e pertanto gestire anche eventuali errori risultanti dai controlli.

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.

9.4 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, ed è resa sempre disponibile da JSDC per la consultazione 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.

9.5 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, e si citano a titolo non esaustivo, informazioni relative a: 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 documentate nella PCD e prevedono l'utilizzo di apposita modulistica.

I PDA sono sottoscritti digitalmente dal RSC e, ad essi, sono associate le relative marche temporali; sono così sottoposti al processo di conservazione digitale e 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, 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 nelle specificità di contratto.

9.6 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.

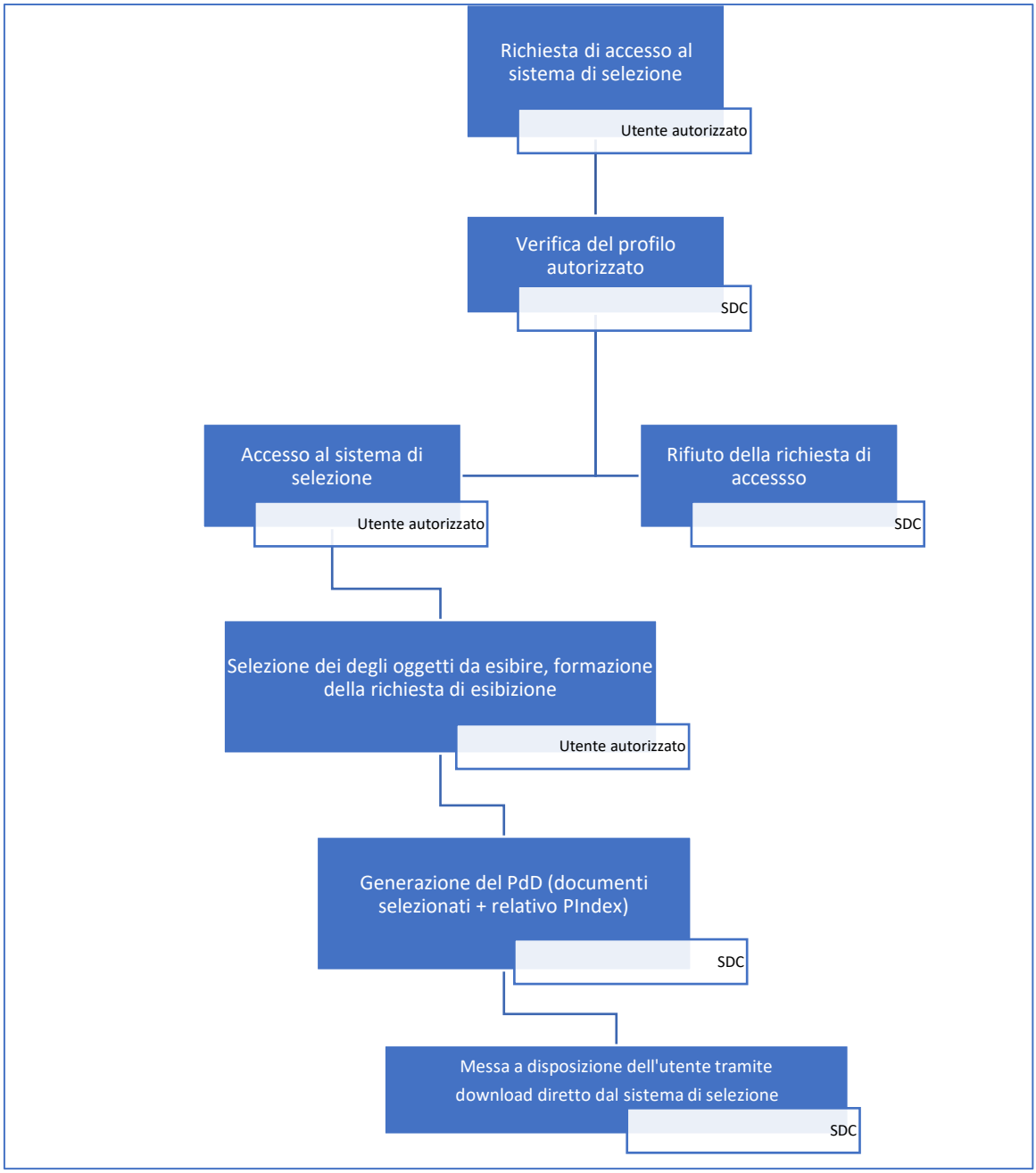
Il sistema provvede quindi a confezionare il PDD contenente i documenti informatici oggetto della selezione ed i relativi file indice (PIndex).

I file PIndex 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. e sono trasportati a cura e responsabilità di personale ENERJ o incaricato da ENERJ sulla base di specifici requisiti definiti dal RdC nella PCD. I dati richiesti sono crittografati con il certificato del destinatario prima della loro spedizione/trasmissione allo stesso.

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 11 - Processo di distribuzione

9.7 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.

9.7.1 Produzione di copie informatiche di documenti analogici

Copie per immagine su supporto informatico 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.

Le procedure di elaborazione di un documento analogico in informatico, menzionate al paragrafo precedente, sono invece gestite dal software JSDC attraverso una opportuna configurazione.

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

Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le medesime disposizioni di cui alla sezione precedente.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla PA, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

9.7.2 Duplicati, copie ed estratti di documenti 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;

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.

9.8 Politiche di conservazione lungo termine (Long Term Preservation Policy) e gestione dell'obsolescenza tecnologica

Al fine mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità dei documenti posti in conservazione il RSC predispone e attua le misure volte ad individuare e correggere eventuali difetti e non congruità dei documenti conservati e dei pacchetti di archiviazione con gli standard tecnologici e la normativa vigente.

I processi di monitoraggio approfonditi nella sezione precedente costituiscono parte integrante delle politiche di conservazione a lungo termine. Oltre ad essi, al fine di garantire il perdurare della validità legale, integrità, leggibilità e riservatezza dei documenti informatici conservati, il sistema prevede le procedure di aggiornamento specificate di seguito.

- **Aggiornamento degli standard di rappresentazione informatica dei documenti**

  La gestione dei metadati dei pacchetti di versamento avviene con uno schema XML che è in grado di recepire gli eventuali aggiornamenti della rappresentazione informatica dei documenti.

- **Aggiornamento applicativo in base al contesto normativo vigente**

  Il sistema di conservazione garantisce una flessibilità di gestione dei metadati che consente di aggiungerne di nuovi o modificarne la lunghezza, permettendo così di adeguare lo standard di ricezione e gestione dei metadati a nuove esigenze sia legate al panorama normativo che ad esigenze specifiche di clienti

- **Gestione dell'obsolescenza tecnologica dei supporti informatici e degli apparati**

  RDT provvede periodicamente ad effettuare le verifiche dei supporti informatici tramite i controlli previsti dal sistema di gestione della sicurezza delle informazioni (ISO 27001).

- **Gestione del tempo di vita del documento**

  L'aspetto del SDC legato alla gestione dello scarto dei documenti conservati è stato affrontato mediante il conferimento, ai set di metadati associati ai documenti, di un campo contenente il tempo di "vita" (data di scarto) del documento nel sistema. Il metadato viene associato al documento in fase di ingresso nel SDC e viene parametrizzato in base alle informazioni ricevute

in merito dal soggetto produttore tramite la relativa documentazione (manuale di gestione, titolario di classificazione, piano di conservazione pregresso) ove esistente.
In caso di indisponibilità del dato dovuta a carenze di carattere tecnico/amministrativo del "soggetto produttore", il SDC possiede un set di default (successivamente integrabile o aggiornabile) definito sulla base di quanto disponibile e rilevabile dal materiale AGID (Linee Guida e documenti di indirizzo).

Il parametro descritto nei punti precedenti è riscontrabile nelle informazioni presenti nell'accordo di versamento (si veda la sezione 2.1.1: "Accordo di versamento (MCD01)").

9.8.1 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 dalle LLGG per la configurazione dei PDA (vedasi sezione 8.4.3 Pacchetto di distribuzione);
- Mantenimento di identità tra Indice Pindex 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, in formato standard SInCRO, previa analisi e valutazione tecnico-economica 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.

9.8.2 Riversamenti

Il procedimento di riversamento degli oggetti informatici si intende attuato nel momento in cui si riversa almeno il formato ed è disposto dal soggetto titolare che, di norma, lo utilizza in relazione ad esigenze strategiche legate alla gestione dei formati e/o alla gestione dello storage.

Il procedimento di riversamento, nel contesto della gestione degli oggetti conservati, viene utilizzato dal titolare degli oggetti conservati per adeguarne le caratteristiche di interoperabilità alle valutazioni previste dall'allegato 2 alle LLGG.

ENERJ coadiuva il cliente nella pianificazione dei procedimenti di riversamento ed opera una duplice azione di:

- verifica progressiva dei formati degli oggetti versati nel SDC dal soggetto produttore tramite il sistema di classificazione di cui alla sezione 8.3.3: "Classe dei Formati",
- informazione al titolare in relazione alla necessità di predisporre eventuali procedimenti di riversamento finalizzati alla conservazione: tramite l'invio al soggetto produttore del rapporto di versamento e la comunicazione dell'accordo di versamento (MCD01).

I titolari degli oggetti conservati valutano l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato tenendo in considerazione quanto previsto dalle LLGG in relazione ai fattori: formati aperti, non proprietari, standard de iure, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo. Il riversamento è effettuato tramite procedure tecniche del SDC in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento" alle LLGG.

9.9 Cessazione del servizio

La cessazione del servizio può essere rivolta ad uno o più soggetti produttori specifici o può riguardare tutto il servizio.

9.9.1 Cessazione del rapporto di servizio con il singolo produttore

Per disciplinare il caso di cessazione del servizio con il singolo produttore ENERJ ha implementato la Procedura di gestione della Conservazione Digitale (PCD) e nell'ambito di questa, l'istruzione di Cessazione del Servizio (ICD03) che descrive nello specifico la gestione dell'interruzione dell'erogazione del servizio ad uno o più clienti e le modalità di restituzione e cancellazione degli archivi conservati.

Per approfondimenti sulle modalità di cessazione del servizio si rimanda alla documentazione citata nel paragrafo precedente e alle specificità contrattuali relative allo specifico rapporto di servizio.

9.9.2 Cessazione del servizio di conservazione

Il documento Technical Specification (TS), pubblicato da ETSI con l'identificativo ETSI TS 119 511, sui requisiti di policy e sicurezza per i trust service providers (TSP) che offrono servizi di conservazione a lungo termine delle firme digitali o, in generale, di dati che usano tecniche di firma digitale, al paragrafo 7.12 stabilisce i requisiti che riguardano il processo di cessazione, richiamando quelli indicati nella norma ETSI EN 319 401 paragrafo 7.12 relativi ai requisiti di policy generali per tutti i TSP, aggiungendo un ulteriore requisito che riguarda specificatamente i TSP che erogano servizi di conservazione di firma digitale o di dati che usano tecniche di firma digitale.

La comunicazione ad AGID e ai clienti del servizio dell'intenzione di cessare l'attività di conservazione è inviata da ENERJ almeno 60 giorni prima della data di cessazione. La comunicazione, predisposta in formato elettronico e firmata digitalmente dal legale rappresentante del conservatore, è trasmessa con strumenti idonei alla verifica della consegna (es. PEC) ed è corredata dal documento di programmazione delle attività di cessazione.

Con la formalizzazione del Piano di Cessazione (PCE), ENERJ definisce le modalità e i criteri adottati nella gestione del sistema di conservazione in caso di cessazione volontaria o involontaria dello stesso. Il documento aggiornato è sempre trasmesso ad AGID anche ai fini del mantenimento dell'iscrizione al marketplace dei conservatori come premesso nella sezione 1 "Introduzione" ed è reso disponibile nel portale servizi dedicato agli utenti come descritto nella sezione 2.1.2: "Portale servizi".

