S.A.P. NA.

Sistema Ambiente Provincia di Napoli S.p.A. a socio unico

Gestione Documentazione
Sede Operativa e Impianti
Flusso Protocollo e Distribuzione Posta

PO.07.2014

	UNITA' ORGANIZZATIVA	FIRMA
Redatto da:	*Ufficio Affari Generali*	*C. Boninfante – M. Lebotti*
Approvato da:	*Amministratore Unico*	*Dott. G. Gargano*
Pubblicazione:	*Ufficio Affari Generali*	

REVISIONE	DATA	DESCRIZIONE
00 – I° emissione	Giugno 2014	Procedura Operativa n.07
01 – Revisione 01	Agosto 2016	Aggiornamento per utilizzo protocollo Software Folium
02 – Revisione 02	Agosto 2022	Aggiornamento normativo-Estensione a TMB e Siti in gestione

SOMMARIO

APPENDICI:

Appendice 1 Manuale di gestione del Protocollo informatico dei flussi documentali e degli Archivi – DEDAGROUP-*Redatto ai sensi degli articoli 3 e 5 del D.P.C.M. 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"*

Appendice 2 Manuale sulla conservazione dei documenti prodotti da SAPNA SpA. –di ENERJ-

1. PREMESSA

Il presente documento ha lo scopo di identificare, regolamentare e tracciare il flusso dei documenti in entrata/uscita dalla SAPNA SpA.

Tale procedura è necessaria al fine di garantire criteri di tracciabilità, reperibilità del documento/informazione, corretta identificazione del mittente e del destinatario, nonché di corretta informazione e diffusione del documento ai preposti degli Uffici, alle Segreterie (qualora presenti) delle le Aree Operative, alla Segreteria Tecnica, alla Segreteria Generale e/o al personale interessato, affinchè questi provvedano alla corretta e tempestiva informazione del competente Responsabile dell'area aziendale, il quale entro i limiti previsti dalle proprie competenze, mansioni e responsabilità, provvederà altrettanto tempestivamente alle azioni consequenziali derivanti dalle informazioni e/o dai documenti ricevuti.

L'obiettivo è quindi quello di conseguire, attraverso il corretto flusso della documentazione, sia il controllo dell'informazione e/o del documento stesso, che l'effettiva e corretta assegnazione dell'informazione al destinatario competente, rispettando criteri di efficacia e di rispetto della riservatezza del dato ed in osservanza alle disposizioni AGID vigenti.

Pertanto il flusso documentale dovrà assicurare l'assegnazione al corretto destinatario - e quindi l'azione amministrativa attesa e l'identificazione delle responsabilità – nonché il corretto trattamento dei dati contenuti nel documento, secondo le procedure aziendali, affinché vengano impedite la diffusione impropria o errata di informazioni e, di conseguenza, il ritardo o l'assenza dell'azione amministrativa attesa.

Sono presupposti necessari:

1) la centralizzazione degli archivi sia in materia amministrativa che tecnica, applicando il procedimento di "smaterializzazione" e usando per quanto possibile tecniche digitali, sfavorendo l'uso del cartaceo,

2) procedere ad una opportuna classificazione/identificazione dei documenti sia tecnici che amministrativi, attribuendo ad essi il necessario protocollo ed indicandone la localizzazione fisica, anche se digitale, ai fini della conservazione sostitutiva,

3) il divieto di tenere archivi "personali" di documentazione aziendale: è d'obbligo da parte di tutti i dipendenti SAPNA SpA evitare di tenere o costituire *archivi paralleli* sia cartacei che in formato elettronico (cartelle/directory in server) che non siano quelli istituzionali e che in qualsiasi modo ne comportassero l'irreperibilità, l'indisponibilità, l'invalidità del documento aziendale o l'esistenza di documentazioni aziendali non correttamente archiviate, o conservate, o per le quali in qualsiasi modo ne sia impedita la condivisione o l'accesso,

4) impedire la diffusione indebita sia all'interno della società che verso l'esterno, delle informazioni, incluso al personale non coinvolto nell'azione richiesta, e sfavorire la diffusione di protocolli riservati, classificati e/o secretati, o comunque di documenti aziendali,

5) applicare criteri di massima trasparenza e disponibilità dell'informazione secondo quanto stabilito dalle procedure interne di accesso agli atti e secondo quanto previsto dalle vigenti Leggi.

La regolamentazione del flusso delle informazioni e documenti da e verso l'Azienda, atteso il contributo di tale azione ai fini del raggiungimento dello scopo sociale della S.A.P.NA., in uno al costante interfacciarsi con le altre procedure aziendali, costituisce uno degli elementi fondamentali per la corretta gestione ed esecuzione dei compiti istituzionali.

La presente procedura è da considerarsi, altresì, presidio per la prevenzione dei reati di cui al D.Lgs 231/01 e ss. mm. e ii. ed è inserita tra le azioni procedurali previste dal Piano Triennale di Prevenzione Corruzione e Trasparenza di questa SAPNA SpA.

2. GENERALITA'

2.1. Riferimenti

La presente procedura fa riferimento a:

- Leggi della Repubblica Italiana;
- Legge n. 26 del 26.02.2010 e ss. mm. e ii.;
- Statuto Aziendale;
- Decreto Legislativo 30 giugno 2003 n. 196 e ss. mm. e ii.;
- Decreto Legge n. 5 del 9 febbraio 2012, convertito in legge n. 35 del 4 aprile 2012;
- Conversione in Legge n. 134 del 7 agosto 2012 del DL 22 giugno 2012, n. 83 Titolo II-Misure urgenti per l'Agenda Digitale e la Trasparenza nella Pubblica Amministrazione;
- Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n.82 e successive integrazioni e modificazioni;
- AGID Agenzia per l'Italia Digitale: indirizzi, regole tecniche, linee guida e metodologie progettuali in materia di tecnologie informatiche;
- GPDP Garante per la Protezione dei Dati Personali: delibere, autorizzazioni, provvedimenti, linee guida;
- Codice Etico aziendale S.A.P.NA. S.p.A.;
- Procedure e Regolamenti vigenti in S.A.P.NA. S.p.A.;
- Modello di Organizzazione e Gestione, Rev. III Ottobre 2020 S.A.P.NA. S.p.A.;
- Regolamento Organismo di Vigilanza S.A.P.NA. S.p.A.;
- Piano Triennale per la Prevenzione della Corruzione (PTPC) – Programma Triennale per l'Integrità e la Trasparenza (PTIT);
- Manuale di gestione del Protocollo informatico dei flussi documentali e degli Archivi Appendice 1 alla presente procedura;
- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e ss. mm. e ii. così come consolidato dal Dlgs 28 dicembre 2001, n. 467;
- Decreto Ministro dell'Economia e Finanze 23 gennaio 2004, *Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto;*
- Servizio di Conservazione Sostitutiva fornito dalla Enerj (certificazione AGID Rif. Circolare n. 65 del 10 aprile 2014), *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.*

2.2. Definizioni

Si riportano di seguito le definizioni usate nel presente documento:
"S.A.P.NA. S.p.A." o più semplicemente SAPNA SpA: la società Sistema Ambiente Provincia di Napoli a Socio Unico per Azioni, interamente partecipata dalla Città Metropolitana di Napoli – soggetto al quale è applicata la presente procedura. Nel presente documento è definita anche AZIENDA;
"CMN": la Città Metropolitana di Napoli, Ente pubblico unico proprietario, che detiene il coordinamento e controllo di S.A.P.NA. S.p.A.;
"Sede operativa": gli uffici della sede operativa ubicati in Via Ponte dei Francesi, 37/E – Napoli;
"Area Operativa": le aree operative aziendali singole o raggruppate in settori o uffici e identificate dall'organigramma aziendale di cui all'allegato "A" della determinazione dell'Amministratore Unico del 25.05.2021 e successive integrazioni di cui alle determinazioni del 20.01.2022 e 04.02.2022;

"Responsabile": il Responsabile della singola area operativa o dell'Ufficio, così come identificato nei paragrafi del presente documento. Nel caso di RUP è inteso quale responsabile del procedimento amministrativo avviato;
"Trattamento": qualunque operazione o complesso di operazioni, effettuati con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, cartacei o digitali, anche se non registrati in una banca di dati;
"Folium": la piattaforma operativa del sistema di protocollazione in uso in tutta la SAPNA SpA il cui accesso da parte degli utenti è regolato da apposita graduazione di livello operativo;
"Protocollo": l'attività di attribuzione, attraverso Folium, di un numero identificativo progressivo unico, non sostituibile, ai documenti in entrata o in uscita ed alle comunicazioni interne, generato dal sistema di archiviazione in uso alla SAPNA SpA. E' usato anche per abbreviare, per estensione, nell'ambito della Segreteria di Direzione, il c.d. "ufficio protocollo" che ne è parte;
"Repertorio": l'attribuzione, attraverso Folium, di un numero identificativo progressivo unico, non sostituibile, agli atti che necessitano di una classificazione d'archivio inserita in una determinata raccolta, come ad esempio il repertorio dei contratti, il repertorio delle determinazioni, etc.
"Conservazione": l'attività che permette, attraverso Folium, al documento protocollato di essere acquisito come file digitale, "bloccato" nella forma, non modificabile, inserito e conservato presso un sito certificato;
"Conservazione sostitutiva": è una procedura legale/informatica, nel caso di SAPNA effettuata tramite Folium, regolamentata dalla Legge, in grado di garantire nel tempo la validità legale di un documento informatico, inteso come una rappresentazione di atti o fatti e dati su un supporto sia esso cartaceo o informatico (delibera CNIPA 11/2004). La conservazione sostitutiva equipara i documenti cartacei a quelli elettronici e permette notevoli risparmi su stampa, stoccaggio e archiviazione, con particolare riferimento ai documenti che devono essere conservati per più anni;
"Archivio": insieme ordinato e sistematico di atti, scritture e documenti prodotti e/o acquisiti da un soggetto pubblico o privato durante l'esercizio delle proprie attività e/o funzioni, che siano stati inviati e conservati in forma cartacea o digitale per la consultabilità e la fruizione, presso un determinato luogo. Nel caso specifico di SAPNA SpA l'archivio è di tipo cartaceo dall'anno 2010 fino al 2016 e dal 2016 in poi è tenuto per il tramite di Folium in modalità smaterializzata;
"Classificazione": è l'organizzare tutti i documenti, per il tramite di Folium, secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione o dell'area aziendale interessata, graduando il documento secondo gradi di accessibilità;
"Fascicolo": è l'insieme degli atti, documenti, informazioni, dati, conservati, per il tramite di Folium, in forma digitale, riferiti ad un unico argomento di trattamento, ovvero ogni fascicolo contiene documenti che sono prodotti nel corso di uno stesso procedimento o attività, classificati in maniera omogenea, in base al contenuto e secondo il grado divisionale attribuito dal titolario (o piano di classificazione). La corretta tenuta del fascicolo garantisce l'esercizio del diritto di accesso;

Sono inoltre usate le seguenti sigle e/o abbreviazioni:

AGID Agenzia per l'Italia Digitale
ANAC Autorità Nazionale Anticorruzione
CMN Città Metropolitana di Napoli – Socio Unico partecipante della S.A.P.NA. S.p.A.
ATO Ambito Territoriale Ottimale - Legge Regione Campania 14/2016

EdA Ente d' Ambito - Legge Regione Campania 14/2016
OdV Organismo di Vigilanza ex Dlgs 231/2001 della S.A.P.NA. S.p.A.
CdS Collegio dei Sindaci della S.A.P.NA. S.p.A.
PA Pubblica Amministrazione (generico)
PTPCT Piano Triennale Prevenzione Corruzione e Trasparenza ex Dlgs 97/2016
RPCT Responsabile della Prevenzione della Corruzione e per la Trasparenza
SAPNA Sistema Ambiente Provincia di Napoli a Socio Unico SpA
AU Amministratore Unico della S.A.P.NA. S.p.A.
DT Direzione Tecnica
AT Area Tecnica (e le unità operative in essa comprese: Contabilità, Ingegneria, Servizi Tecnici, Flussi, Impianti TMB, Siti e Discariche)
ST Segreteria Tecnica
TMB Impianto di Trattamento Meccanico e Biologico
RSPP Responsabile del Servizio di Prevenzione e Protezione
RUP Responsabile Unico del Procedimento
UAP Ufficio Amministrazione del Personale
UAF Ufficio Amministrazione e Finanza
UGC Ufficio Gare e Contratti
UAG Ufficio Affari Generali
AG unità operativa Affari generali in forza all'ufficio UAG
UL unità operativa Legale in forza all'ufficio UAG
SG unità operativa Segreteria Generale in forza all'ufficio UAG
UP unità operativa Protocollo in forza all'ufficio UAG
RS Relazioni Sindacali

