



Istituto Romano di
San Michele

**Manuale di Conservazione
e
Piano 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.*

Approvato con Deliberazione del CdA n. 16 del 21/06 2022

Introduzione	3
1 Terminologia (Glossario e acronimi).....	4
2 Normativa di riferimento.....	7
3 Modello Organizzativo dell'Ente.....	10
3.1 Conservazione in outsourcing	11
4 Ruoli e responsabilità	12
4.1 Titolare dell'oggetto della conservazione.....	12
4.2 Utente/Fruitore	12
4.3 Responsabile della Conservazione	12
4.4 Responsabile del Servizio di Conservazione	14
5 Formati e Metadati.....	14
6 Oggetti sottoposti a conservazione	15
6.1 Tipologie documentali da inviare in conservazione	16
7. Processo di Conservazione	17
7.1 Tipologie di pacchetti informativi.....	18
7.2 Pacchetto di versamento	18
7.3 Pacchetto di archiviazione.....	18
7.4 Pacchetto di distribuzione	18
7.5 Modalità di acquisizione dei Pdv per la loro presa in carico.....	19
7.6 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti.....	19
7.7 Accettazione dei Pdv e generazione del rapporto di versamento e di presa in carico.....	20
7.8 Rifiuto dei PdV e modalità di comunicazione delle anomalie	20
7.9 Preparazione e gestione del PdA	21
7.10 Preparazione e gestione del pacchetto di distribuzione ai finidell'esibizione.....	21
7.11 Produzione di duplicati e copie informatiche ed eventuale intervento del pubblico ufficiale	22
7.11.1 Produzione di duplicati informatici	22
7.11.2 Produzione di copie informatiche ed estratti di documenti informatici.....	22
7.12 Scarto dei pacchetti di archiviazione	22
7.13 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	23
7.14 Conservazione delle comunicazioni intercorrenti tra il SdC e i fruitori del SdC.....	23
8. Il Sistema di Conservazione	24
9. Monitoraggio e controlli.....	24
9.1 Procedure di monitoraggio applicativo	24
9.2 Procedure di monitoraggio infrastrutturale	24
9.3 Verifica dell'integrità degli archivi	24
9.4 Soluzioni adottate in caso di anomalie.....	25
9.5 Sicurezza del SdC	25
10. Approvazione e aggiornamento del Manuale	25

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 norma dei 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 della Istituto Romano di San Michele 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.

L'Istituto Romano di San Michele 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 porre in essere 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'Istituto Romano di San Michele 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 dell'Istituto Romano di San Michele 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 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. 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 dalla 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 è tratto.
Copia per immagine su supporto informatico di documento analogico	Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.
Documento	Viene definito documento una rappresentazione di atti, fatti e dati su un supporto sia esso cartaceo o 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 tra questi 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 informatico non 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 altri dati 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 elettronica qualificata - 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 sistema di 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 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.
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 agli oggetti 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 a proteggere 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 quanto conforme 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 di conservazione dei pacchetti di versamento inviati dal produttore.

Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti 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 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.
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 riguardo al 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

L' Istituto Romano di San Michele è costituito da unico codice AOO:

CODICE UNIVOCO AOO	AE50895
DOMICILIO DIGITALE	istitutoromanosanmichele@pcert.postecert.it (dal 12/04/2019 ad oggi)
INDIRIZZO	Piazzale Antonio Tosti n.4 - Roma (RM)

La struttura, in continuo aggiornamento ed evoluzione può essere consultata all'indirizzo www.indicepa.gov.it L'ente è organizzato in unica Unità Organizzativa; l'organigramma aggiornato dell'Ente può invece essere consultato nell'apposita sezione di "Amministrazione trasparente".

L'Istituto Romano di San Michele 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	ISTITUTO ROMANO DI SAN MICHELE
Codice Fiscale	80112430584
Codice AOO	AE50895
Codice IPA	irms_rm
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale.	Piazzale Antonio Tosti n.4 - Roma (RM)
Casella di posta elettronica istituzionale della AOO	istitutoromanosanmichele@pcert.postecert.it

Nomine:

Nominativo del Responsabile del Servizio di Protocollo informatico e gestione documentale ; Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del DPR 28 dicembre 2000, n. 445.	SILVANA CIANFARANI Determina Direttoriale n.334 del 8/6/2021 (in allegato)
Nominativo del Responsabile della Conservazione documentale ; definisce le politiche del sistema di conservazione e predispose il manuale di conservazione, è il soggetto cui fa capo la responsabilità di verifica del corretto svolgimento del processo di conservazione.	SILVANA CIANFARANI Determina Direttoriale n.334 del 8/6/2021 (in allegato)
Nominativo del Responsabile della Transizione Digitale	MARCO GRASELLI Determina Direttoriale n.334 del 8/6/2021 (in allegato)