9.10 Restituzione degli archivi conservati

Il processo di restituzione degli archivi conservati ai soggetti titolari prevede una serie di azioni comuni sia ai casi di cessazione di servizi relativi ad uno o più specifici titolari, che negli scenari previsti nella terminazione dell'intero servizio di conservazione:

- Disattivazione del servizio
    - Verifica della conclusione effettiva del servizio
    - Disattivazione dei profili dei soggetti produttori
- Analisi preliminare dei pacchetti di archiviazione
- Trasferimento degli archivi di conservazione
    - Predisposizione della documentazione
    - Verifica delle caratteristiche tecniche dei volumi da trasferire
    - Messa a disposizione dei pacchetti di distribuzione tramite accesso diretto a JSDC
    - Ottenimento dei pacchetti di distribuzione tramite accesso ad area FTPS
    - Trasmissione tramite supporto informatico fisico (metodologia deprecata ed attuata in base alle caratteristiche peculiari degli archivi da trasferire)
- Comunicazione delle modalità e tempistiche di trasferimento degli archivi.

Le modalità e le tempistiche di restituzione degli archivi conservati sono specifiche per ciascun titolare degli oggetti conservati e sono definite negli accordi contrattuali e, in modo generale, nella PCD; nel caso di cessazione di JSDC (dell'intero sistema di conservazione) le medesime sono definite e descritte dal piano di cessazione (PCE).

9.11 Scarto e cancellazione dei pacchetti di archiviazione

La procedura di scarto dei documenti conservati negli archivi viene operata e coordinata da RSC sulla base delle disposizioni ricevute dal soggetto produttore, delle disposizioni contenute nei contratti di servizio e in ottemperanza a quanto sancito dal panorama normativo vigente.

RFA e RQS coadiuvano RSC nella ponderazione delle azioni da intraprendere a fronte dell'attuazione di un procedimento di scarto. Tale procedimento viene operativamente attuato da RSI coadiuvato dagli addetti opportunamente individuati dell'area gestione sviluppo software e manutenzione e consiste nelle seguenti fasi:

- interrogazione del database del SDC per l'estrazione dei documenti che hanno superato la soglia temporale di scarto;
- informazione del soggetto produttore tramite interlocuzione diretta con RSC (o operatore incaricato) ed invio di una comunicazione formale tramite PEC;
- esecuzione della procedura batch (configurata ad hoc) per la cancellazione dei documenti condotta manualmente dagli operatori incaricati.

Gli ulteriori dati relativi al soggetto produttore eventualmente custoditi nel sistema informativo di ENERJ sono successivamente sottoposti alle procedure di cancellazione descritte nel Manuale della Sicurezza del Sistema Informativo (MSI) e a cui soggiacciono in generale tutti i dati gestiti. JSDC 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 nel PDS e nella 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 produttore.

10 IL SISTEMA DI CONSERVAZIONE

Il SDC si basa su un complesso di moduli facenti funzioni specifiche all'interno del sistema e tra loro interagenti nella gestione di tutti gli aspetti relativi alla conservazione degli archivi informatici e alla gestione della sicurezza del sistema.

L'erogazione dei servizi di conservazione, a discrezione di ENERJ in funzione delle politiche di carico e di gestione dei sistemi, può essere effettuata alternativamente tramite i sistemi on-premisis o su infrastruttura Cloud riconosciuta come CSP da AGID. ENERJ si configura come Cloud Service Provider, in quanto eroga servizi di conservazione a norma per i propri clienti in modalità Cloud, sia Cloud Service Customer, in quanto utilizza l'infrastruttura IaaS di Aruba (infrastruttura presente all'interno del market place di AGID) per erogare i servizi in modalità SaaS ai sui clienti.

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.

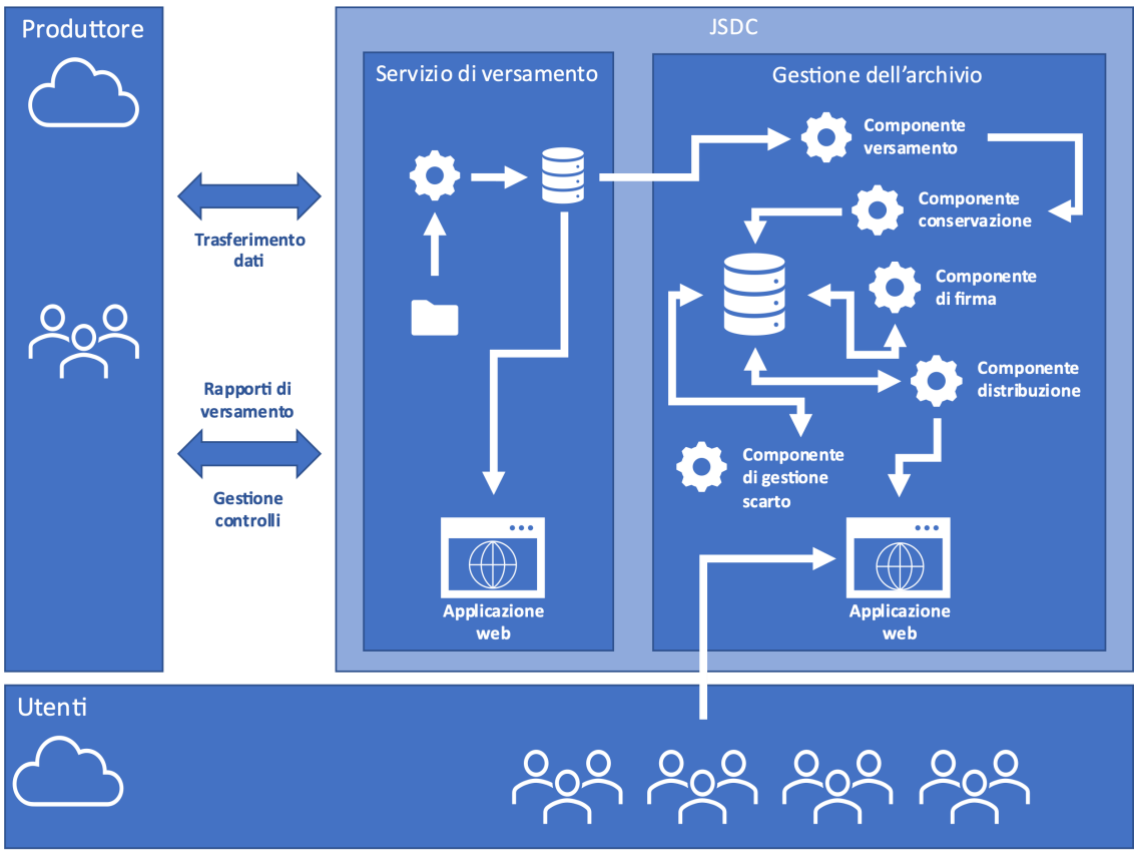
10.1 Componenti Logiche

Il SDC è logicamente rappresentabile nelle sue componenti (interne ed esterne al sistema) la cui interazione è basata sul flusso di informazioni condiviso con gli attori del processo, ossia:

- Produttore: effettua il versamento al SDC dei nuovi PDV generati;
- 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 di Versamento: prende in carico i PDV validati e gestisce l'inoltro al sistema di conservazione;
- Servizio di Conservazione: gestisce la trasformazione da PDV a PDA utilizzando i servizi di firma digitale dei documenti implementati con tecnologia HSM presso una QTSA accreditata convenzionata con ENERJ;
- Servizio di Distribuzione: gestisce la ricerca dei documenti da parte degli Utenti abilitati e la generazione dei PDD è realizzata tramite JDoc;
- 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.



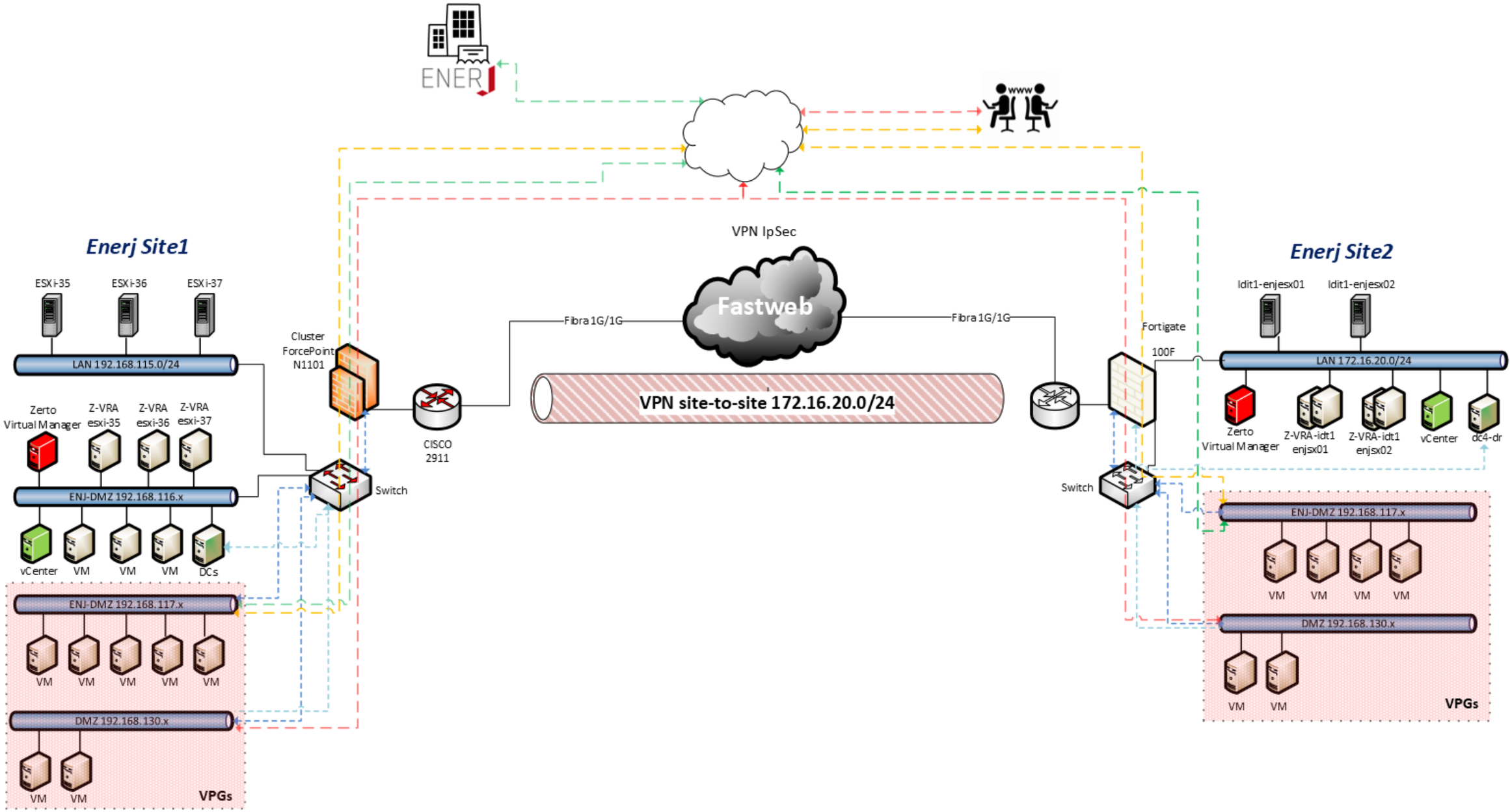
Schema 12 - Schema delle componenti logiche del SDC

10.2 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;
- JView Modulo software per la distribuzione e l'esibizione dei documenti informatici conservati.

L'elenco completo dei software implementati da ENERJ e utilizzati nella gestione del SDC è contenuto negli inventari del software afferenti al ISMS (MCO04 - Inventario del software commerciale, MCO02 - Inventario del software proprietario). Le informazioni contenute negli inventari sono estratte e rese disponibili alle parti interessate dietro richiesta.