2.3. Responsabilità e azioni

Sono responsabili dell'applicazione del presente documento:
- I Responsabili delle Aree Operative della SAPNA SpA;
- Il personale in forza alle singole aree operative, limitatamente alla fase esecutiva.
- I settori che identificano le singole aree operative aziendali sono i seguenti:
  - **A.** Tecnica Operativa
    - Direzione Tecnica
    - Segreteria Tecnica
    - Area Tecnica (contabilità, ambiente, flussi, servizi, etc.)
    - Prevenzione e Sicurezza sul Lavoro
    - Impianto TMB di Giugliano
    - Impianto TMB di Tufino
    - Siti e Discariche
  - **B.** Amministrativo finanziario e contabile
    - Ufficio Amministrazione e Finanza
  - **C.** Approvvigionamenti
    - Ufficio Gare e Contratti
  - **D.** Risorse Umane
    - Ufficio Amministrazione del Personale
    - Formazione
  - **E.** Affari Generali
    - Ufficio Affari Generali
    - Area Legale e Societario
    - Relazioni Sindacali
    - Prevenzione della Corruzione e Trasparenza
    - Segreteria Generale
    - Comunicazioni Istituzionali

- Protocollo

3. GESTIONE DOCUMENTAZIONI – GENERALITÀ E MODALITÀ OPERATIVE[1]

Il trattamento dei documenti e la gestione operativa relativa all'acquisizione e distribuzione degli stessi è effettuata in SAPNA SpA esclusivamente per il tramite del sistema protocollare FOLIUM, software licenziato e certificato posto nelle disponibilità di tutte le unità operative di SAPNA SpA nonché utilizzato - con apposita e diversa licenza - dal Socio Unico CMN e da altri Enti Locali e PA.
Il sistema protocollare siffatto utilizza tre metodologie di identificazione della documentazione, separandola secondo le seguenti MODALITA' di flusso:

- **INGRESSO**
- **USCITA**
- **INTERNA**

I numeri identificativi di protocollo, indipendentemente dalla modalità di flusso del documento, se in ingresso o uscita, o interna saranno attribuiti automaticamente dal sistema e saranno comunque progressivi.
Tutta la documentazione protocollata nelle rispettive modalità, è inserita in un REGISTRO UFFICIALE che è caratterizzato da una successione di elementi identificativi ordinati per Numero (ovvero protocollo attribuito), Data e Ora, Modalità, Oggetto, Mittente/Destinatario, Ufficio Mittente-Ufficio Destinatario, Contenuto ed Operazioni eseguite.
Il documento una volta acquisito (in una qualsiasi delle modalità Entrata-Uscita-Interna) e digitalmente etichettato e salvato in formato *.pdf, **non potrà essere più modificato** e sarà reso disponibile anche per gli usi di conservazione sostitutiva.
L'acquisizione del documento avverrà per il tramite di apposito scanner se è cartaceo o direttamente tramite il sistema protocollare se è in formato digitale.

Gli elementi che, in via generale, contraddistinguono il documento sono essenzialmente le seguenti:

- Indirizzo a cui è destinato il documento
- Nominativo (o nominativi) a cui è destinato il documento
- Oggetto
- Testo
- Protocollo del mittente con data ed eventualmente ora
- Eventuali allegati
- Firma del soggetto mittente (autografa o digitale)

---

[1] E' mutuato ai fini della presente procedura, il Codice dell'Amministrazione Digitale, **D.Lgs. 7 marzo 2005, n.82 Art. 47**. *Trasmissione dei documenti tra le pubbliche amministrazioni*
1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Il documento può essere, altresì, reso disponibile previa comunicazione delle modalità di accesso telematico allo stesso.1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. È in ogni caso esclusa la trasmissione di documenti a mezzo fax;
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
Le pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

- Riferimenti, se presenti, del redattore del documento

Il documento siffatto, una volta protocollato quale "documento principale" potrà pertanto essere solo annullato[2] (con evidenza nel registro e relativa motivazione) o dotato di allegati che possono essere anche aggiunti successivamente, al solo fine di completamento del file per consultazione/archivio. Qualora si rendesse necessario aggiungere ulteriori elementi sostanziali e/o modificativi del file in uscita, la comunicazione dovrà essere ritrasmessa seguendo l'iter previsto per la posta in uscita.
Per altre caratteristiche del sistema ed operazioni si rimanda all'Appendice 1 della presente procedura.
Particolare cura dovrà essere posta nell'attribuzione dell'oggetto in fase di protocollazione al fine di favorire la rintracciabilità del documento in caso di ricerca, utilizzando criteri di omogeneità escludendo l'attribuzione di dizioni diverse per lo stesso oggetto.

3.1 Posta in ENTRATA – Accettazione del documento

Per "Posta in ENTRATA" si intendono tutti i documenti che, dall'esterno, pervengono e/o sono indirizzati:

- alla SAPNA SpA
- all'Amministratore Unico di SAPNA SpA
- a Rappresentanti della SAPNA SpA Delegati o Procurati
- a Dirigenti, Quadri, Responsabili, Coordinatori di SAPNA SpA
- ad un qualsiasi ufficio o area operativa, sito o impianto della SAPNA SpA
- a personale dipendente della SAPNA SpA facente parte dei summenzionati uffici, aree o impianto/sito.

Modalità di accettazione, identificazione del documento[3]
I documenti indirizzati alla SAPNA SpA (flusso in entrata del documento) sono accettati quali "**posta IN INGRESSO"** e possono essere ricondotti alle seguenti tipologie:

a) **di norma,** tutti i documenti in formato digitale ricevuti nella casella di **posta certificata (PEC)** di SAPNA SpA, sapna@pec.it trasmessi da soggetti esterni a quest'ultima, costituiti o dal solo corpo del messaggio della mail o, a mezzo della stessa modalità, dotato di firma autografa o digitale del mittente con allegato documento in formato digitale (*.pdf, *.xls,*.doc, etc.) o senza allegato. E' altresì considerata *posta in entrata* il documento firmato e trasmesso a mezzo PEC da Collegio dei Sindaci, OdV, RPCT indirizzata alla SAPNA SpA o all'Organo Amministrativo o a qualsiasi altro dipendente SAPNA SpA;

b) a mezzo semplice posta elettronica aziendale (PEA) nominativa. In tal caso il documento viene acquisito e trattato come descritto nei successivi paragrafi;

Fermo restando l'orientamento di SAPNA SpA al trattamento dei documenti in forma digitale quale prassi consolidata, non possono escludersi altri **casi in cui il soggetto**

---

[2] L'annullamento totale di un protocollo è il provvedimento che coinvolge tutto il documento. Per normativa (cfr. art. 61 comma 3, DPR 445/2000), è possibile effettuare l'annullamento di un protocollo solo dietro autorizzazione del Responsabile. Si può effettuare l'annullamento di un protocollo laddove siano da modificare campi immodificabili: se, ad esempio, si è acquisito il documento primario non in forma corretta, oppure se prima di protocollare non si è selezionato il box "Dati sensibili" nonostante fosse necessario, oppure se si è protocollato un documento in modalità operativa errata, ecc.

[3] Cfr. Codice dell'Amministrazione Digitale, **D.Lgs. 7 marzo 2005, n.82 Art. 48**. Posta elettronica certificata
1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con le regole tecniche adottate ai sensi dell'articolo 71.
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi alle regole tecniche adottate ai sensi dell'articolo 71.

esterno effettui l'invio del documento **non in formato digitale, ma cartaceo**. In tal caso l'accettazione avverrà anche per le seguenti tipologie:

- **c)** documento cartaceo spedito a mezzo servizio postale istituzionale (Poste Italiane) o altro servizio postale privato o a mezzo corriere o altro mezzo;
- **d)** documento cartaceo notificato a mezzo ufficiale giudiziario;
- **e)** documento ricevuto per il tramite di trasmissione fax (progressivamente in disuso);
- **f)** documento ricevuto e posto agli atti a mezzo incaricato SAPNA munito di delega, previo ritiro, presso uffici postali di giacenza, o presso uffici amministrativi della Sede Legale di Piazza Matteotti,1 Napoli, inclusa la posta giacente presso uffici postali di raccomandate, avvisi, notifiche, anche degli eventuali avvisi giudiziari della quale si è ricevuta informazione;
- **g)** a mezzo consegna a mano;

Identificazione del mittente, firma del mittente

E' di norma **sempre accettato** il documento proveniente da altra PEC, acquisito a mezzo PEC, dotato di firma autografa o digitale e pervenuto **in forma smaterializzata** ovvero **il documento digitale in cui il mittente sia certo.**

Potrà altresì essere accettata quale "posta in INGRESSO" la documentazione **cartacea** indirizzata alla SAPNA SpA **purchè abbia un mittente o che ne sia nota la provenienza**.

- Nel caso particolare e specifico in cui non sia identificato il mittente (mancanza di indicazioni apposte sulla busta contenente il documento, mancanza di riferimenti del firmatario del documento, e similari) ma l'indirizzo di destinazione e/o i destinatari siano correttamente indicati, lo stesso documento sarà acquisito al protocollo in ingresso con nota "mancanza del mittente" e il documento sottoposto all'attenzione del titolare dell'indirizzo di destinazione o del nominativo a cui è indirizzato;
- In presenza di indirizzo in cui si indichi solo "SAPNA SpA" ed in assenza del nominativo o Ufficio o area aziendale di destinazione, l'acquisizione in caso di busta o plico chiuso, sarà effettuata dalla Segreteria Generale mediante apertura della busta ed acquisizione del documento e delle informazioni ivi contenute al fine di poter individuare i destinatari a cui trasmettere il contenuto. Analogamente si procederà in caso di documento privo di busta;
- I documenti ordinari pervenuti a mezzo PEC da soggetti esterni, recanti documenti digitali in allegato ma che siano privi di firma (digitale o autografa) saranno considerati attribuiti ed emessi al mittente della PEC pervenuta. Sono esclusi da tale applicazione i documenti pervenuti da candidati per concorsi di selezione personale o procedure concorsuali di gare d'appalto, per i quali, attesa l'avvenuta acquisizione al protocollo è necessario trasmettere l'intero incartamento al RUP o ad apposito incaricato di quest'ultimo.

Le sopraesposte modalità sono considerate valide ai fini dell'accettazione e attribuzione del protocollo al documento pervenuto, alla sua classificazione, alla collocazione in archivio ed alla sua distribuzione.

Altre modalità specifiche o atipiche di ricezione delle comunicazioni in entrata, **diverse da quelle sopra elencate,** saranno valutate di volta in volta ai fini dell'accettabilità secondo i criteri previsti dal *"Manuale di gestione del Protocollo informatico dei flussi documentali e degli Archivi"* costituente l'**Appendice 1** al presente documento.

Identificazione della tipologia del documento

Le tipologie dei documenti definiti come "posta IN ENTRATA" possono essere, **a titolo indicativo** e non limitativo, riassumibili come segue:

1) Notifiche, Atti Giudiziari (a titolo esemplificativo quali atti di pignoramento, assegnazione delle somme pignorate, verbali di esecuzione di pagamento, esecuzioni mobiliari, etc.) ed equivalenti;
2) Lettere, missive semplici/ordinarie di qualsiasi tipo e loro allegati tecnici e non;
3) Raccomandate, Assicurate, Posta Prioritaria, ed equivalenti;
4) Istanze di vario genere comprese quelle di accesso agli atti;
5) Copie di cortesia di Fatture commerciali, note di credito (trasmesse quale anticipazione informale di fattura elettronica) fatture proforma;
6) Documenti contabili come ad esempio SAL, attestazioni, certificati, DDT, etc.;
7) Estratti conto bancari, comunicazioni bancarie di ogni tipo ed equivalenti;
8) Documenti tecnici e commerciali, provenienti da operatori economici;
9) Assicurazioni, polizze, fidejussioni;
10) Plichi sigillati di partecipazione a Gara/Concorso o per integrazioni a Gare/Concorsi;
11) Buste sigillate o non, indirizzate ad uno qualsiasi degli Uffici della struttura organizzativa della SAPNA SpA;
12) Pacchi, Plichi da Corrieri, etc.;
13) Stampe (periodici, libri, pubblicazioni, etc.);
14) Pubblicità, documenti pubblicitari, inclusi depliants descrittivi inviati da fornitori.