3.1 Conservazione in outsourcing

L'Istituto Romano di San Michele (soggetto titolare dell'oggetto della conservazione) realizza i processi di conservazione all'interno della propria struttura organizzativa affidandoli ad un conservatore accreditato 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 al Conservatore 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 al 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***
- ***Produttore dei PdV***
- ***Utente abilitato***
- ***Responsabile della Conservazione (lato produttore)***
- ***Responsabile del Servizio di Conservazione (RSC)/Conservatore***

Nelle pubbliche amministrazioni, il ruolo di *Produttore del PdV* è svolto da persona interna alla struttura organizzativa. L'*Utente abilitato* può richiedere al SdC l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

4.1 Titolare dell'oggetto della conservazione

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

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

4.2 Utente/Fruitore

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). Pertanto il fruitore rappresenta la comunità degli utenti di riferimento principale; ad essa si affiancano ulteriori soggetti che, nel rispetto della normativa vigente, accedono all'informazione.

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.

4.3 Responsabile della Conservazione

Il Responsabile della Conservazione è la figura cardine che governa il processo della conservazione digitale: è la persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità

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 competenze giuridiche, informatiche ed archivistiche;
- c. può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

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 come previsto dal par. 4.11;
- 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. provvede per le amministrazioni statali centrali e periferiche a versare i documenti Linee Guida sulla formazione, gestione e conservazione dei documenti informatici³⁶ – 41 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;
- m. predispone il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui, come per l'Istituto Romano di San Michele, il Servizio di Conservazione venga affidato ad un conservatore esterno, le attività suddette o alcune di esse, ad esclusione della lettera m), 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 dalle PA.

4.4 Responsabile del Servizio di Conservazione

Il Responsabile del Servizio di Conservazione è il soggetto conservatore nominato dal produttore a svolgere il servizio di conservazione in relazione alla normativa vigente ed alle condizioni sottoscritte nel contratto di Servizio. 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 piena responsabilità 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.

L'Istituto Romano di San Michele gestisce il Sdc attraverso un conservatore accreditato che dispone di un processo tecnico e organizzativo certificato e validato da strutture esterne qualificate nel settore.

Profilo del Conservatore	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
---------------------------------	--

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 tale scopo, 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 amministrativi informatici 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. Sono infatti 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 oggetti informativi 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 normativa vigente.

Durante la vita nel Sistema di gestione corrente, il documento è sottoposto ad una serie di azioni (es. *protocolloazione 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 e la 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, 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 webservice 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'ente riversa in conservazione dalla Piattaforma Gestionale cloud in uso:

Tipologia documento Conservazione	Tempo di conservazione	Versamento – periodicità	Formato doc.
Deliberazioni del Consiglio di Amministrazione	Illimitata	Versamento periodico da Civilia Next	Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades)
Determinazioni Direttoriali e Dirigenziali	Illimitata	Versamento periodico da Civilia Next	Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades)
Ordinanze del Presidente	Illimitata	Versamento periodico da Civilia Next	Pdf, pdf/A, documenti

			con firma digitale (Pades, Cades, Xades)
Contratti	Illimitata	Versamento periodico attraverso piattaforma ad hoc del Conservatore Enerj	Pdf, pdf/A, documenti con firma digitale (Pades, Cades, Xades)
Registro giornaliero di protocollo	illimitata	Versamento giornaliero da Civilia Next	Pdf/A
Fatture elettroniche	10 anni	Le fatture passive vengono riversate periodicamente da Civilia Next.	XML

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 l'Istituto Romano di San Michele per i servizi di conservazione documentale:

Conservatori	Tipologie documentali riversate	Periodo di riferimento
Enerj	Protocollo e Atti Amministrativi	2022 - attualmente
POSTEL	Protocollo	2016 - 2021

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 conservazione documentale identifica, 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 conservazione del 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'utente in risposta ad una sua richiesta. E' un pacchetto informativo che viene ricevuto da un utente come risposta a una 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 11386:2010 Standard SInCRO (Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti Digitali).

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

- Informazioni relative al cliente Produttore (Codice anagrafico, Ragione Sociale, 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 dai soggetti autorizzati 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 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, 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*
- *referimenti 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 le 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 le operazioni eseguite dagli utenti e dai processi informatici relative ai PdV rifiutati dal SdC vengono storicizzate su appositi log.

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 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.

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 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.

7.11.3 Produzione di copie informatiche di documenti analogici

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

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

- *verifiche sull'integrità degli archivi conservati*
- *verifiche sulle copie di sicurezza dei dati*
- *security testing and evaluation (STE): strumenti comprendenti un'ampia gamma di tests sui sistemi;*
- *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, 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 suddetti 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.

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 analisi dei rischi inerenti il Sistema di conservazione.

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).

10. Approvazione e aggiornamento del Manuale

L'Istituto Romano di San Michele 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 22 giugno 2022

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".