Schema 13 - Schema topologico e descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione

10.3 Procedure di gestione e di evoluzione

10.3.1 Conduzione e manutenzione del sistema di conservazione

In relazione alle componenti software di ENERJ la 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.

10.3.2 Gestione e conservazione dei log

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.

Il Sistema di "log management" di ENERJ è descritto nel Manuale di Sicurezza del Sistema Informativo (MSI): nel documento si approfondiscono anche le tematiche legate a:

- modalità di conservazione,
- tempistiche di conservazione,
- modalità di accesso e consultazione,
- misure di sicurezza e protezione dei log.

Le informazioni contenute nel MSI sono ad uso interno, ma possono essere resi disponibili, alle parti interessate, estratti del documento dietro motivata richiesta da inoltrare nelle modalità definite nella sezione 13: "Trasparenza e archiviazione".

10.3.3 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.

10.3.4 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.

10.4 Gestione dei parametri amministrativi del SDC e accesso al Portale Servizi.

L'attivazione del servizio per un cliente avviene dietro accettazione della proposta commerciale e sottoscrizione della documentazione contrattuale e dà quindi luogo alla configurazione dei parametri amministrativi ed operativi che consentono al sistema di operare e di erogare stabilmente il servizio di conservazione nelle modalità concordate.

La predisposizione dei parametri amministrativi, funzionali ed operativi avviene sotto la responsabilità di RGC e tramite l'attività del personale delle aree "Gestione clienti" e "Gestione service" sulla base delle esigenze manifestate dal cliente e formalizzate in fase progettuale e propositiva.

L'attivazione del servizio, inoltre, abilita gli utenti autorizzati dal cliente all'accesso al "Portale Servizi": un'area dedicata dove il soggetto che accede può:

- ottenere informazioni e statistiche dettagliate sulla conduzione dei propri servizi di conservazione;
- consultare gli archivi conservati ed effettuare ricerche parametriche;
- verificare lo stato di conservazione dei documenti;
- effettuare operazioni di distribuzione (creazione di PDD);
- consultare documenti importanti (ad es. il presente manuale o il piano di cessazione) e guide operative per l'utilizzo del portale e del servizio;
- inviare richieste di attivazione, modifica e cessazione delle utenze che accedono al SDC;
- inviare segnalazioni e richieste di assistenza in merito ad anomalie del sistema

Tutte le attività di configurazione amministrativa ed operativa del SDC:

- sono formalizzate e descritte nella procedura interna di gestione del processo di conservazione (PGC) e nelle relative istruzioni (IGC),
- sono inoltrate dal cliente tramite contatto diretto con il proprio referente in ENERJ (Incaricato commerciale o Project manager), mail o mediante segnalazione,
- sono attuate dagli operatori delle aree “Gestione clienti” e “Gestione service”.

Le richieste del cliente, in questo senso, sono sempre mediate e gestite dagli operatori e/o dal personale di ENERJ.

11 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.

11.1 Procedure di monitoraggio applicativo

Gli applicativi software del SDC producono i log delle transazioni dei pacchetti informativi (di cui alla sezione 10.3.2 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.

11.2 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.

11.3 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 e 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 test sui sistemi;
- modalità 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.

11.4 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 PGC.

11.5 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 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).

12 PROTEZIONE DEI DATI

Tutte le operazioni inerenti ai processi produttivi sono realizzate nel rispetto del Regolamento Generale per la Protezione dei Dati personali (Reg. EU 679/2016): ENERJ ha istituito, nell'ambito dei propri sistemi informativi integrati, l'area "Legal & Data protection" a cui si rimanda per qualunque approfondimento in merito e che ospita la documentazione relativa alla gestione della protezione dei dati.

ENERJ ha istituito il proprio registro delle attività di trattamento strutturato sulla base delle indicazioni normative. Periodicamente viene realizzata un Valutazione dell'Impatto sulla Protezione dei Dati personali per stabilire il livello di rischio per gli interessati dal trattamento.

Tutte le esigenze relative alle modalità di gestione e di protezione dei dati personali possono essere richieste dalle parti interessate tramite mail all'indirizzo: dataprotection@enerj.it.

ENERJ ha inoltre incaricato il proprio Responsabile per la Protezione dei Dati (RPD), o anche Data Protection Officer (DPO), sulla base di quanto disposto dall'art. 37 del GDPR. Le questioni da sottoporre all'attenzione del RDP possono essere inoltrate tramite mail all'indirizzo: dpo@enerj.it.

13 Trasparenza e archiviazione

Tutta la documentazione a cui si fa riferimento nel contenuto del presente documento è disponibile alle parti interessate, in forma completa o di estratto, dietro motivata richiesta da inoltrare all'indirizzo PEC: ENERJ@actalispec.it. Al medesimo indirizzo PEC si fa riferimento nel contenuto del presente documento ogni qual volta viene citato come sistema per la gestione delle comunicazioni da e verso le altre parti.

L'originale di tutta la documentazione prodotta dal SDC ed attinente al servizio di conservazione viene archiviato dal sistema stesso e sottoposto a procedura di conservazione. I documenti sono conservati dal SDC di ENERJ sulla base di quanto disposto dalle procedure interne e comunque in ottemperanza a quanto sancito dal panorama normativo vigente ed agli accordi contrattuali.

Tutta la documentazione relativa al sistema di gestione della qualità e sicurezza delle informazioni è condivisa in modo sicuro tramite i sistemi informativi integrati di ENERJ basato su piattaforma Microsoft.

14 Revisioni

14 del 30/05/2022

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Aggiunta della sezione 10.4 “Gestione dei parametri amministrativi del SDC e accesso al Portale Servizi”; aggiornamento della sezione 10.3.2 “Gestione e conservazione dei log”

13 del 13/04/2022

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Aggiornamento del titolo del manuale, apportate correzioni ortografiche e sintattiche.

12 del 18/01/2022

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Adeguamento alle LLGG sulla formazione, gestione e conservazione dei documenti informatici emanate da AGID in data 11/09/2021.

11 – settembre 2015

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Aggiornamento.

10 – febbraio 2014

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Aggiornamento.

9 – novembre 2014

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).
- Note di versione: Aggiornamento.

8 – marzo 2013

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Giovanni Auletta (DIR).

- Note di versione: Aggiornamento.

7 – marzo 2010

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

6 – marzo 2009

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

5 – novembre 2008

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

4 – marzo 2007

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

3 – ottobre 2006

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

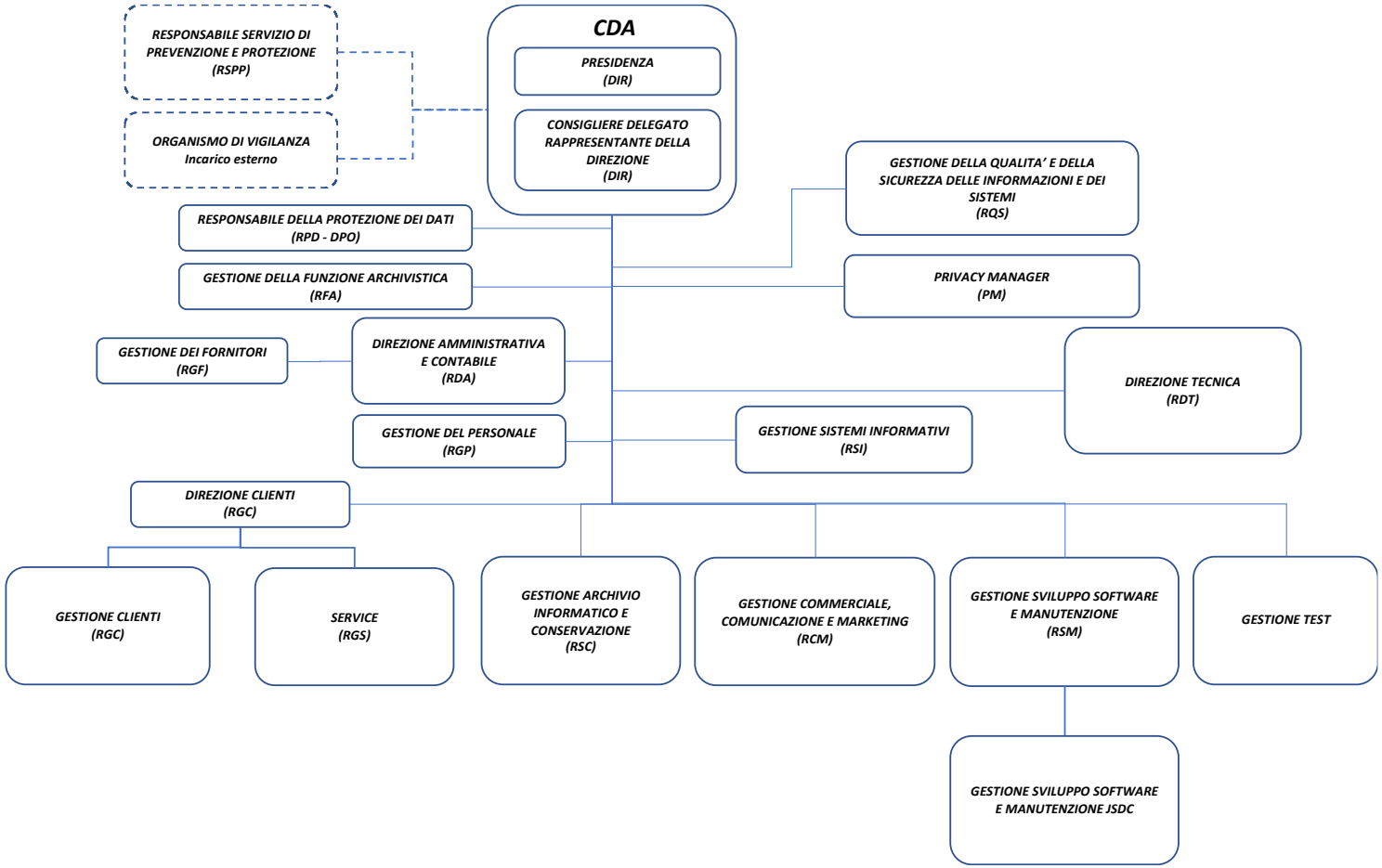
2 – febbraio 2006

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Aggiornamento.

1 – settembre 2005

- Redazione: Silvano Artioli (RQS), riesame: Ferdinando Auletta (RSC), approvazione: Ferdinando Auletta (DIR).
- Note di versione: Stesura.

Si riporta in appendice l'organigramma di ENERJ



tinexta
infocert

Manuale della Conservazione

Emittente: InfoCert SpA
Sito web: infocert.it infocert.digital

tinexta
infocert

Sommario

tinexta
infocert

Registro delle versioni

N° versione	Data emissione	Modifiche apportate
01	Luglio 2014	Prima versione
02	Novembre 2015	Utilizzo dello schema proposto da AgID
03	Febbraio 2016	Correzioni formali e di layout
04	Marzo 2016	Correzioni formali e di layout
05	Settembre 2017	Glossario, Normativa, Mission, Comunità di riferimento, Riferimenti a policy aziendali interne
05.1	Novembre 2017	Specificità del contratto
06	Luglio 2018	Normativa GDPR, semplificazione glossario e nuovi Responsabili
07	Gennaio 2019	Nuovo logo aziendale
08	Maggio 2019	Nuovo Responsabile sistemi
09	Ottobre 2020	Glossario, nuovi Responsabili, aggiornamento procedure di monitoraggio, semplificazione delle Specificità del contratto
10	Novembre 2020	Ampliamento servizi di storage e introduzione Linee Guida AgID
11	Aprile 2022	Semplificazione nella descrizione dei processi Introduzione del servizio SAFE LTA Aggiornamento procedure di monitoraggio
12	Maggio 2023	Nuovo logo Aggiornamento TSS per la marca temporale
13	Agosto 2024	Semplificazione e aggiornamento Responsabili, Profilo InfoCert (indirizzi e qualificazione ACN), Sistema SAFE LTA e Specificità del contratto
14	Aprile 2025	Nuovo logo Cambio Responsabile del servizio

SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il **manuale della conservazione di InfoCert S.p.A.** (Tinexta InfoCert), ai sensi delle **Linee Guida AgID**, Agenzia per l'Italia Digitale, su formazione, gestione e conservazione dei documenti informatici di maggio 2021, richiamate dal **Codice dell'Amministrazione Digitale** - decreto legislativo n. 82 del 2005.