3.2 Posta in INGRESSO - Modalità di protocollazione e distribuzione

I documenti che siano accettati per il tramite di una qualsiasi delle modalità elencate al par. 3.1 lettere a), b), c), d), e), f) e g) dovranno essere protocollate, quali documenti in INGRESSO da parte della Segreteria Generale, utilizzando il predisposto software "FOLIUM" con i seguenti criteri:

A) Per i documenti di cui all'elenco summenzionato, pervenuti con uno qualsiasi dei mezzi previsti dalle modalità di accettazione, si dovrà procedere a protocollare, <u>in ogni caso:</u>

1) Notifiche, Atti Giudiziari (a titolo esemplificativo quali atti di pignoramento, assegnazione delle somme pignorate, verbali di esecuzione di pagamento, esecuzioni mobiliari, etc.) ed equivalenti;
2) Documentazione da lettere, missive semplici/ordinarie di qualsiasi tipo;
3) Raccomandate, Assicurate, Posta Prioritaria, ed equivalenti;
4) Istanze di vario genere compresa quelle di accesso agli atti;
5) Copie di cortesia di Fatture commerciali, note di credito (trasmesse quale anticipazione informale di fattura elettronica) note e/o fatture proforma;
6) Documenti contabili come ad esempio SAL, attestazioni, certificati, DDT, etc.;
7) Estratti conto bancari, comunicazioni bancarie di ogni tipo ed equivalenti;
8) Documenti tecnici e commerciali, provenienti da operatori economici;
9) Assicurazioni, polizze, fidejussioni;
10) Plichi sigillati di partecipazione a Gara/Concorso o per integrazioni a Gare/Concorsi;
11) Eventuali buste sigillate o non, contenenti documenti, indirizzate ad uno qualsiasi degli Uffici della struttura organizzativa della SAPNA SpA;
12) Pacchi, Plichi da Corrieri, etc.;

Per quanto attiene invece i punti:

13) Stampe (periodici, libri, pubblicazioni, etc.);
14) Pubblicità, documenti pubblicitari, inclusi depliants descrittivi inviati da fornitori.

questa NON sarà soggetta a protocollazione.

B) In particolare, per la posta in ingresso di cui all'elenco summenzionato, che sia **pervenuta in busta chiusa**[4] a mezzo servizio postale o corriere, si procederà come segue:

Posta di cui al precedente punto 7) Estratti conto bancari in busta chiusa, comunicazioni bancarie di ogni tipo ed equivalenti;

Sarà effettuata la copia della busta chiusa fronte retro su un unico foglio avendo cura di ben evidenziare gli estremi del destinatario, incluso eventualmente il "serial number" o codice identificativo, visibile nella busta a finestra, affinchè possano essere chiaramente identificabili e leggibili. La copia ottenuta sarà scansionata e sulla scansione ottenuta si procede ad acquisire il numero di protocollo. Sarà possibile, per dare pronta evidenza della posizione in archivio del documento, apporre l'etichetta autoadesiva recante gli estremi del protocollo sulla busta chiusa. Il documento cartaceo, costituito in questo caso dalla busta chiusa, dovrà essere materialmente trasmesso all' Ufficio Amministrazione e Finanza che prenderà in carico il documento (cartaceo) e la scansione (tramite protocollo);

Posta di cui al precedente punto 10) Plichi sigillati di partecipazione a Gara/concorsi o per integrazioni a Gare/concorsi;

La SAPNA adotta la procedura, ove applicabile, delle gare telematiche per le quali la tracciabilità documentale viene assicurata dalla piattaforma di sistema utilizzata. Tuttavia, qualora dovessero adottarsi le procedure che prevedano la ricezione di plichi sigillati contenenti documentazioni e/o offerte economiche, per i Plichi Sigillati da Gara o anche per tutte le buste chiuse che recassero la dicitura *"Non Aprire"* oppure *"gara N….."* *"gara CIG….."* oppure *"Offerta …"* *"Concorso…oppure Pubblica selezione"* e/o scritte similari che paventino contenuti sensibili di tipo commerciale o informazioni personali è necessario apporre il protocollo solo all'esterno, sulla busta chiusa e sigillata, avendo cura di non alterare né i sigilli né la busta stessa che devono conservare la loro integrità, e porre agli atti la sola fotocopia della busta o del plico così ricevuti, inviando debita comunicazione al RUP competente (che può essere o della gara d'appalto o del concorso/selezione pubblica) ed all' Ufficio Gare e Contratti (in caso di gara d'appalto) o all'Ufficio Amministrazione del Personale (in caso di candidature a concorsi) utilizzando il servizio di posta elettronica ordinaria aziendale.

Le buste o i plichi, così sigillati e protocollati dovranno essere conservati in una delle due casseforti disponibili in azienda notificando al RUP e all' Ufficio Gare e Contratti o nel caso all'Ufficio amministrazione del Personale, sempre a mezzo e-mail, l'avvenuto deposito, indicando il numero della gara/estremi del concorso, i plichi custoditi e in quale cassaforte sono ubicati. I plichi saranno custoditi fino al giorno previsto per l'apertura. Le casseforti disponibili sono ubicate nel Corridoio Uffici Segreteria;

Posta di cui al precedente punto 11) Buste chiuse e sigillate o semplicemente chiuse, indirizzate all' Ufficio Amministrazione del Personale, incluse buste chiuse provenienti da

[4] E' mutuata l'applicazione del Codice Art. 49. Segretezza della corrispondenza trasmessa per via telematica
1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

laboratori di analisi cliniche, INPS, INAIL, Agenzia delle Entrate, Equitalia, che riguardino espressamente e personalmente i dipendenti in indirizzo presso la SAPNA SpA;

Analogamente come indicato al precedente punto per i plichi e/o buste chiuse o sigillate destinate all' Ufficio Amministrazione del Personale è necessario apporre il protocollo solo all'esterno, sulla busta chiusa e sigillata, avendo cura di non alterare né i sigilli né la busta stessa che devono conservare la loro integrità e porre agli atti la sola fotocopia della busta o del plico così ricevuti, notificando l'avvenuta consegna della busta o del plico all' Ufficio Amministrazione del Personale. Le buste o i plichi, così protocollati dovranno essere consegnati materialmente all' Ufficio Amministrazione del Personale che ne ha la competenza e la custodia, subito dopo l'arrivo e l'attribuzione del protocollo. L'Ufficio Amministrazione del Personale prenderà in carico il documento (cartaceo) e la scansione (protocollata);

L' Ufficio Amministrazione del Personale, oltre alla possibilità di depositare le predette documentazioni presso il proprio Archivio tenuto in apposito locale segregato, potrà disporre sempre di una delle casseforti disponibili in azienda.

Posta di cui al precedente punto 11) Buste chiuse e sigillate o semplicemente chiuse, indirizzate ad uffici Aziendali e/o al Responsabile dell'Uffcio e/o espressamente a dipendenti presso uno degli uffici aziendali presso la SAPNA SpA;

Analogamente come indicato al precedente punto per i plichi e/o buste chiuse o sigillate destinate generalmente ad uno dei vari uffici aziendali è necessario apporre il protocollo solo all'esterno, sulla busta chiusa e sigillata, avendo cura di non alterare né i sigilli né la busta stessa che devono conservare la loro integrità e porre agli atti la sola fotocopia della busta o del plico così ricevuti, notificando l'avvenuta consegna della busta o del plico al Responsabile dell'ufficio di destinazione che ne ha la competenza e la custodia, subito dopo l'arrivo e l'attribuzione del protocollo. L'Ufficio di destinazione prenderà in carico il documento (cartaceo) e la scansione (protocollata) e provvederà, se necessario, a protocollare con l'ausilio della Segreteria Generale il documento in ingresso;

Per quanto attiene le istanze di accesso agli atti di cui al punto 4);

le stesse, preventivamente acquisite e protocollate, dovranno essere trasmesse al Responsabile della Prevenzione della Corruzione e della Trasparenza che disporrà le azioni del caso secondo la regolamentazione aziendale vigente.

C) Per la posta in ingresso di cui all'elenco summenzionato, **pervenuta a mezzo PEC** all'indirizzo istituzionale sapna@pec.it **incluse le candidature per selezioni pubbliche o concorsi** o **provenienti da istituzioni di Polizia Giudiziaria su disposto dell'Autorià Giudiziaria,** si procederà come segue:

- accettazione del documento ricevuto a mezzo PEC con data ed ora,
- acquisizione degli eventuali allegati, in forma integra senza accedere o aprire il file;
- protocollazione in ingresso con trascrizione dell'oggetto del documento;
- classificazione del documento utilizzando laddove necessario criteri di riservatezza fissati in base ai dati contenuti nel documento (vedi manuale Folium Appendice 1),
- nel caso di selezioni pubbliche la candidatura viene trasmessa al RUP, in altri casi la distribuzione è effettuata a mezzo Folium ai soggetti aziendali in indirizzo direttamente o per conoscenza se inseriti,
- distribuzione a mezzo Folium anche a quei soggetti aziendali non in indirizzo ma che devono essere messi al corrente dei contenuti del documento per opportunità di diffusione dell'informazione, con esclusione dei casi di condidature per selezioni e/o concorsi pubblici;

- nel caso di PEC provenienti dall'Autorità Giudiziaria o da istituzioni di Polizia Giudiziaria il cui contenuto comporti l'acquisizione di informazioni, anche nei confronti di dipendenti, in ambito penale o comunque soggette a riservatezza del dato, la PEC sarà trattata e classificata con i criteri di riservatezza previsti per le candidature, ma trasmettendo il documento in forma riservata all'attenzione dell'Amministratore Unico, il quale provvederà alle eventuali azioni dovute ed ai provvedimenti previsti in tali casi.

Tutti i soggetti aziendali destinatari riceveranno all'indirizzo di posta elettronica PEA personale una notifica automatica che reca il numero di protocollo ricevuto ed una sintesi dell'oggetto del documento.

I soggetti destinatari sono tenuti ad acquisire il documento così ricevuto tempestivamente e provvedere alle opportune consequenziali azioni se di competenza o, se ricevuto per conoscenza, a porre in essere il proprio contributo, anche se non principalmente coinvolti, affinchè non si determini un impedimento per il regolare svolgimento dell'azione amministrativa.

Al successivo par. 4.0 sono definiti i soggetti destinatari della posta in ingresso protocollata in ragione della tipologia di documento acquisito in ingresso, con la determinazione della modalità "competenza" e "conoscenza".

*Per quanto riguarda la distribuzione delle **stampe e le pubblicità**, pervenute con qualsiasi mezzo, queste **non saranno protocollate** e messe nelle disponibilità agli eventuali destinatari in azienda qualora fossero indicati nell'indirizzo. In assenza, o se non di interesse, elasso il periodo di giacenza di dieci giorni, il cartaceo afferente stampe e pubblicità sarà avviato allo smaltimento/recupero secondo norma.*

3.3 Posta in USCITA-Esterna

Per posta in uscita si intendono tutti i documenti **che vengono emessi dalla SAPNA SpA**, intesa **quale soggetto omogeneo costituito da vari Uffici ed unità operative interne,** che siano **preventivamente firmati** e ancorchè **protocollati,** trasmessi a soggetti esterni alla stessa. **Il formato del documento deve essere di tipo digitale.**
Tali documenti possono essere, a titolo indicativo e non limitativo, riassumibili nelle seguenti tipologie:

1) Documenti approntati da Segreteria Generale/Legale per l'Amministratore Unico a firma di quest'ultimo, inclusi contratti di servizio con gli Enti Locali;
2) Qualsiasi missiva, lettera, nota e comunicazioni ordinarie necessarie al *funzionamento **amministrativo*** della SAPNA SpA a firma dell'Amministratore Unico;
3) Qualsiasi missiva, lettera, nota e comunicazioni ordinarie necessarie al *funzionamento **tecnico*** della SAPNA SpA a firma dell'Amministratore Unico;
4) Documenti **approntati dalla Direzione Tecnica** a firma del Direttore Tecnico;
5) Documenti **approntati dall'area Amministrazione del Personale** anche a firma del Responsabile dell'Ufficio;
6) Documenti approntati **dall'Ufficio Amministrazione e Finanza** anche a firma del Responsabile dell'Ufficio;
7) Documenti approntati **dall'area Affari Generali**;
8) Documenti approntati dall'**Ufficio Gare e Contratti** anche a firma del Responsabile dell'Ufficio;
9) Documenti approntati dal **RPCT** a firma di quest'ultimo;

10) Documenti approntati dal **Responsabile delle Relazioni Sindacali** anche a firma di quest'ultimo;

Esulano dalla forma digitale, qualora non sia possibile utilizzare tale formato, le seguenti tipologie, nel caso in cui siano necessariamente richieste di tipo cartaceo:

11) Note Raccomandate, Posta Prioritaria, ed equivalenti;

per le quali, in assenza di possibilità di digitalizzazione, è richiesta la firma autografa;

Per tutti i documenti aziendali che siano approntati da qualsiasi redattore, di qualsiasi Ufficio o Area Aziendale, inclusi gli impianti TMB, Siti e Discariche **è necessario apporre, in calce a sinistra al documento stesso, una sigla che identifichi il redattore materiale del documento, composta di 4 lettere,** formata dalle prime due lettere del cognome in maiuscolo succedute dalle prime due lettere in minuscolo del nome[5].
La redazione del documento firmato solo dal Responsabile dell'Ufficio, privo della sigla del redattore materiale, è attribuita al Responsabile dell'Ufficio.