Il manuale della conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

In caso di ispezione da parte delle autorità di vigilanza preposte, il manuale della conservazione permette un agevole svolgimento di tutte le attività di controllo.

Ogni soggetto produttore, cliente dei servizi di conservazione di InfoCert e titolare dei documenti conservati, può liberamente far riferimento al presente documento nel proprio manuale della conservazione.

tinexta
infocert

TERMINOLOGIA

TERMINE	DEFINIZIONE
ACCESSO	Operazione che consente di prendere visione dei documenti informatici.
AFFIDABILITÀ	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIO	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
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 in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
CERTIFICAZIONE	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
CLASSIFICAZIONE	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
CONSERVATORE	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
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, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
DESTINATARIO	Soggetto o sistema al quale il documento informatico è indirizzato.
DIGEST	Vedi Impronta crittografica.

TERMINE	DEFINIZIONE
DOCUMENTO AMMINISTRATIVO INFORMATICO	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
DOCUMENTO ELETTRONICO	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
DOCUMENTO INFORMATICO	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DUPLICATO INFORMATICO	Vedi art. 1, comma 1, lett) i quinquies del CAD.
ESEAL	Vedi sigillo elettronico.
ESIBIZIONE	operazione che consente di visualizzare un documento conservato
ESIGNATURE	Vedi firma elettronica.
ESTRAZIONE STATICA DEI DATI	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc..), attraverso metodi automatici o semi-automatici
EVIDENZA INFORMATICA	Sequenza finita di *bit* che può essere elaborata da una procedura informatica.
FASCICOLO INFORMATICO	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
FILE	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
FIRMA ELETTRONICA	Vedi articolo 3 del Regolamento eIDAS.
FIRMA ELETTRONICA AVANZATA	Vedi articoli 3 e 26 del Regolamento eIDAS.
FIRMA ELETTRONICA QUALIFICATA	Vedi articolo 3 del Regolamento eIDAS.
FLUSSO (BINARIO)	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
FORMATO CONTENITORE	Formato di file progettato per consentire l'inclusione ("imbustamento" o *wrapping*), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
FORMATO DEL DOCUMENTO INFORMATICO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.

TERMINE	DEFINIZIONE
FUNZIONE DI *HASH* CRITTOGRAFICA	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o *digest* (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
GESTIONE DOCUMENTALE	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
HASH	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "*digest*" (vedi).
IDENTIFICATIVO UNIVOCO	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
IMPRONTA CRITTOGRAFICA	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di *hash* crittografica a un'evidenza informatica.
INTEGRITÀ	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
INTEROPERABILITÀ	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
LEGGIBILITÀ	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
MANUALE DI CONSERVAZIONE	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
METADATI	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.

TERMINE	DEFINIZIONE
OGGETTO DIGITALE	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
PACCHETTO DI ARCHIVIAZIONE	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
PACCHETTO DI DISTRIBUZIONE	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
PACCHETTO DI FILE (*FILE PACKAGE*)	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
PACCHETTO DI VERSAMENTO	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
PACCHETTO INFORMATIVO	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
PATH	Percorso (*vedi*).
PATHNAME	Concatenazione ordinata del percorso di un file e del suo nome.
PERCORSO	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
PIANO DI CONSERVAZIONE	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
PIANO DI ORGANIZZAZIONE DELLE AGGREGAZIONI DOCUMENTALI	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
PIANO GENERALE DELLA SICUREZZA	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio 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 e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare

TERMINE	DEFINIZIONE
	dell'oggetto di conservazione e il responsabile del servizio di conservazione.
PROCESSO	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
PRODUTTORE DEI PDV	Persona fisica, 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.
QSEAL	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
QSIGNATURE	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
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.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RESPONSABILE DELLA CONSERVAZIONE	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
RESPONSABILE DELLA FUNZIONE ARCHIVISTICA DI CONSERVAZIONE	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
RIFERIMENTO TEMPORALE	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
RIVERSAMENTO	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
SCARTO	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
SIGILLO ELETTRONICO	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
SISTEMA DI CONSERVAZIONE	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.

TERMINE	DEFINIZIONE
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
TIMELINE	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di *timeline* un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
TITOLARE DELL'OGGETTO DI CONSERVAZIONE	Soggetto produttore degli oggetti di conservazione.
TRASFERIMENTO	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
UTENTE ABILITATO	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.
VERSAMENTO	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

tinexta
infocert

NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito l'elenco dei principali riferimenti normativi in materia, ordinati secondo il criterio della gerarchia delle fonti:

- eIDAS (electronic IDentification Authentication and Signature) Reg. 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market, così come modificato dal Reg. (UE) 2024/1183 of the European Parliament and of the Council of April 2024.
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- 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 ss.mm.ii. – 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 ss.mm.ii – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e ss.mm.ii. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e ss.mm.ii. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e ss.mm.ii. (D. Lgs. 26 agosto 2016, n.179) – Codice dell'amministrazione digitale (CAD) e ss.mm.ii.;
- 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 per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005 [parzialmente abrogate dalle Linee Guida AgID a partire da gennaio 2022];
- 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 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.
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici pubblicate a settembre 2020, aggiornate nel maggio 2021 e pienamente applicabili dal gennaio 2022.

- Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici di dicembre 2021 (marketplace).

Si riportano di seguito gli standard di riferimento:

- UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 14721 - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO 15836 - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;
- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- SIARD Software Independent Archiving of Relational Databases 2.0;
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de donnéès pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS – PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for

protection of personally identifiable information (PII) in public clouds acting as PII processors;

- ETSI TS 101 533-1 V1.2.1 - 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 V1.2.1 - 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.

Inoltre, si segnalano due procedure aziendali interne connesse al servizio:

- **Procedura di handover e scarto**, che descrive le modalità di richiesta ed esecuzione delle attività di versamento da/a un altro Conservatore e delle attività di cancellazione fisica e logica dei documenti, nel rispetto delle Linee Guida AgID e del GDPR.
- **Piano di cessazione**, che descrive le attività di InfoCert in caso di cessazione dei servizi di conservazione, in modo da fornire a utenti e clienti il supporto necessario alla migrazione verso altri Conservatori.

RUOLI E RESPONSABILITÀ

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità.
I ruoli individuati dalle Linee Guida AgID sono:

a) **TITOLARE DELL'OGGETTO DELLA CONSERVAZIONE** (soggetto produttore degli oggetti di conservazione);
b) **PRODUTTORE DEI PACCHETTI DI VERSAMENTO** (persona fisica, 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, anche attraverso l'utilizzo di piattaforme o sistemi InfoCert);
c) **UTENTE ABILITATO** (persona, ente o sistema che interagisce con i servizi di conservazione, al fine di fruire delle informazioni di interesse, cioè per le attività di ricerca ed esibizione a norma);
d) **RESPONSABILE DELLA CONSERVAZIONE** (interno al cliente/produttore, che scegliere di affidare il servizio a InfoCert);
e) **CONSERVATORE** (InfoCert).

I primi quattro ruoli sono tipicamente individuati all'interno dell'organigramma di quello che per InfoCert è il cliente/produttore.
Quest'ultimo affida in *full outsourcing* il servizio di conservazione a InfoCert S.p.A., in accordo con quanto previsto dai documenti contrattuali descritti al capitolo 'Specificità del Contratto' e dalle Linee Guida AgID. In particolar modo, nell'Atto di affidamento' sono elencate funzioni e ambiti oggetto della delega.
All'interno dell'organigramma di InfoCert, sono, invece, individuati un **Responsabile del servizio di conservazione**, un **Responsabile della funzione archivistica** (come previsto dal Regolamento AgID) e gli altri ruoli qui di seguito riportati.

PROFILO DI INFOCERT

InfoCert si pone sul mercato europeo come **Trust Service Provider** qualificato ai sensi del Regolamento eIDAS, leader del mercato nei servizi di digitalizzazione e dematerializzazione, nonché una delle principali Certification Authority a livello europeo, fornendo servizi di Posta Elettronica Certificata, Firma Avanzata e Digitale, Conservazione Digitale dei documenti e gestore accreditato AgID dell'identità digitale di cittadini e imprese, in conformità ai requisiti regolamentari e tecnici dello SPID (Sistema Pubblico per la gestione dell'Identità Digitale).
Da sempre la **mission aziendale** è credere nel futuro e nella trasformazione digitale, per questo dedichiamo la nostra esperienza, la nostra capacità di innovazione e la nostra passione per l'eccellenza, a tutti coloro che, in Italia e nel mondo, ricercano sicurezza e affidabilità nelle soluzioni digitali. Investiamo in ricerca e sviluppo per dare vita a nuove idee che supportino i nostri clienti nella costruzione di modelli e processi di business innovativi e conformi alle normative, guidandoli verso una efficace trasformazione digitale e un futuro maggiormente sostenibile per le aziende, le persone e la realtà sociale.

La mission aziendale si declina anche nel servizio di Conservazione digitale: innovazione, sicurezza, affidabilità e conformità normativa, con lo scopo di assicurare la corretta gestione, archiviazione e

conservazione dei documenti informatici di diversi soggetti produttori, assicurando l'esibizione a norma dei documenti conservati e la consulenza specialistica su progetti di paperless design.

InfoCert dal 2014 è stata tra le prime aziende italiane accreditate dall'Agenzia per l'Italia Digitale (AgID) come Conservatore, requisito normativo necessario per erogare servizi di Conservazione digitale per la Pubblica Amministrazione.

Da febbraio 2022, è iscritta al Marketplace dei servizi di conservazione di AgID come conservatore qualificato - https://conservatoriqualificati.agid.gov.it/

Inoltre, InfoCert è tra i fornitori presenti nel Catalogo delle Infrastrutture digitali e dei Servizi Cloud di ACN (Agenzia per la Cybersicurezza Nazionale), requisito normativo necessario per offrire alla Pubblica Amministrazione, le proprie soluzioni di conservazione digitale a norma: SAFE LTA (SaaS - ID Scheda in ACN: SA-3452) e LegalDoc (SaaS - ID Scheda: SA-779), con la sua Infrastruttura CSP di Tipo B -

https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud

- **denominazione sociale:** InfoCert S.p.A.
- **sede legale:** Piazzale Flaminio 1/b, 00196 Roma
- **sedi operative:** Piazza da Porto, 3, 35131 - Padova
  Via Fernanda Wittgens, 6, 20123 – Milano
  Via Gian Domenico Romagnosi 4, 00196 Roma
- **telefono:** 049.7849350
- **sito web**: www.infocert.it
- **e-mail**: info@infocert.it
- **PEC:** infocert@legalmail.it
- **codice fiscale / partita IVA:** 07945211006
- **numero REA:** RM – 1064345

Oggi il servizio di conservazione di InfoCert si declina in due prodotti:

- **LegalDoc**, storico servizio, sviluppato sulla base delle Regole Tecniche del 2013, pensato per il mercato italiano e accreditato AgID dal 2014.
- **SAFE LTA** (***Long-Term-Archiving***), sviluppato nel 2021, sulla base delle specifiche *eArchiving building block* del *Connecting Europe Facility* (CEF), in ottica internazionale.

La **comunità di riferimento** del servizio di Conservazione digitale di InfoCert è un gruppo identificato di clienti e di potenziali utenti in grado di comprendere un determinato set di informazioni: si tratta di un'unica comunità, ben definita, ma con alcune differenziazioni interne (multiple user communities), a seconda del mercato di riferimento (Pubblica Amministrazione centrale e locale, Sanità, Industry, Banking, Pharma, Utilities, Insurance, Ordini e Associazioni, PMI, liberi professionisti) e delle varie geografie internazionali.

Il fine ultimo del servizio di Conservazione digitale è rendere i Pacchetti di Distribuzione ricercabili, esibibili, leggibili, integri, affidabili, autentici e fruibili dagli utenti della comunità di riferimento, attraverso la mediazione del soggetto produttore, in ottemperanza ai principali standard internazionali di *records management* (OAIS ISO14721 e ISO15489).

InfoCert è costantemente impegnata nel monitoraggio della propria comunità designata, al fine di acquisire nuove informazioni o esigenze o standard tecnologici, anche con lo scopo di combattere l'obsolescenza tecnologica.

InfoCert, inoltre, nello svolgimento delle proprie attività, ha conseguito le seguenti certificazioni: https://www.infocert.it/certificazioni

RESPONSABILI INFOCERT

Si riportano di seguito i profili professionali di responsabilità legate al servizio di conservazione e le rispettive attività di competenza.
Tutti i Responsabili sono assunti a tempo indeterminato.

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
Responsabile del servizio di Conservazione	Lucia Bortoletto	• 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 (in collaborazione con Ufficio Legale e Product Marketing Manager), definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	da marzo 2025
Responsabile funzione archivistica di conservazione	Marta Gaia Castellan	• 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	da settembre 2015

RUOLI	NOMINATIVI	ATTIVITA'	PERIODI
		competenza; • controlli periodici a campione sulla leggibilità dei documenti conservati.	

Di seguito sono storicizzate le figure professionali che hanno ricoperto ruoli di responsabilità precedentemente:

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile del servizio	Nicola Maccà	Da luglio 2018 a marzo 2025
Responsabile sviluppo e manutenzione del sistema di conservazione	Lucia Bortoletto	da luglio 2018 a gennaio 2022 (data in cui il Regolamento AgID ha ristretto le figure di responsabilità alle due nella precedente tabella)
Responsabile trattamento dati personali	Ilenia Gentilezza	da marzo 2020 a luglio 2023
Responsabile Sicurezza dei sistemi per la conservazione	Giovanni Belluzzo	da luglio 2018 a gennaio 2022
Responsabile sistemi informativi per la conservazione	Stefano Mameli	da maggio 2019 a ottobre 2020
Responsabile trattamento dati personali	Valentina Zoppo	da luglio 2018 a marzo 2020
Responsabile sistemi informativi per la conservazione	Nicolò Poniz	da luglio 2018 a maggio 2019
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Maccà	da gennaio 2013 a luglio 2018
Responsabile sistemi informativi per la conservazione	Massimo Biagi	da marzo 2014 a luglio 2018
Responsabile funzione archivistica di conservazione precedente	Silvia Loffi	da dicembre 2014 ad agosto 2015
Responsabile trattamento dati personali	Alfredo Esposito	da gennaio 2011 a luglio 2018
Responsabile Sicurezza dei sistemi per la conservazione	Alfredo Esposito	da gennaio 2011 a luglio 2018

RUOLI	NOMINATIVI PRECEDENTI	PERIODI
Responsabile del servizio di Conservazione	Antonio Dal Borgo	da luglio 2008 a luglio 2018
Responsabile del servizio di Conservazione	Pio Barban	da luglio 2007 a luglio 2008

OGGETTI SOTTOPOSTI A CONSERVAZIONE

In generale si definisce '**pacchetto**' un contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche).
I pacchetti sono contrattualizzati con il soggetto produttore e si basano sui documenti che fanno parte delle 'Specificità del Contratto'.

Per "**PACCHETTO DI VERSAMENTO**" si intende l'insieme di documenti che il soggetto produttore invia al sistema di conservazione in un'unica sessione o in una singola chiamata. Le modalità di versamento sono diverse: dal caricamento manuale attraverso portale web, all'utilizzo di chiamate applicative. Il sistema ritorna una Ricevuta di versamento.

Per "**PACCHETTO DI ARCHIVIAZIONE**" si intende un pacchetto informativo composto dalla trasformazione di pacchetti di versamento, depositato nei data center InfoCert e associato a un file XML, detto Indice del Pacchetto di Archiviazione (IPdA o indice di conservazione UNI SInCRO) sigillato e marcato temporalmente dal Responsabile del servizio di InfoCert. In LegalDoc coincide con il Rapporto di versamento.
Questo indice di conservazione, secondo lo standard **UNI 11386 SInCRO 2020**, contiene: una sezione di SelfDescription (con i riferimenti dell'applicativo e del Conservatore), una sezione di PVolume (con lo schema xsd), una sezione MoreInfo per LegalDoc (con token, bucket, policy, operation, target), una sezione FileGroup (con token, hash e SHA dei vari file del pacchetto), una sezione Process (con i riferimenti al manuale, al Responsabile del servizio e al riferimento temporale).
Ogni documento da conservare viene identificato in modo univoco attraverso un token (es. per LegalDoc TB853E72B7552EBB8D0AF3FE9EE1EAB3D97519959346B83DD5E539).

Per "**PACCHETTO DI DISTRIBUZIONE**" si intende un pacchetto informativo inviato dal sistema di conservazione all'utente, in risposta a una sua ricerca e richiesta di esibizione. Il suo contenuto coincide con il "pacchetto di archiviazione".

Eventuali specificità sono concordate con il Soggetto produttore e descritte nelle 'Specificità del Contratto' - Specifiche tecniche per l'integrazione – Allegato Tecnico al Contratto LegalDoc o SAFE LTA.
Un pacchetto di archiviazione in LegalDoc è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato dal Responsabile del servizio di InfoCert)
- File di parametri (contenente le informazioni per la leggibilità nel tempo)
- File di indici (contenente i metadati del documento conservato)
- File di dati (documento conservato)

Un pacchetto di archiviazione in SAFE LTA è composto da:

- L'Indice di Conservazione UNI SInCRO, altrimenti detto Indice del Pacchetto di Archiviazione o Indice di Conservazione (sigillato e marcato da InfoCert)
- Metadata Descriptive (file XML di metadatazione)
- Metadata Preservation (file XML di metadatazione secondo lo standard PREMIS)
- Schemas (file XSD di metadatazione)

- Representation (documento conservato)

FORMATI

Tipologie documentali e formati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione'.
In LegalDoc i visualizzatori di alcuni formati (definiti in InfoCert come 'standard' perché maggiormente richiesti) sono automaticamente assegnati all'atto dell'attivazione del proprio ambiente di conservazione e sono forniti da InfoCert al soggetto produttore all'atto di attivazione del servizio.

Formato	Estensione	MIME-Type	Standard
PDF o PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

Tutti i documenti inviati in conservazione sono associati al visualizzatore configurato per il particolare formato.
Conservare documenti in altri formati (jpeg, Open Document Format, eml, DICOM, ecc..), in conformità con l'**Allegato 2 delle Linee Guida AgID**, è sempre possibile. Qualora un soggetto produttore necessiti di formati aggiuntivi rispetto a quelli standard, può segnalarlo nei 'Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA (compresi nelle 'Specificità del Contratto') o configurarli autonomamente utilizzando l'apposita funzionalità ed eventualmente conservare gli appositi visualizzatori all'interno del sistema. Un'apposita sezione dell'ambiente di conservazione, infatti, è dedicata alla conservazione dei visualizzatori dei formati (*viewer*), che può essere arricchita a seconda delle esigenze.
Inoltre, il Responsabile del servizio della conservazione mantiene un archivio di tutte le componenti hardware e software obsolete, non più compatibili con i programmi di visualizzazione garantiti e/o depositati dal soggetto produttore, nel caso questi siano i soli strumenti che consentono di rendere leggibili i documenti conservati associati a tale *viewer*.

METADATI

I metadati sono dati associati ai documenti da conservare in fase di formazione, per identificarli, descrivendone il contesto, il contenuto e la struttura, così da permetterne la gestione del tempo. Nei sistemi di conservazione sono anche utilizzati come chiavi di ricerca.

Le Linee Guida di AgID su formazione gestione e conservazione dei documenti informatici, all'**Allegato 5**, prevedono un set di metadati obbligatori per il documento informatico (maggiormente diffuso), il documento amministrativo informatico (pensato per le pubbliche amministrazioni) e per le aggregazioni documentali (come per esempio i fascicoli).
In breve:

Identificativo del Documento
Un set di metadati serve a identificare il documento da conservare. Si indica il numero utilizzato nel sistema di gestione documentale dove il documento viene formato e gestito, per es. documentID, o identificativo SdI per le fatture o ID SAP o DossierID. Si indica anche l'impronta di hash e l'algoritmo utilizzato (si suggerisce SHA-256).

Modalità di Formazione
Questo metadato serve a dichiarare come il documento da conservare è stato formato. Le possibilità sono:

- per 'creazione tramite l'utilizzo di strumenti software' (es. documenti scritti al pc)
- per 'acquisizione per via telematica o della copia per immagine' (es. documenti scansionati)
- per 'transazioni o processi informatici o moduli o formulari resi disponibili all'utente' (es. documenti compilati come form online)
- per 'generazione da registrazioni o banca dati' (es. estrazioni da database).

Tipologia Documentale
Metadato che può essere compilato con un valore fisso (default) per determinati processi e che indica per es. contratti, libri sociali, libri e registri contabili, fatture, determine, nota spese, ecc.

Dati di Registrazione
Questo set di metadati descrive un'eventuale registrazione del documento su un registro o repertorio prima del suo versamento in conservazione.

Il flusso può essere:

- in uscita se il documento viene spedito all'esterno dell'azienda/amministrazione
- in entrata se il documento è stato ricevuto dall'esterno
- interno se il documento resta all'interno dell'azienda/amministrazione che lo ha formato.

Il tipo di registro può essere:

- Nessuno
- Protocollo Ordinario/ Protocollo Emergenza
- Repertorio/Registro.

È necessario anche indicare la data e ora di registrazione e il numero attribuito al documento (es. numero del contratto, numero della nota spese, o nel caso dei libri sociali potrebbe coincidere con il

progressivo del verbale di assemblea o nel caso di libri fiscali il numero potrebbe essere un progressivo formato da mese e anno).

Oggetto
In questo campo si indica l'oggetto del documento, con particolare attenzione alle parole chiave con cui verrà ricercato in futuro.

Soggetti e Ruoli
Questo set di metadati indica i soggetti vari che sono coinvolti nella formazione e gestione del documento prima del suo versamento in conservazione.

I valori ammessi da AgID sono:

- assegnatario
- autore
- mittente
- destinatario
- operatore
- produttore
- RGD= Responsabile della Gestione Documentale
- RSP= Responsabile del Servizio di Protocollo
- Soggetto che effettua la registrazione
- Altro
- Amministrazione che effettua la registrazione
- RUP= Responsabile Unico del Procedimento

Almeno un soggetto che effettua la registrazione del documento (tipicamente l'Organizzazione che protocolla) e un autore o un mittente vanno indicati obbligatoriamente.

Questi set di metadati possono essere ripetibili.
Per es. possiamo indicare il mittente e il destinatario di una fattura, l'autore e il soggetto che effettua la registrazione di un libro sociale o fiscale, o di una nota spese, l'autore di un contratto.

Per ciascun ruolo è necessario poi specificare anche il tipo di soggetto, tra:

- AS per Assegnatario
- PF per persona fisica
- PG per organizzazione
- PAI per amministrazione pubblica italiana
- PAE per le Amministrazioni Pubbliche estere
- SW per i documenti prodotti automaticamente (Se Ruolo = Produttore)
- RUP per Responsabile Unico del Procedimento.

E per ciascuno si specificano poi rispettivamente nome, cognome (se PF) o denominazione (se PG), ed eventualmente anche il codice fiscale e gli indirizzi mail.

Allegati
Questo set di metadati serve a indicare se il documento da conservare ha allegati, quanti sono (valori ammessi: 0, 1, 2, 3…) e quali sono, legando il documento padre e i suoi allegati con un reciproco rimando, basato sul numero identificativo di ciascun documento.