La necessità di identificare univocamente le tipologie di documenti in uscita e la firma degli stessi discende dall'obbligo di conformarsi alla normativa corrente (rif. Codice dell'Amministrazione Digitale-Decreto Legislativo 7 marzo 2005, n. 82 e ss. mm. e ii.) che prevede l'utilizzo della PEC per qualsiasi scambio di informazioni e documenti **anche al fine di identificare correttamente ed univocamente il mittente ed il firmatario del documento, dando valore legale a quest'ultimo.**

3.4 Posta in USCITA a Firma dell'Amministratore Unico

La modalità di trasmissione per la posta in uscita istituzionalmente prevista verso soggetti esterni, normalmente utilizzata dalla SAPNA SpA è la PEC, indirizzo sapna@pec.it, sincronizzata con il sistema protocollare Folium, convenzionalmente utilizzata dall'Organo Amministrativo per le comunicazioni formali verso l'esterno.
Tutti i documenti **firmati dall'Amministratore Unico**, anche approntati da altri soggetti aziendali secondo le modalità previste dalla presente procedura, sono trasmessi **ai destinatari a mezzo PEC a carico della Segreteria Generale[6]** che provvederà a:

nel caso di documento approntato dall'Amministratore Unico

- AU procederà a firmare digitalmente il documento approvato, Segreteria Generale a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato da altri soggetti aziendali

- ad acquisire il documento in formato *pdf trasmesso da altri soggetti aziendali
- a condividere il contenuto con l'Amministratore Unico
- AU procederà a firmare digitalmente il documento, Segreteria Generale a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato da altri soggetti aziendali a doppia firma di cui una dell'Amministratore Unico

- ad acquisire il documento in formato *pdf proveniente da altri soggetti aziendali già provvisto di firma (digitale o autografa) di altro soggetto
- a condividere il contenuto con l'Amministratore Unico
- AU procederà a firmare digitalmente o autograficamente il documento, Segreteria Generale a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

[5] Ad esempio: Mario Rossi corrisponderà RO/ma. In caso di cognomi e nomi coincidenti con più di una persona si utilizzeranno, in successione la terza lettera o la quarta , ad es. RO/mar, (Rossi Mario) RO/mart, (Rossi Martino), etc.
[6] Intesa quale area omogenea costituita dalla Segreteria Generale e dagli addetti/collaboratori ad essa afferenti

Qualora non sia disponibile la firma digitale**, il documento dovrà essere firmato in ogni caso** con firma autografa dell'Amministratore Unico.

3.5 Posta in USCITA a Firma del Direttore Tecnico

La modalità di trasmissione per la posta in uscita istituzionale da parte del Direttore Tecnico, limitatamente alle procure e deleghe conferite, verso soggetti esterni, normalmente utilizzata dalla SAPNA SpA è la PEC, indirizzo sapna@pec.it , sincronizzata con il sistema protocollare Folium. Tutti i documenti **firmati dal solo Direttore Tecnico**, nell'ambito dell'esercizio delle sue funzioni, anche approntati da altri soggetti aziendali secondo le modalità previste dalla presente procedura, sono trasmessi ai destinatari **a mezzo PEC a carico della Segreteria Tecnica**[7] che provvederà a:

nel caso di documento approntato dal Direttore Tecnico

- DT procederà a firmare digitalmente il documento approvato, Segreteria Tecnica a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato da altri soggetti aziendali per conto del Direttore Tecnico

- ad acquisire il documento in formato *pdf proveniente da altri soggetti aziendali
- a condividere il contenuto con il Direttore Tecnico
- DT procederà a firmare digitalmente il documento, Segreteria Tecnica a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato anche da altri soggetti aziendali (con esclusione dell'AU) a doppia firma di cui una del Direttore Tecnico

- ad acquisire il documento in formato *pdf proveniente da altro soggetto aziendale già provvisto di firma (digitale o autografa)
- a condividere il contenuto con il Direttore Tecnico
- DT procederà a firmare digitalmente il documento, Segreteria Tecnica a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

Qualora non sia disponibile la firma digitale**, il documento dovrà essere firmato in ogni caso** con firma autografa del Direttore Tecnico.

3.6 Posta in USCITA a Firma di RUP non coincidente col Direttore Tecnico

La modalità di trasmissione per la posta in uscita istituzionale da parte del RUP Responsabile Unico del Procedimento, quale soggetto interno alla SAPNA SpA che non sia il Direttore Tecnico, limitatamente alle responsabilità ed azioni relative alla funzione espletata e verso soggetti esterni, utilizzata dalla SAPNA SpA è la PEC, indirizzo sapna@pec.it , sincronizzata con il sistema protocollare Folium. Tutti i documenti **firmati dal RUP**, nell'ambito dell'esercizio delle sue funzioni, anche approntati da altri soggetti aziendali secondo le modalità previste dalla presente procedura, sono trasmessi ai destinatari **a mezzo PEC a carico della Segreteria Tecnica**[8] **(o Segreteria Generale nel caso in cui il RUP non sia risorsa dell'Area Tecnica)** che provvederà a:

nel caso di documento approntato dal RUP

- Il RUP procederà a firmare digitalmente il documento approvato, Segreteria Tecnica (o Segreteria Generale nel caso di RUP non di Area Tecnica) a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato da altri soggetti aziendali per conto del RUP

- ad acquisire il documento in formato *pdf proveniente da altri soggetti aziendali
- a condividere il contenuto con il RUP

[7] Intesa quale area omogenea costituita dalla Segreteria Tecnica e dagli addetti/collaboratori ad essa afferenti

[8] Intesa quale area omogenea costituita dalla Segreteria Tecnica e dagli addetti/collaboratori ad essa afferenti

- il RUP procederà a firmare digitalmente il documento, Segreteria Tecnica (o Segreteria Generale nel caso di RUP non di Area Tecnica) a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

nel caso di documento approntato dal RUP o da altri soggetti aziendali (con esclusione dell'AU) a doppia firma di cui una del Direttore Tecnico

- ad acquisire il documento in formato *pdf proveniente da altri soggetti aziendali già provvisto di firma (digitale o autografa)
- a condividere il contenuto con il RUP e con il Direttore Tecnico
- il RUP procederà a firmare digitalmente il documento, Segreteria Tecnica a protocollare ed inviare il documento a mezzo PEC ai destinatari indicati in indirizzo

Qualora non sia disponibile la firma digitale, **il documento dovrà essere firmato in ogni caso** con firma autografa del RUP o, in caso di firma congiunta, anche del Direttore Tecnico.

3.7 Posta in USCITA a Firma di Responsabili d'ufficio muniti di Procura o Delega

La modalità di trasmissione per la posta in uscita istituzionale approntata da soggetti interni alla società - che per funzioni aziendali o in forza di specifiche procure e/o deleghe che non rientrano nella casistica precedente, limitatamente alle responsabilità ed azioni relative alla funzione espletata verso soggetti esterni - utilizzata dalla SAPNA SpA è la PEC, indirizzo sapna@pec.it, sincronizzata con il sistema protocollare Folium.

Nello specifico tali soggetti sono così identificati:

- **Responsabile dell'Ufficio Amministrazione e Finanza**
- **Responsabile dell'Ufficio Amministrazione del Personale**

Tutti i documenti **firmati dai predetti Responsabili** nell'ambito dell'esercizio delle rispettive funzioni, anche approntati da diversi operatori afferenti alle singole aree di competenza secondo le modalità previste dalla presente procedura, **saranno preventivamente firmati (digitalmente o con firma autografa)** ed inviati (a mezzo mail allegando il documento in formato *.pdf completo di eventuali allegati o, in casi eccezionali, in forma cartacea se con firma autografa) alla **Segreteria Generale**[9] che provvederà, per il tramite del protocollo, all'acquisizione del documento, alla protocollazione ed alla trasmissione dello stesso **a mezzo PEC.**
L'emittente, nella mail di trasmissione dovrà indicare i destinatari e gli eventuali altri soggetti posti per conoscenza.
Segreteria Generale e, per essa il protocollo, darà avviso all'emittente dell'avvenuta azione.

3.8 Posta in USCITA a Firma del Responsabile Ufficio Gare e Contratti

La posta in uscita dall'Ufficio Gare e Contratti di SAPNA SpA **-** occorrente limitatamente alle necessarie comunicazioni tenute verso gli operatori economici, afferenti - a titolo indicativo - a procedure di gara, documentazioni, dichiarazioni, atti negoziali, contrattuali e quanto altro connesso ai procedimenti per l'indizione, verifica ed affidamento di appalti di beni, lavori e servizi **–** a firma del Responsabile dell'ufficio è effettuata utilizzando la PEC gare.sapna@pec.it essenzialmente adottata per l'uso con la piattaforma web dell'albo fornitori.
Tale indirizzo PEC, **non sincronizzato con il sistema protocollare aziendale**, è utilizzato in funzione e coerenza con l'uso del portale della Piattaforma di gestione dell'Albo Fornitori e delle Gare Telematiche posto sul sito web istituzionale di SAPNA SpA, per

[9] Intesa quale area omogenea costituita dalla Segreteria Generale e dagli addetti/collaboratori ad essa afferenti

favorire l'operatività dell'ufficio Gare e Contratti, al fine di una maggiore rapidità ed efficienza dell'azione amministrativa.

3.9 Posta in USCITA a Firma del RPCT

La modalità di trasmissione per la posta in uscita istituzionale approntata dal **Responsabile per la Prevenzione della Corruzione e della Trasparenza,** limitatamente alle responsabilità ed azioni relative alla funzione istituzionalmente espletata, sia verso soggetti interni che esterni, è la PEC, indirizzo anticorruzionesapna@pec.it sincronizzata con il sistema protocollare Folium per la sola posta in uscita.
Tutti i documenti **firmati dal Responsabile** nell'ambito dell'esercizio delle proprie funzioni, anche approntati da operatori afferenti alla propria area di competenza, **saranno preventivamente firmati (digitalmente o con firma autografa) dal RPCT e protocollati** nonché trasmessi direttamente [10] **a mezzo PEC.**

3.10 Modalità di gestione della Posta in USCITA

Il documento in uscita dall'Azienda verso qualsiasi soggetto esterno, che sia privo di protocollo attribuito dal sistema di gestione "Folium" e non trasmesso a mezzo PEC non viene riconosciuto come documento proveniente dall'Azienda ed emesso da quest'ultima, in quanto non inserito nell'archivio dei documenti protocollati e posti agli atti di questa Società.

Tutte le documentazioni/comunicazioni "in uscita" afferenti l'attività dell'azienda dovranno essere approntate dalle varie aree aziendali interessate, le quali provvederanno anche a controllare che le stesse siano complete dei requisiti minimi:

- redatte sulla carta intestata adottata ufficialmente
- munite di sigla e/o riferimenti del compilatore
- chiara evidenza dei destinatari e/o soggetti per conoscenza (se possibile anche degli indirizzi mail e/o PEC)
- chiaro riporto dell'oggetto
- chiaro riporto della firma

Una volta approntato il documento in uscita, il soggetto responsabile della compilazione del documento ne renderà disponibile il file presso il sistema di protocollazione, che provvederà a predisporlo pronto per l'invio nei casi in cui ne sia prevista la trasmissione a carico della Segreteria Generale oppure della Segreteria Tecnica (vedasi le casistiche del precedente par. 3.3.).