Classificazione e Fascicolazione
Questo set di metadati, tipicamente utilizzato dalle pubbliche amministrazioni, indica il riferimento al titolo e alla classe del titolare/piano di classificazione, con la possibilità di inserirne la codifica, la descrizione e l'URI per un rimando puntuale.

È possibile indicare anche l'identificativo dell'aggregazione documentale (es. del fascicolo o della serie) a cui il documento da conservare fa riferimento.

Booleani
Alcuni metadati, definiti come 'booleani' vengono popolati solo con 'vero' o 'falso', indicando se il documento conservato è o non è riservato, è o non è firmato digitalmente, è o non è marcato temporalmente, è o non è sigillato, è o non è accompagnato da una certificazione di processo (se scansionato).

Formato
Un set di metadati indica il formato del documento da conservare (es. PDF, XML, ecc.), specificando opzionalmente anche il prodotto software, la versione e il produttore.

Nome File e Versione
Tra i metadati si indicano anche il nome file del documento da conservare e la sua versione (es. 1, 2, 3).
Se la versione è maggiore di 1, cioè si sta versando in conservazione un documento che è una rettifica o un'annotazione o integrazione di un documento già conservato, questa modifica va tracciata con un set di metadati che indica il tipo di modifica, l'identificativo della versione precedente, chi l'ha fatta e quando.

Tempo di Conservazione
Opzionalmente è possibile inserire tra i metadati anche il riferimento alle tempistiche di conservazione, per facilitare le attività di selezione e scarto.

Nei servizi erogati in ambito internazionale, i metadati sono concordati con il produttore, in base alla normativa locale e specifica.
Tipologie documentali e metadati sono sempre concordati con il soggetto produttore, e vengono elencati nelle 'Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA, che contengono anche delle note operative per una corretta metadatazione, secondo le Linee Guida AgID e nel 'file di configurazione', che descrive nel dettaglio l'ambiente di conservazione (bucket o Company).
Tuttavia, il produttore può in autonomia aggiungere ulteriori metadati ad ogni versamento.

tinexta
infocert

IL PROCESSO DI CONSERVAZIONE

I sistemi di conservazione sono erogati in modalità **SaaS** (*Software as a Service*) secondo uno schema di *Business Process Outsourcing* (BPO).
I servizi hanno l'obiettivo di mantenere e garantire nel tempo l'integrità, la leggibilità e la validità legale di tutti i documenti informatici conservati, nel rispetto della normativa vigente.

Il processo può essere così schematizzato:

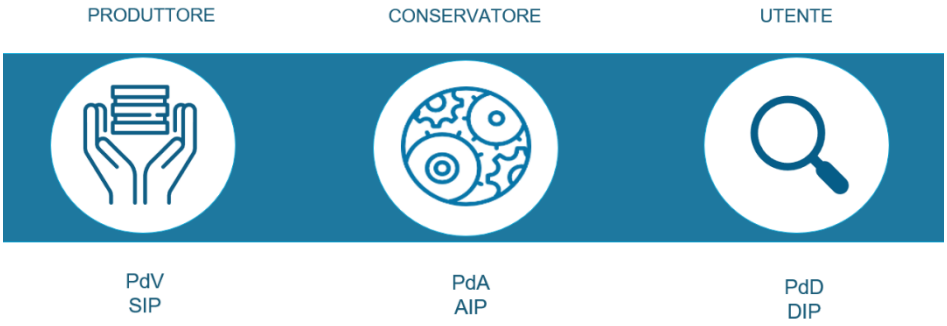


Figura 1 disegno di processo

1. *il produttore invia i documenti in conservazione con un pacchetto di versamento, contenente anche i metadati necessari;*
2. *il pacchetto viene preso in carico dal sistema se rispetta la configurazione concordata (formati, metadati, parametri, policy…) e se l'impronta di hash calcolata coincide con quella contenuta nel pacchetto;*

   in SAFE LTA, il sistema restituisce al produttore il link per potere reperire il rapporto di versamento;
3. *il sistema crea i pacchetti di archiviazione; il Responsabile del servizio sigilla e marca temporalmente l'indice di conservazione UNI SInCRO di ogni singolo pacchetto di archiviazione, a garanzia di integrità, immodificabilità e autenticità;*

   in LegalDoc, il sistema restituisce al produttore l'indice di conservazione come ricevuta (rapporto di versamento);
4. *il database del sistema viene aggiornato, il pacchetto di archiviazione viene indicizzato, memorizzato e ridondato più volte (ogni pacchetto è soggetto a controlli periodici di integrità e leggibilità a distanza di tempo);*
5. *il documento conservato può essere ricercato attraverso i metadati, su richiesta dell'utente in possesso delle apposite credenziali, in qualsiasi momento, ed esibito mediante un pacchetto di distribuzione, che contiene tutte le evidenze del processo.*

I sistemi consentono, quindi, le funzionalità di:

- **accettazione del pacchetto di versamento**, formato dal documento da conservare e dai metadati ad esso associati dal produttore;
- **conservazione del pacchetto di archiviazione**, a norma di legge e per tutta la durata prevista dal contratto;
- **rettifica del pacchetto di archiviazione**, modifica logica, nel pieno rispetto del principio di tracciabilità;
- **ricerca** tra i documenti conservati, utilizzando uno o più metadati popolati in fase di versamento;
- **esibizione del pacchetto di distribuzione**, contente sia il documento conservato che gli altri documenti a corredo della corretta conservazione, che possono essere scaricati in autonomia, in qualsiasi momento;
- **scarto**, su richiesta formale del Responsabile della conservazione del produttore, cioè cancellazione fisica e logica dei pacchetti di archiviazione e di ogni loro duplicato.

I sistemi di conservazione, quindi, integrano il sistema di gestione documentale del soggetto produttore, sia esso un'azienda o un ente, e ne estendono i servizi con funzionalità di archivio di deposito.
Le fasi di formazione e gestione dei documenti sono organizzate liberamente dal cliente/produttore all'interno del proprio sistema di gestione documentale, in quanto i servizi qui descritti intervengono solamente nella fase di conservazione e solamente per i documenti che il soggetto produttore sceglie di conservare.

CONTROLLI DI VERSAMENTO

In fase di versamento vengono automaticamente eseguiti dei controlli sui pacchetti:

- formato dichiarato del documento da conservare (mime type)
- correttezza della struttura dei pacchetti di versamento
- controlli formali di coerenza rispetto alla configurazione
- validazione dei tracciati dei file di indice (metadati)
- abilitazione utenza all'attività di versamento
- validità sessione in uso

secondo regole e policy concordate in fase di attivazione 'Specificità del Contratto – Scheda Dati Tecnici per LegalDoc o *Submission Agreement* per SAFE LTA di attivazione e File di configurazione'.

All'interno delle 'Specificità del Contratto' SPT/NDOCERR – Descrizione dei codici di errore di LegalDoc è presente la griglia riassuntiva dei codici errore che il servizio LegalDoc restituisce in seguito a situazioni che impediscono la corretta e completa esecuzione del servizio richiesto. I campi codice e descrizione vengono inseriti nel corpo della risposta HTTP.

La documentazione tecnica per integrare SAFE LTA con altri sistemi via API è disponibile su https://developers.infocert.digital/

Al terzo rifiuto del pacchetto, sarà necessario contattare il servizio di assistenza tecnica di InfoCert per tentare una soluzione del problema.

L'assistenza è contattabile mediante ticket https://help.infocert.it/

tinexta
infocert

PRODUZIONE DI COPIE O DUPLICATI

All'attivazione del servizio vengono concordate con il soggetto produttore le modalità di ricerca ed esibizione dei documenti conservati ('Specificità del Contratto' - 'Scheda Dati Tecnici di attivazione' per LegalDoc o *Submission Agreement* per SAFE LTA) e vengono create apposite credenziali (user/password).

Gli utenti abilitati possono in qualsiasi momento ricercare e scaricare pacchetti di distribuzione, attraverso interfaccia web o chiamate applicative.

Ogni documento informatico così scaricato in locale è da considerarsi un duplicato, ovvero il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (CAD art. 1 - i quinquies).

Laddove richiesto dalla natura delle attività, il Responsabile della Conservazione può in autonomia formare copie su diversi supporti dei documenti ottenuti dai pacchetti di distribuzione, anche con l'intervento di un pubblico ufficiale, a garanzia della loro conformità all'originale.

Anche il Responsabile del servizio può valutare il coinvolgimento di un pubblico ufficiale, in relazione all'evolversi dei formati e del contesto tecnologico dei sistemi.

VERIFICHE DI INTEGRITÀ E LEGGIBILITÀ

I sistemi di memorizzazione utilizzati, grazie alle caratteristiche intrinseche dei supporti, alla configurazione architetturale e alle procedure di memorizzazione permanente dei dati, garantiscono l'immodificabilità, l'integrità, la leggibilità e la reperibilità nel sistema di quanto conservato, ai fini della corretta esibizione.
I sistemi mantengono traccia di tutte le operazioni effettuate sui documenti in appositi file di log.
Inoltre, è garantita la tracciatura di tutti i documenti esibiti dal soggetto produttore mediante interrogazione al sistema e conseguentemente esibiti, che rappresenta un'ulteriore prova di leggibilità, effettuata direttamente dal soggetto produttore.
In aggiunta, InfoCert ha attivato sottosistemi di controllo automatico dedicati alla simulazione della navigazione nel sistema e delle operazioni che effettua l'utente, svolgendo controlli di coerenza dei dati e attività di ripristino da situazioni di errore.
In ogni occasione in cui il file viene copiato o spostato di posizione, funzionalità automatiche verificano che le sue dimensioni non siano mutate durante lo spostamento e che non siano intervenute alterazioni, che possano inficiarne la visualizzazione.
I servizi assicurano la **verifica periodica**, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi con procedure automatiche e manuali.
L'apposita procedura, detta **verificatore binario**, esegue il test di integrità mediante il continuo calcolo delle impronte dei documenti conservati, con successivo confronto con l'hash del documento contenuto nel file delle direttive della conservazione inviato dal soggetto produttore. Se la procedura non registra differenze tra i due hash, il documento è inalterato rispetto a quanto trasmesso dal produttore.

Vengono eseguiti i seguenti passi operativi:

- calcolo dell'impronta del documento;
- confronto con quella contenuta all'interno del file IPdA;

- generazione di un report che viene automaticamente sottoposto alla conservazione nell'area dedicata al Responsabile del servizio della conservazione (quindi a sua volta sigillato e marcato temporalmente dal Responsabile del servizio della conservazione stesso).

In caso di anomalie, se il documento risulta corrotto in uno dei repository, il sistema tenta il ripristino automatico con il dato presente nel repository integro. Se invece ambedue le copie sono alterate, viene inviato un *alert* al Responsabile del servizio della conservazione, che tenterà il ripristino manuale partendo da un'altra sorgente (per esempio le copie di backup). Se nessuna sorgente è disponibile viene redatto un verbale di incidente, sottoscritto e conservato dal Responsabile del servizio per attestare la situazione rilevata. Analoga procedura viene applicata in caso di perdita di tutte le copie del dato.
In aggiunta alla verifica automatica dell'integrità binaria, il Responsabile del servizio e i suoi Responsabili incaricati sono dotati di apposita strumentazione (detta CORE, **Console del Responsabile**), con credenziali dedicate, con la quale procedono manualmente e periodicamente ad una verifica campionaria di leggibilità 'umana' dell'archivio documentale conservato, scegliendo ed esibendo casualmente un campione di documenti presenti nel sistema di conservazione.
Anche in questo caso viene poi redatto automaticamente un verbale con gli identificativi dei documenti visualizzati, successivamente sottoscritto e conservato dal Responsabile del servizio.

SCARTO DEI PACCHETTI DI ARCHIVIAZIONE

I servizi di conservazione di InfoCert consentono lo scarto archivistico, cioè la **cancellazione di un pacchetto di archiviazione** e di qualsiasi suo duplicato prodotto durante le attività di conservazione, sia dal punto di vista logico che dal punto di vista fisico, su richiesta formale del Responsabile della conservazione interno al soggetto produttore/titolare del documento.
La procedura può essere attivata per varie ragioni, sia alla chiusura del contratto, sia in continuità di servizio (in itinere), per il venir meno della rilevanza amministrativa, legale o storica dei documenti conservati per il suo produttore, anche in relazione alla *retention period policy* configurata in fase di attivazione del servizio.
Il così detto **scarto in itinere** si può, quindi, richiedere al Customer Care di InfoCert tramite apposito **modulo**, oppure può essere attivato tramite **chiamate applicative**. In entrambi i casi è richiesta una lista di token firmata digitalmente dal Responsabile della Conservazione interno al produttore/titolare.
Per gli enti pubblici e per gli archivi privati dichiarati di notevole interesse storico, le richieste di scarto sono sottoposte a nulla osta delle soprintendenze archivistiche o delle commissioni di sorveglianza di competenza.
La distruzione degli eventuali supporti ottici rimovibili di back-up è effettuata mediante strumentazione adeguata e seguendo le procedure definite per lo smaltimento dei rifiuti prodotti.
Il Responsabile del servizio della conservazione mantiene traccia delle richieste di scarto ricevute e correttamente eseguite, e vengono redatti **Attestati di scarto** firmati digitalmente dal Responsabile del servizio.
Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover tra conservatori e scarto'.

HANDOVER E INTEROPERABILITÀ

Gli archivi di conservazione generati dai sistemi InfoCert sono conformi allo standard di interoperabilità **UNI SInCRO**. L'adozione di tale standard permette l'interoperabilità e la trasferibilità dei dati in modo semplificato.
Nel caso il soggetto produttore decida di rescindere, chiudere o interrompere il contratto di affidamento del servizio di conservazione, in qualsiasi momento può effettuare il **download** dei propri **pacchetti di distribuzione** in autonomia, attraverso la procedura di esibizione, o, in alternativa, richiedendo il **servizio di restituzione** (su supporto da concordare in base a volume ed esigenze) tramite apposito **modulo**.
Al termine della procedura di handover verso il nuovo Conservatore, i pacchetti verranno cancellati.
Seguendo i dettami dello standard OAIS, il versamento in InfoCert di pacchetti di distribuzione (PdD) provenienti da un altro Conservatore dovrà riguardare sempre **interi pacchetti**, qualsiasi sia il 'modo' con cui vengono formati e le tipologie di metadati o indici che hanno, e non dovrà mai riguardare il singolo documento. È fondamentale in questa procedura di versamento conservare in InfoCert quante più informazioni possibili sul processo di conservazione precedente e sul Conservatore di provenienza.
Per ulteriori dettagli si rimanda all'apposito documento interno 'Procedura di handover e scarto'.

RICERCA ED ESIBIZIONE DEI DOCUMENTI CONSERVATI

La ricerca e l'esibizione a norma dei documenti conservati può avvenire tramite chiamate applicative o tramite portale WEB.
Le chiavi di ricerca sono i metadati popolati in fase di versamento.
I sistemi restituiscono un pacchetto di distribuzione, contente sia il documento conservato che tutti i report e le evidenze di conservazione.
La guida al portale LegalDoc WEB è disponibile qui:
https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-legaldoc-web?lang=it
La guida al portale SAFE LTA WEB è disponibile qui:
https://knowledgecenter.infocert.digital/Home/Guida/manuale-utente-safe-lta

tinexta
infocert

I SISTEMI DI CONSERVAZIONE

I sistemi sono organizzati su più siti nel territorio italiano, con applicazioni software in architettura distribuita, molteplici componenti e con una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firme digitali e sigilli, supporti di conservazione).
I servizi sono accessibili online, tramite portale o chiamate applicative.
Dal punto di vista architetturale **LegalDoc** è realizzato utilizzando la tecnologia dei Web Services, secondo architettura REST su protocollo HTTPS. È erogato su cloud AWS e protetto da firewall configurati in alta affidabilità e costantemente aggiornati per assicurare i massimi livelli di protezione possibile. L'intero sistema viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria.
I sistemi sono collocati nella Region AWS Milano e utilizzano servizi AWS in modalità SaaS. Solo per un ristretto numero di Clienti viene utilizzato uno storage presente nel DataCenter di Milano.
Dal punto di vista architetturale **SAFE LTA** è erogato in modalità SaaS (Software as a Service): si basa su tecnologie open-source che incorporano le specifiche dei blocchi di costruzione dell'eArchiving (Programma CEF: *Connecting Europe Facility*) e incorporano gli standard comuni per i pacchetti informativi E-ARK (*European Archival Records and Knowledge Preservation*), in coerenza con lo standard ISO 14721 recante il reference model OAIS (*Open Archival Information System*) utilizzato a livello internazionale per la conservazione di risorse digitali.
Quindi, SAFE LTA è interamente erogato su cloud AWS.

Si tratta di un'applicazione basata su architettura a microservizi integrata con altri servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, firma digitale, sigillo elettronico qualificato, ecc.).

SAFE LTA è erogato come servizio in *Hybrid-Cloud architecture* attraverso provider AWS su zona geografica italiana e risiede entro perimetri di virtual private cloud per ragioni di sicurezza. Il servizio è da considerarsi ibrido in quanto fa uso di diversi servizi InfoCert.

I servizi sono:

- Identity Provider InfoCert, in quanto Provider ed erogatore di servizi riferiti alla identità digitale,
- SignAPI InfoCert, in quanto Provider ed erogatore di servizi legati alla Certification Authority.

Sia le applicazioni WEB di interfaccia sia le API REST sono adoperabili solo previa autenticazione:

- l'autenticazione da interfaccia web è governata attraverso flusso di *authorization-code-flow*, così come previsto da standard,
- l'autenticazione da agenti software che integrano le API REST è governata da flusso di *client-credential-flow*, così come previsto da standard.

SAFE LTA può essere facilmente integrato con altri sistemi attraverso API RESTful. Queste possono essere sfruttate nell'ambito di diverse funzionalità, incluse:

- Provisioning
- Gestione utenti, gruppi e autorizzazioni
- Invio in conservazione dei pacchetti di versamento e trasformazione in pacchetti di archiviazione E-ARK

- Attività di ricerca avanzata
- Recupero di documenti e metadati
- Download di pacchetti di distribuzione.

SAFE LTA non solo effettua la validazione di pacchetti di versamento, ma si occupa anche di effettuare una verifica formale dei formati.
L'autenticità dei dati inviati in conservazione è garantita dalla registrazione dei metadati PREMIS ogni qualvolta un'azione viene effettuata su un oggetto digitale.
Tutte le interazioni tra gli utenti e l'archivio sono registrate in appositi log per ragioni di sicurezza e trasparenza.
Ogni *endpoint* è protetto tramite autenticazione con Kong e Keycloak.

La configurazione degli ambienti di conservazione di SAFE LTA prevede le seguenti definizioni:

- **Company Group**: identifica un contenitore logico dal quale possono dipendere una o più Company, cioè aree di conservazione. Ogni Company Group è ad uso esclusivo di un solo cliente/titolare.
- **Company**: area di conservazione dei documenti, che può essere usata, ad esempio, per raggruppare i documenti delle diverse società/aziende di un gruppo (Company Group), denominando ogni Company con il nome della singola azienda facente parte del Gruppo.
- **Country**: identifica gli standard normativi adottati dal sistema per la conservazione rispetto alle varie geografie, ed è configurabile a livello di Company.
- **Document Class**: identifica una tipologia documentale con i suoi metadati. Ad esempio: fatture attive, contratti, libri e registri contabili, ecc.

La documentazione tecnica di dettaglio è disponibile su https://developers.infocert.digital/

SIGILLO DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, il Responsabile del servizio della conservazione di InfoCert appone un sigillo qualificato su ogni pacchetto di archiviazione. Fino al 2025 per LegalDoc è stata utilizzata una firma digitale automatica, con certificato intestato al Responsabile del servizio di conservazione di InfoCert (oggi viene utilizzato un sigillo qualificato a nome di InfoCert). Il servizio utilizza un sistema automatico erogato dalla CA - Certification Authority – InfoCert.

MARCA TEMPORALE DEI PACCHETTI DI ARCHIVIAZIONE

Al buon esito del processo di conservazione, viene apposta anche una marca temporale su ogni pacchetto di archiviazione. La marca temporale viene richiesta al TSS - *Time Stamping Service* - InfoCert, che la restituisce firmata con un certificato emesso dalla TSA - *Time Stamping Authority* - InfoCert. Il TSS è sincronizzato tramite i segnali forniti dai sistemi satellitari GPS, Galileo e GLONASS ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

STORAGE

L'intero sistema di conservazione viene interessato periodicamente da processi di back-up completo dei documenti, delle evidenze qualificanti il processo, dei database di gestione del sistema e di ogni altra informazione necessaria per la sicurezza.

Il sistema di conservazione di InfoCert e dei suoi partner tecnologici supporta la memorizzazione dei file sia su storage magnetici ad alte performance che su sistema Object Storage S3. Tali storage, scelti tra i primari fornitori di tecnologie presenti sul mercato, garantiscono adeguati requisiti di affidabilità e di ridondanza interna del dato e rispondono all'esigenza di memorizzazione a lungo termine dei *fixed content*, ossia dei file che devono essere conservati con garanzia nel tempo di integrità e disponibilità del contenuto.

Per garantire la riservatezza vengono applicate appropriate politiche sulle autorizzazioni che prevedano la cifratura dei documenti che contengono dati sensibili ed eventualmente anche degli altri.

I sistemi di storage sono stati valutati da InfoCert e dai suoi partner tecnologici sotto molteplici profili e, in virtù delle loro caratteristiche fisiche e architetturali, sono ritenuti idonei ad essere utilizzati nel sistema di conservazione.

Per il sistema di *Object Storage S3* InfoCert si avvale dei servizi cloud computing Amazon Web Services (AWS) che garantisce la ridondanza e il rispetto delle misure di sicurezza.

Per entrambi i servizi cloud è stata scelto AWS Europe (*Region Milan*), quindi, tutti i dati risiedono in **territorio italiano**.