3.11 Posta in USCITA-Interna

La posta interna, ovvero la trasmissione di documenti formali inclusi i relativi allegati tra le varie aree aziendali, seguirà lo stesso iter adottato per la posta in uscita **con la sola variazione che i mittenti e i destinatari possono essere solo dipendenti SAPNA.**
Nella posta interna è annoverata la **"Comunicazione Interna"** alla quale è attribuito un protocollo e lavorata come una comunicazione ordinaria.
I documenti in uscita come posta interna devono essere protocollati (e inviati), hanno valore formale e validità endoprocedimentale e possono essere approntati dai Responsabili delle varie Aree Aziendali nonché dai loro collaboratori, o dal RUP o dai

[10] A cura dell'Ufficio Affari Generali e/o dagli operatori ad esso afferente incaricati di tale compito

collaboratori del RUP o da altre funzioni, per ottemperare alle necessità interne previste dagli obblighi istituzionali e/o da procedimenti esterni (ad esempio: comunicazioni formali, trasmissione di documenti formali, convocazioni in riunioni formali, richieste documentali, richieste di approvazione, proposte di determina, trasmissione di SAL, DDT, attestazioni, certificazioni richieste di autorizzazione, etc.) L'approntamento, la protocollazione, la firma ed il relativo invio per il tramite di Folium spetta al singolo ufficio.

Per quanto attiene gli abituali scambi di informazioni, comunicazioni o scambio informale di documenti di vario tipo tra tutti i dipendenti, è preferibile che venga usato il normale sistema di posta elettronica di cui ogni dipendente abilitato è dotato, evitando il passaggio/scambio di documenti cartacei, raccomandando fortemente l'approntamento e l'utilizzo di documenti in formato digitale.

Le trasmissioni di documentazioni di diffusione aziendale (regolamenti, comunicati ai dipendenti, etc.) devono seguire preferibilmente il percorso telematico, assicurandosi che la posta elettronica sia effettivamente recapitata al destinatario a mezzo della doppia ricevuta (recapitato-letto).

- **Deposito del documento cartaceo presso il mittente/destinatario**

Nei casi eccezionali in cui si avrà necessità della prova documentale dell'avvenuta trasmissione e deposito del documento cartaceo protocollato in ingresso/uscita, quindi già acquisito a mezzo Folium, trasmesso e depositato presso il mittente/destinatario, il quale abbia fatto richiesta di custodire necessariamente il documento cartaceo originario, è necessario ottenere firma autografa del ricevente completa di data apposta sulla copia del documento dalla quale si evincano i riferimenti di protocollo (in genere copia della prima facciata del documento).
In questo caso in archivio, in uno al *pdf del documento trasmesso, sarà allegata anche la scansione della parte del documento su cui è stata apposta la firma del ricevente a comprova dell'avvenuta ricezione del cartaceo originario ed il protocollo recherà la nota "cartaceo in deposito presso il mittente/destinatario".

- **Riservatezza del documento interno**

E' vietato, per motivi legati all'obbligo di riservatezza sia del dato personale che amministrativo e/o commerciale, anticipare, comunicare o trasmettere a terzi il contenuto delle comunicazioni interne e tutto quanto sia riconducibile a documentazioni endoprocedimentali (come ad esempio a titolo indicativo e non limitativo, determinazioni, proposte di determine, informazioni relative a richieste di acquisto o di offerta, richieste di approvazioni firmate, verbali di gara in seduta riservata, verbali di riunione aziendali, pagamenti, etc.) prima che tali informazioni siano rese nelle disponibilità dei soggetti autorizzati al trattamento dell'informazione o prima che i detti contenuti siano resi pubblici o disponibili ai legittimi destinatari, in applicazione delle norme sulla riservatezza del dato Dlgs 467/2001, disposizioni GPDP, nonché sulla Trasparenza previste dal Dlgs 14 marzo 2013, n. 33 "Decreto Trasparenza" e ss. mm. e ii. e dal Piano Triennale per la Prevenzione Corruzione e Trasparenza aziendale.

3.12 Posta Elettronica Aziendale (PEA)

La casella di posta elettronica individuale, **in breve definita PEA**, è un mezzo di comunicazione in dotazione a tutti i dipendenti SAPNA SpA, **che l'azienda pone nelle disponibilità personali di quest'ultimo al fine di assolvere agli obblighi previsti dalle proprie mansioni e compiti nell'ambito dello svolgimento delle attività lavorative nonché anche al fine di ricevere comunicazioni da parte dell'Azienda.**
Tale mezzo di comunicazione e corrispondenza dovrà essere sempre preferibilmente utilizzato per tutte le comunicazioni e scambio dati interno.

L'utilizzo della posta elettronica quale mezzo di comunicazione con soggetti esterni è disciplinato dalle Leggi in materia di protezione e salvaguardia dei dati di proprietà dell'Azienda.

- **Non può essere utilizzata la posta aziendale per scopi personali o comunque per scopi che non siano strettamente afferenti all'esercizio delle proprie funzioni in Azienda.**
- **Non è possibile inviare messaggi da caselle di posta elettronica ordinaria quando il contenuto di questi impegni la SAPNA SpA verso terzi.**

La SAPNA SpA non effettua controlli sistematici sull´utilizzo degli strumenti elettronici posti nelle disponibilità dei dipendenti,[11] riservandosi tuttavia la facoltà - qualora dovessero verificarsi casi specifici, indispensabili e indifferibili - di intervenire per controlli sulla PEA per esclusive necessità di operatività aziendale e/o di sicurezza informatica del sistema di rete dati, procedendo ad informare con congruo anticipo l'interessato, e comunque in tutti i casi operando secondo la normativa vigente del Codice di protezione dei dati personali e, qualora dovesse delinearsi l'eventualità di accedere per il tramite della PEA del dipendente a dati non aziendali o personali, ad eseguire la predetta azione alla presenza ove possibile dell'interessato e di almeno un testimone, limitandosi a segnalare, nei casi opportuni, l'esito all'Organismo di Vigilanza della SAPNA SpA.

Nel caso di cessazione del rapporto di lavoro del titolare di account di PEA, in osservanza agli indirizzi dell'Autorità GPDP e in conformità ai principi in materia di protezione dei dati personali, **gli account di PEA riconducibili a persone identificate o identificabili saranno rimossi** previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi, contemperando le aspettative di riservatezza sulla corrispondenza da parte dei dipendenti nonché degli stessi terzi.

Fanno eccezione i casi che rientrino nelle **indagini dell'Autorità Giudiziaria** nei confronti del soggetto aziendale titolare di PEA, a seguito delle quali l'Azienda provvederà, nell'eventualità, alle azioni dovute, in osservanza alle disposizioni dell'Autorità.

3.13 Posta Elettronica Certificata (PEC)

L' Azienda è dotata di una univoca casella di posta certificata istituzionale denominata sapna@pec.it.
L'uso della PEC è prerogativa della Segreteria Generale e unità operativa Protocollo per quanto attiene l'acquisizione di documenti in INGRESSO (posta in entrata).
A quest'ultima è devoluto il compito di lettura e gestione della posta elettronica certificata aziendale in ingresso e lo smistamento delle comunicazioni pervenute a mezzo PEC dall'esterno alle varie Aree Aziendali. Per il tramite di PEC è effettuata anche la trasmissione della corrispondenza in uscita approntata dalla Segreteria Generale o dagli altri Uffici della SAPNA SpA secondo le previsioni riportate nel presente documento.
Sono altresì in dotazione alla SAPNA SpA le seguenti PEC, costituite in ordine alla funzionalità delle varie attività aziendali:

sapnaruoli@pec.it
utilizzata esclusivamente per la gestione della riscossione coattiva della TARSU, nei contenziosi TARSU e nelle attività residuali in ordine al contratto di concessione per il

[11] Cfr. Disciplina di settore in materia di controlli a distanza (cfr. artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, legge 20.5.1970, n. 300). Tale disciplina infatti, pure a seguito delle modifiche disposte con l´art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l´effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell´attività del lavoratore (v. Linee guida per posta elettronica e internet citate in premessa, spec. par. 4, 5.2. lett. b) e 6; Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec(2015)5, spec. princ. 14).

servizio di gestione ordinaria e straordinaria, riscossione volontaria e coattiva, della tassa sui rifiuti solidi urbani (T.A.R.S.U.) e della tariffa d'igiene ambientale (T.I.A.) nel territorio della Provincia di Napoli dagli addetti coordinati dall'Ufficio Affari Generali;

gare.sapna@pec.it
utilizzata esclusivamente per gli scopi previsti dal precedente paragrafo 3.3 dall' Ufficio Gare e Contratti per quanto attiene le modalità di posta in uscita;

anticorruzionesapna@pec.it
utilizzata dal Responsabile per la Prevenzione della Corruzione e della Trasparenza per le comunicazioni istituzionali sia verso soggetti esterni che verso soggetti interni alla SAPNA SpA;

odvsapna@pec.it
utilizzata dall' Organismo di Vigilanza per le comunicazioni istituzionali sia verso soggetti esterni che verso soggetti interni alla SAPNA SpA;

sindacisapna@pec.it
utilizzata dal Collegio dei Sindaci per le comunicazioni istituzionali sia verso soggetti esterni che verso soggetti interni alla SAPNA SpA;

3.14 Firma Digitale dell'Amministratore Unico e di altri soggetti aziendali

L'Amministratore Unico, il Direttore Tecnico, i Quadri, i Responsabili degli Uffici ed altri soggetti aziendali che per funzioni specifiche necessitano di apporre la propria firma su documenti aziendali formalmente utilizzati, sono dotati di firma digitale.
La firma, autografa o digitale che sia, è la massima espressione formale della volontà personale, che per sua stessa natura non è delegabile.
Pertanto la firma digitale di cui all'art. 24 del D. Lgs. n. 82/2005 e ss.mm.ii. è nelle disponibilità del titolare e può essere apposta solo da quest'ultimo[12].
Il deposito delle firme digitali siffatte è in Azienda presso i singoli titolari.
L'Amministratore Unico, preventivamente informato circa l'utilizzo della Firma Digitale, provvederà a firmare i documenti preferibilmente con firma digitale oltre alla possibilità di avvalersi di firma autografa, che sarà utilizzata nei casi di documenti di trascrizione su foglio vidimato da notaio delle determinazioni dell'Amministratore e delle trascrizioni dei Verbali di Assemblea del Socio Unico.
L'utilizzo della Firma Digitale da parte di tutti i soggetti che ne detengono l'uso, dovrà effettuarsi esclusivamente per lo scopo dichiarato e limitatamente all'attività necessaria.

4. DISTRIBUZIONE INTERNA E TRASMISSIONE DELLA DOCUMENTAZIONE

4.1 Documento digitale

La distribuzione della **documentazione in ENTRATA** (posta in arrivo), acquisita a mezzo della **PEC istituzionale** sapna@pec.it debitamente protocollata, dovrà essere eseguita da Segreteria Generale – Protocollo, con il seguente criterio:

[12] In tal senso, l'art. 32 comma 1 del CAD Codice dell'Amministrazione Digitale è chiaro:
Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma. In caso di danni causati ad altri, il titolare della firma deve dimostrare di aver adottato tali misure; in caso contrario, sarà tenuto a risarcire i danni.

1) **Diffide, Notifiche, Atti Giudiziari, Pignoramenti, Note provenienti da Avvocati, da Studi Legali o Aree legali di altre amministrazioni pubbliche e/o private nonché atti equivalenti:**

Distribuzione a: all' Amministratore in ogni caso ed **ai destinatari in indirizzo** e comunque ai seguenti uffici, e per conoscenza ad eventuali uffici cointeressati:

- Amministrazione e Finanza
- Amministrazione del Personale
- Affari Generali-Legale

2) **Lettere, missive, note e documenti di qualsiasi tipo provenienti da operatori economici, professionisti, studi associati, soggetti giuridici in genere, altre società partecipate, pubbliche amministrazioni, nonché documentazione equivalente, indirizzata alla SAPNA SpA:**

Distribuzione a: all' Amministratore in ogni caso ed **ai destinatari in indirizzo** delle Area/ee aziendale/i di competenza secondo il seguente schema di distribuzione, indicativo e non limitativo:

- Amministrazione e Finanza
- Amministrazione del Personale
- Direttore Tecnico e per esso Segreteria Tecnica
- Gare e Contratti
- Affari Generali-Legale
- Affari Generali-TARSU
- Anticorruzione e Trasparenza

che tenga conto dei contenuti di ogni singolo documento e/o del soggetto posto in indirizzo o dell'area aziendale alla quale è indirizzato il documento.
Per quanto attiene le funzioni di:

- Relazioni sindacali: distribuire e trasmettere solo le note provenienti da OOSS o contenenti in indirizzo il Responsabile Relazioni Sindacali;
- RUP: distribuire e trasmettere solo le note indirizzate al RUP o contenenti in indirizzo per conoscenza il Responsabile del Procedimento;

3) **Copia di cortesia fatture elettroniche, di note di credito, note proforma provenienti da operatori economici, professionisti, tecnici, amministrativi, avvocati ed equivalenti:**

Distribuzione a: all' Amministratore in ogni caso ed **ai destinatari in indirizzo** delle Area/ee aziendale/i di competenza secondo il seguente schema di distribuzione, indicativo e non limitativo

- Amministrazione e Finanza
- Direttore Tecnico e per esso Segreteria Tecnica
- Affari Generali-Legale
- Amministrazione del Personale

4) **Documenti tecnici, Capitolati, Disciplinari, SAL, SAS, documenti contabili e non, note, missive, documenti provenienti da operatori economici**

Distribuzione a: ai destinatari in indirizzo delle Area/ee aziendale/i di competenza secondo il seguente schema di distribuzione, indicativo e non limitativo e per conoscenza ad uffici eventualmente cointeressati:

- Direttore Tecnico e per esso Segreteria Tecnica
- RUP

5) Assicurazioni, polizze, fidejussioni provenienti da fornitori
Distribuzione a: ai destinatari in indirizzo delle Area/ee aziendale/i di competenza secondo il seguente schema di distribuzione, indicativo e non limitativo e per conoscenza ad uffici eventualmente cointeressati:

- Direttore Tecnico e per esso Segreteria Tecnica
- RUP
- Amministrazione e Finanza
- Gare e Contratti
- Affari Generali-Legale

che tenga conto dei contenuti di ogni singolo documento e/o del soggetto posto in indirizzo o dell'area aziendale alla quale è indirizzato il documento.

4.2 Documento non digitale (cartaceo)

La distribuzione della **documentazione in ENTRATA** (posta in arrivo), **acquisita da documentazione cartacea,** ovvero non in forma digitale, una volta debitamente protocollata, dovrà essere eseguita da Segreteria Generale – Protocollo, con il seguente criterio, **ferme restando le casistiche e le relative disposizioni del precedente par. 3.1 lettera B)**:

1) Raccomandate, Posta Prioritaria, ed equivalenti
Distribuzione a: **ai destinatari in indirizzo** e comunque **ognuno per le rispettive competenze** ai seguenti uffici, e per conoscenza ad eventuali uffici cointeressati:

- Amministrazione e Finanza
- Amministrazione del Personale
- Affari Generali-Legale
- Gare e Contratti
- Direttore Tecnico e per esso Segreteria Tecnica

2) Plichi sigillati da Gara d'Appalto o provenienti da operatori economici
Distribuzione a: **ai destinatari in indirizzo** e comunque ai seguenti uffici:

- Gare e Contratti
-

3) Buste indirizzate all' Ufficio del Personale
Distribuzione a: **ai destinatari in indirizzo** e comunque ai seguenti uffici:

- Amministrazione del Personale

4) Pacchi, Corrieri, etc.
Distribuzione a: Copia (fronte pacco/busta) Segreteria\Amministratore-Originale ed **ai destinatari in indirizzo** e comunque **ognuno per le rispettive competenze** ai seguenti uffici, e per conoscenza ad eventuali uffici cointeressati:

- Amministrazione e Finanza
- Amministrazione del Personale
- Affari Generali-Legale
- Gare e Contratti
- Direttore Tecnico e per esso Segreteria Tecnica

5) Stampe (giornali, periodici, pubblicazioni, etc.) <u>DA NON PROTOCOLLARE</u>
Distribuzione a: Copia (fronte pacco/busta) Segreteria\Amministratore-Originale Area/ee aziendale di competenza

6) **FIR quarta copia**
Distribuzione a: **ognuno per le rispettive competenze** ai seguenti e comunque ai seguenti uffici:
- Responsabili siti e discariche,
- Responsabili TMB
- Ufficio tecnico (contabilità) e direzione tecnica
- Il cartaceo va ai responsabili perché devono tenerli in sito. Quindi ricevuta la comunicazione per il ritiro degli originali si dirigono presso l'ufficio protocollo

7) **Polizze assicurative, garanzie fidejussorie, ed equivalenti**
Distribuzione a:
- RUP
- Segreteria Tecnica nel caso in cui il RUP sia il Direttore Tecnico

5. INFORMAZIONI SULL'UTILIZZO DEL PROTOCOLLO AZIENDALE

Il c.d. "Protocollo Aziendale" è un sistema che, attribuendo un progressivo univoco, permette di classificare, marcare ed archiviare, secondo criteri predefiniti, le documentazioni, **sia in entrata che in uscita.**
Al momento della ricezione del documento da protocollare l'operatore, una volta che abbia avuto accesso al sistema con un proprio ID e propria password, provvederà ad inserirne le relative informazioni, procedendo alla compilazione dei campi che automaticamente appariranno a video.
Lo stesso deve essere applicato per le comunicazioni in uscita.

Le procedure da utilizzare afferenti al sistema software Folium, adottato dalla SAPNA SpA, sono descritte nell' *"Appendice 1"* **alla presente procedura, mentre nell'***"Appendice 2"* **è disponibile il Manuale sulla conservazione dei documenti prodotti da SAPNA SpA.**

Una volta proceduto **all'identificazione** si procederà **all'archiviazione** del documento che sarà effettuata, in caso di documento cartaceo, per il tramite di scansione dello stesso. Per i documenti pervenuti in forma digitale tale processo non richiederà la scansione materiale del documento in quanto il dato digitale è di norma già presente.
Ai fini della pura archiviazione farà fede il solo testo scansionato e depositato in forma "dematerializzata" ovvero in file *pdf posto in archivio sul server aziendale.

Il documento scansionato e/o acquisito per il tramite del sistema protocollare "Folium" sarà considerato come unico "originale" di riferimento anche ai fini della conservazione sostitutiva.

Atteso l'obbligo di produrre gli originali dei documenti aziendali in formato digitale in conformità alle previsioni del Codice dell'amministrazione digitale, ne deriva la necessità di dare seguito al processo di dematerializzazione finalizzato ad eliminare l'utilizzo della carta. Per la realizzazione di questo importante obiettivo sono di seguito sommariamente descritti i vari passi da compiere per la corretta gestione di un documento digitale, dalla sua creazione alla sua protocollazione:

a) L'operatore/redattore crea il documento utilizzando un comune programma di video scrittura (Word, ecc.);

b) L'operatore/redattore salva il documento in formato *.pdf (scegliendo il formato *.pdf nel menu a tendina "Salva come:" di Word). Laddove possibile, sarebbe auspicabile salvare il documento in formato pdf/A;
c) L'operatore/redattore invia il documento in formato *.pdf, al firmatario. L'invio può avvenire tramite email o caricando il documento su una cartella condivisa;
d) Il firmatario firma digitalmente il documento ricevuto utilizzando, possibilmente, una firma di tipo PAdES (vedi Differenza tra firme CAdES e PAdES) e ottenendo in questo modo un nuovo file ancora in formato *.pdf;
e) Il firmatario invia il documento firmato digitalmente all'operatore o direttamente o per il tramite della Segreteria di riferimento per l'acquisizione al protocollo. Anche in questo caso, l'invio può avvenire tramite e-mail o caricando il documento su una cartella condivisa;
f) L'operatore protocolla il documento firmato digitalmente caricando su Folium direttamente il file ricevuto dal firmatario per poi disporne l'invio;

durante l'iter appena descritto, il documento non viene mai stampato. Infatti la stampa, e successiva eventuale scansione, di un documento firmato digitalmente non hanno alcun valore giuridico; il documento informatico sottoscritto con firma digitale o con altro tipo di firma elettronica qualificata, ha l'efficacia [della forma scritta] prevista dall'articolo 2702 del codice civile (art. 21, c. 2 CAD).

Le postazioni che non siano quelle della Segreteria Generale e dell'unità Protocollo sono abilitate secondo le autorizzazioni di sistema di cui all'Allegato 3 alla presente procedura. Nel caso si necessitasse di ulteriori abilitazioni e/o autorizzazioni alla visione di documenti di classificazione diversa o superiore, è necessario produrre istanza scritta indirizzata all'Ufficio Affari Generali riportante le motivazioni della richiesta, che sarà sottoposta al vaglio dell'Amministratore Unico e ad eventuale approvazione di quest'ultimo.

6. REGISTRAZIONI e REPERTORIO

Il sistema protocollare utilizzato in SAPNA SpA permette di effettuare registrazioni del documento dotando lo stesso di **un numero di repertorio avente esclusiva validità interna** e classifica il documento attribuendo allo stesso data ed ora certa. Tale attribuzione costituisce la formazione di un Registro Ufficiale oltre che per la documentazione in Entrata, Uscita ed Interna anche per la modalità "repertorio" e viene usata per la conservazione di documenti come ad esempio determinazioni dell'Amministratore Unico, Contratti d'appalto, Appendici, etc.
Attualmente sono disponibili le seguenti modalità di repertoriazione, corrispondenti rispettivamente alle sigle identificative indicate:

- REPAPP Repertorio Appendici contrattuali
- REPCONTR Repertorio Contratti di fornitura, lavori, servizi, etc.
- REPDO Repertorio Disposizioni Organizzative
- REPDETAU Repertorio Determinazioni dell'Amministratore Unico
- REPMEPA Repertorio acquisizioni Mercato Elettronico PA
- REPVSU Repertorio Verbali di Somma Urgenza

Il numero attribuito in modalità Repertorio differisce da quello utilizzato per il protocollo in quanto è attribuito separatamente al fine di identificare un documento facente parte di una specifica raccolta di cui alle sigle sopraelencate. Anche in questo caso il documento sarà acquisito in formato *.pdf e automaticamente salvato dal sistema in forma non accessibile e non modificabile.

7. INDISPONIBILITA' DEL SISTEMA PROTOCOLLARE

In caso di guasti, indisponibilità del sistema, interruzioni di energia elettrica o altri eventi che non permettono l'utilizzo del software, si ricorrerà alla protocollazione manuale, per il tramite di scritta manuale su apposito registro.

- Se in assenza prolungata di energia elettrica si provvederà alla protocollazione del documento su registro cartaceo, indicando la data e l'ora del disservizio e protocollando la documentazione attribuendo numeri progressivi identificativi dei documenti in ingresso ed in uscita (in questo caso solo cartacei e dotati di firma autografa) in un apposito elenco trascrivendo manualmente i dati delle documentazioni, riportando data, ora oggetto e mittente/destinatari, nonché tipologia del documento (entrata, uscita, interna).
- Nel caso in cui si avesse l'indisponibilità prolungata solo dell'uso del programma protocollare, si procederà manualmente rilevando la posta certificata in entrata e procedendo con la posta in uscita, dotando i documenti della scritta "protocollo provvisorio" ed il numero successivo attribuito con le stesse modalità eseguite in precedenza per il protocollo cartaceo.
- Nel caso in cui, per guasti alle stampanti o al sistema, dovessero essere trascritti manualmente protocolli in entrata su buste o plichi afferenti gare o concorsi per le quali è necessario attestare oltre ai suindicati dati anche l'ora della consegna, si procederà manualmente, alla presenza di almeno un testimone che attesterà la data di ricezione che sarà apposta sul plico o busta, per il tramite di penna a sfera.
- Nel caso la trasmissione avvenga a mano, direttamente presso il soggetto destinatario, è necessario fare apporre timbro dell'Ente accettante su copia del documento, che riporti data, ora e firma dell'accettante sul documento trasmesso. Anche in questo caso le ricevute dell'avvenuta trasmissione devono essere consegnate alla Segreteria Generale per l'archiviazione in uno alla pratica emessa.