SICUREZZA E PROTEZIONE DEI DATI

InfoCert si impegna a mantenere i più alti livelli di qualità e sicurezza, assegna un'importanza strategica alla gestione sicura delle informazioni e riconosce la necessità di sviluppare, mantenere, controllare e migliorare costantemente un **sistema di gestione della sicurezza delle informazioni (ISMS)** in conformità alla **norma UNI CEI EN ISO/IEC 27001: 2017**. Nella policy di sicurezza di InfoCert per ciascun capitolo della norma ISO vengono fornite le indicazioni da seguire nello svolgimento di tutte le attività. In particolar modo:

- *Management direction for information security,*
- *Organization of information security,*
- *Human resource security,*
- *Asset management,*
- *Access control, Cryptography,*
- *Physical and environmental security,*
- *Operations security,*
- *Communications security,*
- *System acquisition, development, and maintenance,*
- *Supplier relationships,*
- *Information security incident management,*
- *Information security aspects of business continuity management,*
- *Compliance with legal and contractual requirements.*

InfoCert ha anche ottenuto il **Report SOC 2 Tipo II**, su sicurezza, disponibilità, integrità del trattamento, riservatezza e privacy dei servizi, in conformità all'International **Standard on Assurance Engagements (ISAE) 3000**.
I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio. L'azienda ha mappato tutti i flussi di dati interni e di quelli da e per l'esterno. Sono implementati controlli automatici per evitare l'interconnessione con server esterni non autorizzati. L'accesso alla rete e ai sistemi è consentito esclusivamente agli utenti

autorizzati, seguendo quanto prescritto dalla policy aziendale relativa agli Amministratori di Sistema e alla gestione degli accessi logici. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione. Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity e al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti.
A supporto di tali censimenti è stato implementato un CMDB (*Configuration Management Data Base*).
Viene effettuata una valutazione di impatto sulla protezione dei dati personali. Il ciclo di vita dei dati è definito e documentato.
Tutti gli accessi (fisici e logici) sono regolati da policy apposite. I diritti di accesso sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni.
L'integrità di rete è protetta. Le reti di comunicazione e controllo sono protette.
I processi di risk management sono stabiliti, gestiti e concordati tra i responsabili.
Sono attivi ed amministrati piani di *Incident Response* e di *Business Continuity, Incident Recovery, Disaster Recovery e Vulnerability Management.*
I sistemi informativi, il personale e gli asset sono costantemente monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione. Sono implementati meccanismi che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse.
È attiva una policy di gestione dei log, inclusiva della conservazione dei log di sicurezza dei sistemi.
L'organizzazione ha implementato un processo formalizzato di *Incident Management* che include i criteri per documentare l'incidente ai fini del *problem management*, delle comunicazioni istituzionali e delle comunicazioni verso gli stakeholder.
Tutti gli utenti sono informati e addestrati.
Ai sensi del Regolamento UE n. 679/2016 GDPR, InfoCert assume il ruolo di Responsabile del trattamento dei dati personali. La nomina è inserita all'interno delle ''Specificità del Contratto – Atto di Affidamento''.
Il trattamento dei dati è effettuato:

- ai soli fini dell'erogazione del servizio,
- con l'adozione delle misure di sicurezza ex art. 32 del Regolamento
- nel rispetto degli obblighi posti in carico al Responsabile del trattamento dall'art. 28 del Regolamento.

PROCEDURE DI GESTIONE E MONITORAGGIO

I sistemi di conservazione di InfoCert e i processi da questi implementati rispondono interamente alle norme di legge che regolano la materia. La loro progettazione e il loro continuo miglioramento sono il frutto di una intensa opera di confronto tra le professionalità e le competenze delle diverse funzioni aziendali, al fine di giungere all'erogazione di servizi architetturalmente stabili, affidabili, e che garantiscano elevati livelli di servizio all'utente, in condizioni di assoluta sicurezza, certezza degli accessi e tracciabilità delle operazioni.
Punto fondante del processo di progettazione è l'attenta disamina delle norme e degli standard, al fine di definire puntualmente i requisiti di *compliance*. Oltre a questi sono definiti ulteriori requisiti funzionali, di architettura e di connettività e interoperabilità, anche in relazione con le evoluzioni tecnologiche,

sfruttando le economie di scala e di conoscenza. I Responsabili InfoCert, infatti, sono costantemente impegnati nell'attività di *technology watch* attraverso la partecipazione a gruppi di lavoro nazionali e internazionali, forum e associazioni di settore, con lo scopo di monitorare e prevenire l'obsolescenza tecnologica sia logica che fisica.
Inoltre, InfoCert ha deciso di adottare un sistema di gestione dei servizi IT (SMS) conforme a **ISO IEC 20000** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli SLA concordati.
Inoltre, InfoCert ha adottato un sistema di gestione dei servizi IT (SMS) certificato per la norma **ISO/IEC 20000-1:2018** (standard internazionale di gestione dei servizi IT) al fine di mantenere e migliorare la qualità dei servizi aziendali che fornisce. Questi hanno un'attenzione particolare alle esigenze dei clienti, sostenuti da un ciclo continuo di monitoraggio, reporting e revisione degli **SLA concordati**.
Tale modello di *Service Management System* ha permesso di:

- mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione ai Livelli di servizio operativi garantiti internamente e quelli contrattuali garantiti dai fornitori;
- strutturare e governare la catena di composizione del valore dei servizi;
- ottimizzare la gestione dei processi aziendali integrando processi produttivi con processi di business fornendo un modello per la gestione sui servizi erogati;
- facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti;
- garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi;
- migliorare la qualità dei servizi di business erogati.

Le attività di istituzione, attuazione, monitoraggio e sviluppo del Service Management System-SMS seguono il modello ciclico PDCA che si sviluppa nelle seguenti fasi:

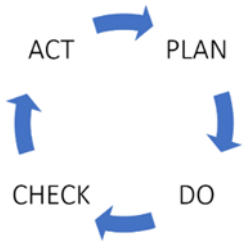


Figura 2 Rappresentazione del modello PDCA SMS

- istituzione del sistema - SMS (Plan) in cui si definiscono e si pianificano le politiche e i requisiti per la gestione dei servizi inerenti il campo di applicazione; si stabiliscono gli obiettivi di gestione del servizio a tutti i livelli pertinenti;
- implementazione ed attuazione del sistema-SMS (Do) e dei processi di design, transition, delivery e improvement continuo dei servizi sulla base di quanto definito nel service management plan, con particolare attenzione al controllo delle modifiche al SMS valutando e limitando I rischi;
- azioni di monitoraggio e revisione del sistema-SMS (Check);
- attuazione di misure a miglioramento del sistema-SMS (Act) ove sono pianificate e attuate idonee azioni correttive sulla base dei risultati della fase precedente.

Il processo di gestione dei Livelli di Servizio [Service Level Management] è considerato un processo cardine del Service Management System in quanto ha effetto sui tre obiettivi principali quali:

- allineare i servizi di business con i bisogni correnti e futuri del cliente
- coordinare i requisiti del mercato sui servizi offerti con gli obbiettivi aziendali
- migliorare la qualità dei servizi di business erogati
- fornire attraverso gli SLA una base per la determinazione del valore del servizio.

Nello specifico InfoCert ha definito degli SLA baseline di riferimento in relazione ai seguenti KPI (*Key Performance Indicator*):

- orario di servizio
- disponibilità di servizio.

Inoltre, InfoCert si è dotata di una soluzione di monitoraggio denominata **NEW RELIC**, un Software as a Service che permette la completa gestione dei dati ai team DEVOPS.
Questa è una piattaforma di osservabilità di secondo livello, in grado di identificare e prevedere problemi di tipo infrastrutturale e applicativo.
Utilizzando un evoluto sistema di gestione e raccolta dati effettua un monitoring full-stack, fornisce gli strumenti per la prevenzione e l'ottimizzazione dei servizi, oltre ad un'efficiente gestione di segnalazione degli incident. Inoltre, è stata sviluppata l'integrazione con la piattaforma di controllo ***Cloudwatch***, tool nativo di AWS, che consente di avere il pieno controllo e la gestione delle metriche di tutte le componenti presenti in cloud.

Il tool è composto da tre elementi fondamentali:

- AGENT: risiedono sui server e collezionano le metriche inviando (con connessione unidirezionale) i dati alla piattaforma centrale posta in cloud attraverso protocollo TLS. Gli agent effettuano un controllo sia di tipo infrastrutturale che di performance, consentendo anche la costruzione di schemi architetturali tra i servizi;

- NEWRELIC ANALYTICS PLATFORM: è il cuore dello strumento, dove vengono raccolte ed elaborate le metriche e che consente di gestire, aggregare ed elaborare i dati, definendo la modalità di visualizzazione e gestione degli alert;

- LOCATIONS: server nei quali risiedono gli script che simulano la user experience, possono essere privati o pubblici e grazie a questa diversa collocazione è possibile verificare il corretto funzionamento di un servizio sia della rete interna che da rete pubblica.

Con le metriche raccolte si popola una base di dati in ottica di *business intelligence*, che risulta di fondamentale importanza per la redazione della reportistica riguardante gli SLA dei vari servizi ma anche, e soprattutto, per supportare i processi di decisione aziendale.
La soluzione di monitoraggio fin qui descritta risulta indispensabile per individuare e prevenire tempestivamente anomalie sui servizi erogati da InfoCert, segnalando in modo puntuale le componenti impattate.

Il monitoring della disponibilità del servizio viene svolta coerentemente con le procedure generali di InfoCert. In particolare, tutte le componenti costituenti il sistema di conservazione, ovvero i servizi applicativi, i processi di elaborazione batch e le interfacce per l'utente finale, sono monitorate con i tool definiti nella piattaforma NEW RELIC precedentemente descritta.
A fronte di anomalie rilevate, lo strumento, grazie all'integrazione nativa, invia delle segnalazioni ad OPSGENIE, tool di gestione delle notifiche in conformità ai processi di Incident Management aziendali. Tali processi sono descritti nelle procedure che definiscono il Sistema di gestione integrato InfoCert.

CONTROLLI PERIODICI E AUDIT

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli del sistema per tutte le applicazioni. La struttura si avvale di un gruppo di lavoro trasversale, ed effettua la raccolta dei dati relativi al funzionamento dei servizi. Il gruppo si riunisce periodicamente, al fine di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.
Ad ogni semestre il Responsabile del servizio della conservazione effettua un riesame generale del sistema insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento. Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).
Inoltre, il programma di audit aziendale è attuato secondo le procedure del Sistema Integrato di Gestione, con il fine di determinare se i processi aziendali sono:

- in accordo con quanto previsto nei documenti di riferimento
- *compliant* alla normativa di riferimento
- *compliant* agli standard adottati dai sistemi di conservazione
- attuati efficacemente
- idonei al conseguimento degli obiettivi della Qualità e miglioramento servizi.

L'audit è un processo fondamentale per lo screening dei sistemi, in quanto consente l'individuazione delle aree critiche d'intervento e la pianificazione dei necessari interventi, ragion per cui è svolto periodicamente.
In ogni processo aziendale, le modalità di audit sono improntate alle indicazioni dello standard UNI EN ISO 19011 ed hanno per oggetto:

- strutture organizzative
- risorse utilizzate
- procedure
- processi
- prodotti e i risultati dell'attività
- documentazione
- addestramento
- segnalazioni dei clienti e terze parti.

Le attività di audit sono in capo all'area *Management System*, che le esegue direttamente o le delega a personale esterno qualificato.
A fronte di non conformità rilevate in sede di verifica ispettiva, il Responsabile del servizio valutata definisce un piano di attuazione delle azioni correttive o migliorative richieste.

SPECIFICITÀ DEL CONTRATTO

Le ***Condizioni Generali di Contratto*** o ***Accordo Quadro*** regolano la vendita in generale di tutti i servizi InfoCert.

A questi tipicamente si aggiungono i seguenti allegati:

- **Allegato A – Offerta Commerciale,**
- **Allegato B – DPA - *Data Processing Agreement*,**
- **Allegato C – Allegato Tecnico,**
- **Allegato D – Misure di Sicurezza,**
- **Allegato E – Manuale Operativo**, cioè il presente manuale.

Nell'**Allegato C – Allegato Tecnico** sono descritte le condizioni particolari di LegalDoc e SAFE LTA ed è inserito l'***Atto di Affidamento***, che rappresenta la formalizzazione della delega ad InfoCert del servizio di conservazione e stabilisce espressamente quali attività di fatto vengano assunte da InfoCert e quali, al contrario, rimangano a carico dell'affidatario, soggetto produttore, come stabilito dalle Linee Guida AgID.
Qui è maggiormente dettagliata anche l'infrastruttura tecnica e l'architettura di ciascun servizio.
Sono richiamati anche la ***Scheda dati tecnici d'attivazione*** per LegalDoc e il ***Submission Agreement*** per SAFE LTA, con cui il soggetto produttore/cliente/titolare fornisce tutte le informazioni necessarie su tipologie documentali, metadati, formati e utenze di accesso, per la configurazione degli ambienti di conservazione.

tinexta
infocert

think next,
trust now

Registro cronologico delle verifiche effettuate dal Responsabile della conservazione

Data	Tipo di controllo	Classe documentale	Descrizione controllo	Esito	Eventuali note
04/05/25	Verifica Rapporto di versamento	Registro giornaliero Protocollo	Verifica della corretta ricezione del Rapporto di versamento dal conservatore esterno e relativa analisi del contenuto	Positivo	