<<<<FINE DOCUMENTO>>>>

PO.07.2016

APPENDICE 1

GESTIONE DOCUMENTAZIONE

SEDE OPERATIVA

FLUSSO PROTOCOLLO E DISTRIBUZIONE POSTA

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI –DEDAGROUP-

Sistema Ambiente
Provincia di
Napoli

Manuale di Gestione
del protocollo informatico,
dei flussi documentali e degli archivi

(artt. 3 e 5 DPCM 3/12/2013)

DEDAGROUP
ICT NETWORK

Sommario

SEZIONE 1. Disposizioni generali

1.1 *Ambito di applicazione*

Il presente Manuale di gestione dei documenti è adottato ai sensi degli articoli 3 e 5 del D.P.C.M. 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", e descrive il sistema di ricezione, formazione, registrazione, trattamento e conservazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti della Società Ambiente Provincia di Napoli (S.A.P.NA.) S.p.A.

1.2 *Definizioni dei termini*

Per quanto riguarda la definizione dei termini, che costituisce la corretta interpretazione del dettato del presente Manuale, si rimanda, per quanto non specificato di seguito, al Glossario allegato (Allegato n.1).

SEZIONE 2. Articolazione e organizzazione delle Strutture

2.1 *Area Organizzativa Omogenea*

Ai fini della gestione dei documenti è individuata un'unica Area Organizzativa Omogenea denominata S.A.P.NA. S.p.A., composta dall'insieme di tutte le sue unità operative come da schema allegato (Allegato n.2).

Il codice identificativo dell'ente, rilasciato in fase di iscrizione presso l'Indice delle Pubbliche Amministrazioni (Codice iPA) è "sapns" a cui corrisponde la casella di posta elettronica certificata istituzionale sapna@pec.it.

Altre informazioni sono disponibili sul sito: www.sapnapoli.it

2.2 *Servizio archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi*

Nell'ambito dell'Area Organizzativa Omogenea, ai sensi dell'articolo 61, comma 1, del DPR 445/2000, è istituito il Servizio Archivistico per la gestione informatica del protocollo, dei documenti, dei flussi documentali e degli archivi (in seguito più brevemente: Servizio Archivistico). Il Servizio, ai sensi dell'articolo 61, comma 3, del DPR 445/2000 ha competenza sulla gestione dell'intera documentazione archivistica, ovunque trattata, distribuita o conservata, della S.A.P.NA. S.p.A. ai fini della sua corretta registrazione, conservazione, selezione e ordinamento.

Ai sensi del D. Lgs. 22 gennaio 2004 n. 42 e del DPR 445/2000, la S.A.P.NA. S.p.A. individua nell'Archivio una funzione essenziale per garantire la certezza, la semplificazione e la trasparenza dell'agire amministrativo, il reperimento di informazioni affidabili sotto il profilo giuridico, la tutela della memoria storica dell'Ente e il diritto di tutti i cittadini all'accesso all'informazione, alla formazione ed allo sviluppo della conoscenza.

L'Archivio, pur nella distinzione delle fasi di vita dei documenti e della loro valenza giuridica e storica, è da ritenersi logicamente unico e funzionalmente integrato.

Al Titolare del Servizio Archivistico per la tenuta del protocollo informatico e della gestione dei flussi documentali, sono affidati i compiti di cui all'art. 61, comma 3, del DPR 445/2000 e all'art. 4 del DPCM 03/12/2013.

2.3 Unicità del protocollo informatico

Nell'ambito dell'Area Organizzativa Omogenea la numerazione delle registrazioni di protocollo è unica e progressiva, senza distinzione fra i tre i tipi di documenti ("ingresso", "uscita" ed "interni"); tuttavia, a norma dell'articolo 53, comma 5, del DPR 445/2000 sono possibili registrazioni particolari.

La numerazione delle registrazioni si chiude al 31 dicembre di ciascun anno solare e ricomincia all'inizio dell'anno successivo.

Ciascun documento viene identificato mediante l'assegnazione di un unico numero di protocollo composto da almeno sette cifre numeriche e non è consentita l'attribuzione del medesimo numero ad altri documenti.

Con l'entrata in vigore del presente Manuale di Gestione cessano di avere effetto tutti i registri particolari o settoriali e relativi protocolli di settore e di reparto.

La S.A.P.NA. S.p.A. non riconosce validità a registrazioni particolari che non siano quelle individuate nell'elenco allegato (Allegato n. 3).

2.4 Modello operativo adottato per la gestione dei documenti

Per la gestione dei documenti è adottato un modello operativo semi-decentrato: l'ufficio protocollo è abilitato in generale alla ricezione e alla protocollazione della documentazione in arrivo ed in uscita.

Alcune unità, per motivi legati all'operatività aziendale, ed esclusivamente per i servizi afferenti le competenze della singola Unità, sono abilitate alla consultazione e/o alla protocollazione della sola corrispondenza generata in uscita dalle Unità medesime.

Nello specifico il modello operativo è il seguente:

1. **Protocollo in ingresso**
2. **Protocollo in Uscita**
3. **Protocollo interno**
4. **Invio dei Documenti**

ed è regolato dalla procedura operativa PO.07.2014-REV. 02 – 2022.

Questo modello comporta la partecipazione attiva di più uffici ed utenti abilitati a svolgere soltanto le operazioni di loro competenza di cui all'apposito elenco allegato (Allegato n.5).

La configurazione, il rilascio e la revoca delle competenze e delle abilitazioni sono autorizzati dal Titolare del Servizio Archivistico (Ufficio affari Generali-Segreteria Generale)

SEZIONE 3. Formazione dei documenti

3.1 Modalità di formazione dei documenti e contenuti minimi

Le modalità di formazione dei documenti, del loro contenuto e della loro struttura sono determinate da quanto previsto dal presente manuale; per quanto riguarda i documenti informatici la loro produzione è regolata sulla base di modelli standard presenti nel sistema informatico di gestione documentale.

Il contenuto minimo deve comunque garantire la presenza delle seguenti informazioni:

- Denominazione della SAPNA SpA, comprensiva del codice fiscale o partita IVA; per quanto riguarda i documenti su supporto cartaceo si utilizza il formato predisposto

dalla SAPNA SpA (carta intestata);
- Indirizzo completo (via, numero civico, codice avviamento postale, città, sigla della provincia, numero di telefono, numero di fax, indirizzo di posta elettronica dell'ente, PEC);
- Data: giorno, mese, anno, completa del luogo di emissione;
- Destinatario corredato degli elementi per la completa identificazione;
- Oggetto del documento, sufficientemente esaustivo del testo (ogni documento deve trattare un solo oggetto);
- Elenco numerato degli allegati, se presenti;
- Numero di protocollo;
- Testo;
- Indicazione del redattore del documento (nome e cognome anche abbreviato);
- Sottoscrizione autografa o elettronico/digitale.

3.2 Formato dei documenti informatici

I documenti informatici prodotti dalla SAPNA SpA - quali rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti ai sensi dell'art. 1, lett. p, del CAD - indipendentemente dal *software* utilizzato, prima della loro sottoscrizione con firma elettronico/digitale sono convertiti in uno dei formati *standard* previsti dalla normativa vigente in materia di conservazione (PDF, XML e TXT).

In particolare il formato PDF è previsto dalla normativa vigente in materia di conservazione, al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

I documenti ricevuti in un formato diverso da quelli prescritti dal presente manuale, se sottoscritti con firma digitale sono recepiti dal sistema e mantenuti e archiviati nel loro formato originale. Il sistema informativo converte il documento originale in uno dei formati standard previsti ai soli fini della corretta visualizzazione del contenuto.

In caso di migrazione dei documenti informatici, la corrispondenza fra il formato originale e quello migrato è garantita dal Responsabile della Conservazione.

3.3 Sottoscrizione dei documenti informatici

La sottoscrizione dei documenti informatici è ottenuta con un processo di firma elettronico/digitale conforme alle disposizioni di legge.

3.4 Tipologie particolari di documenti per i quali si stabiliscono modalità di trattamento specifiche

Tutti i documenti di cui all'Allegato n. 3 sono sottoposti a registrazione particolare con eventuali applicativi gestionali informatici autonomi. Gli elementi obbligatori della registrazione particolare sono riportati nella Sezione 6 di questo manuale.

3.5 Documenti cartacei: formazione e gestione dei documenti di base, minute e copie

Per ogni documento analogico destinato a essere spedito sono scritti due o più esemplari quanti sono i destinatari.

Uno di questi esemplari con apposito timbro di segnatura si conserva nel fascicolo del procedimento al quale si riferisce o nell'apposita serie documentaria. L'esemplare che si conserva nel fascicolo (minuta) può avere la dicitura "Minuta" o "Copia per gli atti".

Qualora si renda necessario, per ragioni amministrative, si possono produrre copie di un medesimo documento. Su ciascuna copia va apposta la dicitura "copia" a cura della struttura.

Le copie trasmesse per ragioni amministrative ad altre strutture organizzative sono conservate per tutto il tempo necessario allo svolgimento del procedimento cui il documento si riferisce e quindi eliminate secondo le norme previste.

3.6 Documenti informatici: originali, duplicati, copie

Gli atti formati con strumenti informatici, i dati e i documenti informatici, comunque detenuti dalla SAPNA SpA, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, duplicati, copie ed estratti, nei termini e per gli usi consentiti dalla legge.

Le diverse tipologie di copie, sia analogiche/cartacee sia informatiche, di documenti informatici, nonché i duplicati informatici, sono elencati nelle definizioni del CAD (Art. 1) e richiamate nel Glossario al presente Manuale (Allegato n. 1).

Le stesse, così come gli estratti, hanno la stessa efficacia probatoria dell'originale da cui sono tratte, quando la loro conformità all'originale non è espressamente disconosciuta o qualora risulti attestata nelle forme di cui agli artt. 23 e 23-*bis* del CAD.

SEZIONE 4. Ricezione dei documenti

4.1 Documenti in entrata

La ricezione di tutti i documenti in entrata e il rispettivo smistamento ai destinatari è a cura esclusivamente del Protocollo. Tutti i documenti indirizzati e pervenuti alla SAPNA SpA devono essere registrati, protocollati e smistati ai destinatari afferenti alle unità operative aziendali competenti, ad eccezione dei documenti non soggetti a registrazione di Protocollo (Allegato n. 4).

4.2 Ricezione dei documenti informatici tramite casella di posta elettronica certificata

La ricezione dei documenti informatici è assicurata tramite casella di Posta Elettronica Certificata riservata a questa funzione e accessibile solo dalla postazione dell'Ufficio di Protocollo. L'indirizzo PEC istituzionale dell'ente è: sapna@pec.it

L'applicativo di protocollo e gestione documentale utilizzato dalla SAPNA SpA è un *software PEC compliant*, in grado cioè di garantire anche la ricezione/spedizione dei messaggi di PEC in regime di interoperabilità, nonché di assicurare:

- La registrazione semiautomatica dei messaggi o del documento principale ed eventuali allegati (con parziale intervento dell'operatore nella compilazione di alcuni campi);
- La gestione automatica delle ricevute PEC;
- La gestione automatizzata di tutti gli oggetti legati al messaggio di PEC, quali le ricevute, gli avvisi di anomalia, etc.;
- La trasmissione di messaggi di PEC in partenza, per i dipendenti a ciò abilitati.

4.3 Ricevute attestanti la ricezione dei documenti

La ricevuta della consegna di un documento cartaceo, laddove richiesta, è costituita dalla fotocopia, prodotta dall'interessato, del primo foglio del documento stesso, con un timbro che attesti il giorno della consegna o dalla ricevuta di protocollazione prodotta dal sistema informatico.

Per la corrispondenza consegnata da vettori postali viene timbrata la modulistica del vettore con indicazione della data e firma dell'addetto ricevente.

Nel caso di ricezione dei documenti informatici, per esempio PEC, la notifica al mittente dell'avvenuto ricevimento è assicurata dal sistema elettronico.

SEZIONE 5. Registrazione a protocollo e segnatura dei documenti

5.1 Documenti soggetti a registrazione di protocollo

Tutti i documenti prodotti e ricevuti dalla SAPNA SpA, inclusi gli atti giudiziari, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati successivamente (articoli 5.2 e 6.1), sono registrati al protocollo.

5.2 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo (Allegato n. 4): gazzette ufficiali, bollettini ufficiali, notiziari della pubblica amministrazione, disposizioni organizzative interne, materiale statistico, atti preparatori interni, giornali, riviste, materiale pubblicitario, inviti a manifestazioni, stampe varie, plichi di libri e tutti quei documenti già soggetti a registrazione particolare da parte dell'ente, il cui elenco è allegato al presente manuale (Allegato n. 3).

5.3 Elementi obbligatori della registrazione di protocollo dei documenti ricevuti e spediti

La registrazione dei documenti ricevuti o spediti è effettuata in un'unica operazione. I requisiti necessari di ciascuna registrazione di protocollo sono:

a) Numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) Indicazione se trattasi di documento in entrata o in uscita o interno;
c) Data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
d) Mittente o destinatario dei documenti ricevuti o spediti, registrato in forma non modificabile;
e) Allegati (numero e descrizione)
f) Oggetto del documento, registrato in forma non modificabile;
g) Data e numero di protocollo dei documenti ricevuti, se disponibili;
h) Impronta del documento informatico, se trasmesso per via telematica, registrato in forma non modificabile;
i) Documento elettronico originale se trasmesso per via telematica attraverso posta elettronica certificata istituzionale associato a firma elettronica;

5.4 Registrazione dei documenti interni

I documenti prodotti dalla SAPNA SpA a solo uso interno, che non costituiscono atti preparatori e non rientrano in quelli esclusi da protocollazione, indipendentemente dal supporto sul quale sono formati, sono protocollati con modalità "Interna" sul Registro Ufficiale e vengono sottoposti allo stesso trattamento dei documenti ricevuti dall'esterno (registrazione, protocollazione, assegnazione).

La registrazione dei documenti interni è a cura degli uffici che producono il documento stesso.

5.5 Segnatura di protocollo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile (art. 55 del DPR 445/2000).

La segnatura di protocollo apposta o associata al documento è effettuata contemporaneamente alla registrazione di protocollo.

5.6 Segnatura dei documenti analogici

La segnatura di protocollo viene posta, di norma, sul primo foglio del documento analogico mediante un timbro o un'etichetta.

5.7 Elementi della segnatura

I requisiti necessariamente presenti sul timbro/etichetta di protocollo sono:

a) Denominazione della SAPNA SpA;
b) Indicazione se trattasi di documento in entrata/uscita/interno;
c) Titolo e classe ;
d) Data e orario di protocollo;
e) Numero progressivo di protocollo (anteponendo al numero ordinale una successione di simboli "zero", fino a costituire le sette cifre richieste);

Qualora la segnatura di protocollo riguardi documentazione la cui presentazione è soggetta a termini di scadenza (domande di concorso, bandi/avvisi pubblici, selezioni, gare, etc.), sulle buste consegnate *brevi manu*, in aggiunta alla segnatura viene specificato l'orario di consegna; la specifica oraria viene, pertanto, a contrassegnare l'orario di consegna all'Ufficio di Protocollo e, nel caso di consegna oltre il limite orario stabilito, evidenzia la documentazione pervenuta oltre la prevista scadenza.

5.8 Segnatura dei documenti informatici

Il software appone automaticamente la segnatura al documento informatico, riportando gli stessi elementi previsti per la segnatura del documento analogico.

Per i documenti informatici trasmessi ad altre pubbliche amministrazioni attraverso sistemi di interoperabilità, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un *file* conforme alle specifiche dell'*Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) e comprendono anche:

a) Oggetto del documento;
b) Mittente/destinatario o destinatari.

5.9 Annullamento delle registrazioni di protocollo

Il software di gestione del protocollo informatico consente, attraverso specifiche funzioni, di annullare, in tutto o in parte, le registrazioni di protocollo.

L'annullamento totale deve essere effettuato dagli operatori abilitati, previa autorizzazione del Responsabile dell'Unità operativa che ha prodotto il documento.

Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema con apposita dicitura "ANNULLATO". Il sistema durante la fase di annullamento registra le motivazioni che hanno reso necessario tale annullamento.

Per annullamento parziale si intende la rettifica di elementi erroneamente inseriti nella registrazione di protocollo.

Non è possibile, in nessun caso, annullare il numero di protocollo e mantenere valide le altre informazioni di registrazione o mantenere il numero di protocollo associandolo ad altre.

Le registrazioni annullate, nelle due fattispecie sopra individuate, rimangono comunque memorizzate nella base dati e sono evidenziate dal sistema.

5.10 Differimento dei termini di protocollazione

La registrazione della documentazione pervenuta avviene di norma nell'arco della giornata lavorativa successiva a quella di ricezione, ad eccezione di eventi particolari e/o ostativi che ne ritardino la protocollazione.

L'Ufficio di Protocollo può effettuare la registrazione in tempi successivi, fissando un limite di tempo entro il quale i documenti devono essere protocollati e, in caso di scadenze predeterminate, conferendo valore, attraverso apposita comunicazione che dia atto della causa del rinvio (es. sciopero, assenza del personale per motivi eccezionali, etc.), al timbro datario apposto sui documenti di cui si è differita la registrazione al protocollo e, in caso di documenti pervenuti a mezzo PEC, alla data di ricezione della stessa.

All'atto della registrazione dei documenti differiti, l'Ufficio di Protocollo registra anche la data effettiva di ricezione.

5.11 Registro di protocollo

Il Registro di protocollo è atto pubblico di fede privilegiata che certifica l'effettivo ricevimento e l'effettiva spedizione di un documento ad una data certa, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici a favore o a danno delle parti.

Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

5.12 Registro giornaliero e annuale di protocollo

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

La stampa PDF del registro giornaliero di protocollo viene effettuata giornalmente in maniera automatica dal sistema e trasmessa.

Quotidianamente è garantito il *back-up* di tutti i dati del sistema di gestione documentale, secondo quanto previsto dalla Sezione 12 del presente Manuale, dal Piano di Continuità Operativa e *Disaster Recovery* e dal Piano di Conservazione, ai sensi dell'articolo 50-*bis* del CAD, in conformità alle norme vigenti in materia di conservazione.

Delle registrazioni del protocollo informatico è sempre possibile estrarre evidenza analogica.

5.13 Registro di emergenza

Si definisce con "Emergenza di protocollo" qualsiasi situazione in cui gli addetti al Registro ufficiale di protocollo non abbiano la possibilità, per qualsiasi motivo, ad effettuare le normali registrazioni di protocollo per un periodo di tempo sufficientemente lungo.

Data la natura ufficiale del Registro di protocollo non è possibile stabilire a priori - deterministicamente - né le condizioni ambientali né i tempi che determinano le condizioni per l'apertura dell'emergenza. Sarà quindi valutato, di volta in volta e caso per caso, la necessità di ricorrere agli strumenti di protocollazione di emergenza. A titolo puramente indicativo, vengono rappresentati i casi più frequenti:

- Assenza di alimentazione dell'energia elettrica e malfunzionamento delle unità di continuità
- Malfunzionamento del programma software
- Assenza del collegamento al dominio (rete dati interno)
- Assenza del collegamento Internet (rete dati esterno)
- Disconnessione dei PC per motivi di sicurezza interna

Nei vari casi, lo svolgimento delle operazioni di protocollo saranno effettuate su un registro di emergenza a norma dell'articolo 63 del DPR 445/2000 e successivamente si opererà per il riversamento dei dati nel protocollo informatico, tramite le procedure previste e la modulistica allegata. (vedi Allegato 6)

Per quanto attiene l'azione da espletare in caso di emergenza, si distinguono due diverse situazioni:

- Sistema di protocollo informatico non accessibile e contemporanea indisponibilità di qualsiasi strumento informatico (ad esempio nel caso di mancata fornitura di energia elettrica) Rif. Successivo Par. 5.14;
- Sistema di protocollo informatico non accessibile ma disponibilità del Personal Computer "client" normalmente adibito a funzioni di protocollazione, Rif. Successivo Par. 5.15;

5.14 *Registro cartaceo di emergenza*

Nel primo caso l'emergenza sarà gestita su supporto cartaceo: all'inizio di ogni anno solare l'Ufficio di Protocollo provvede a istituire il registro di emergenza. La numerazione delle registrazioni di emergenza sarà progressiva in ragione d'anno, inizia da 1 per ogni anno solare e per ogni sede centrale o decentrata di protocollazione. Sui registri cartacei di emergenza l'operatore di protocollo registra cronologicamente gli eventi di inizio e termine dell'emergenza annotando gli estremi del provvedimento di autorizzazione (o di revoca) allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Al termine dell'emergenza il Registro (cartaceo) di emergenza sarà chiuso attraverso una particolare registrazione che renderà evidente l'ultimo numero di protocollo utilizzato in emergenza e registrerà data ed ora del ritorno alle condizioni di normale funzionamento.

Nell'eventualità di un secondo, successivo, avvio dell'emergenza nel corso dello stesso anno solare, il numero di protocollo ripartirà sequenzialmente dall'ultimo numero registrato.

Nel caso in cui le registrazioni di emergenza siano effettuate attraverso lo strumento cartaceo, non è obbligatoria, di norma, alcuna operazione di trascrizione dei dati dal registro di emergenza al registro di protocollo informatico. Non è infatti possibile garantire, in tali situazioni, la registrazione delle informazioni del registro di emergenza prima del ritorno alla normale operatività sul registro ufficiale.

5.15 *Registro elettronico di emergenza*

Nel secondo caso l'emergenza viene gestita attraverso uno strumento informatico installato su un elaboratore adibito alla funzione, di solito quello dell'Ufficio di Protocollo che effettua di norma le operazioni di registrazione, e viene attivato contestualmente all'avvio delle operazioni di autorizzazione alle procedure di emergenza.

Trattandosi di un'applicazione che, per sua natura, deve essere in grado di operare "fuori rete", ciascuna eventuale postazione di protocollazione di emergenza sarà associata ad un particolare codice identificativo che permetterà di distinguere univocamente le varie registrazioni di protocollo.

Per ogni sessione (una sessione può estendersi anche su più di una giornata lavorativa) di emergenza il numero di protocollo riparte dal numero 1.

Al termine dell'emergenza il Registro (elettronico) di emergenza sarà chiuso attraverso la "trasmissione" telematica di tutti i dati raccolti in emergenza verso il server (in cui l'applicativo di protocollo è nel frattempo stato ripristinato). L'utente riceverà conferma della

corretta trasmissione dei dati che, contestualmente, saranno totalmente cancellati (in maniera definitiva) dal database locale. Il numero di protocollo per la successiva, eventuale protocollazione di emergenza sarà ripristinato ad 1.

Successivamente dovrà procedersi alla verifica (attraverso apposita funzionalità dell'applicativo) della presenza dei pacchetti di dati di tutti gli eventuali operatori "di emergenza" e di procedere, senza alcuna possibilità di alterare i dati stessi, all'importazione definitiva sul Registro di protocollo generale.

La numerazione di protocollo dei documenti inseriti in emergenza segue la normale sequenza. La data di protocollazione è quella in cui avviene l'operazione di importazione.

La relazione fra il numero e la data del protocollo registrato in emergenza e numero progressivo acquisito sul registro ufficiale viene stabilita in modo univoco ed immodificabile attraverso la registrazione delle informazioni di collegamento su di un campo predisposto a tale scopo.

Il registro giornaliero (della data in cui è avvenuta l'importazione dei dati) di protocollo conterrà anche i protocolli acquisiti in emergenza.

L'operatore di protocollo abilitato avrà la facoltà, in qualsiasi momento, di individuare, fra tutte le registrazioni del Registro Ufficiale, quelle derivanti da registrazione di emergenza.

SEZIONE 6. Documentazione particolare

6.1 Determinazioni dell'Amministratore Unico, Determinazioni Dirigenziali (se utilizzate), Disposizioni Organizzative, Contratti con fornitori, pubblicazioni all'albo pretorio di gare, affidamenti, aggiudicazioni e pubblicazioni varie.

I documenti in titolo sono soggetti a repertoriazione e pertanto oggetto di attribuzione di data certa. Per quelli da ritenere già soggetti a registrazione particolare da parte di SAPNA SpA (ad esempio Determinazioni, pubblicazioni, etc.) non sussiste l'obbligo di registrazione al protocollo. Per i documenti per i quali vi è obbligo di legge, gli stessi sono portati in conservazione (vedasi elenco di cui all'Allegato n. 3).

Ogni registrazione riporta:

a) Dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile);
b) Numero di repertorio progressivo e annuale (generato in modo non modificabile).

Per le pubblicazioni all'albo pretorio si rimanda all' apposito regolamento.

6.2 Documentazione di gare telematiche.

Per la documentazione delle gare telematiche, la SAPNA SpA si avvale delle procedure di gara gestite mediante il mercato elettronico Consip (ME.PA.).

6.3 Corrispondenza con più destinatari e documenti originali plurimi

Tutte le comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo. Nel caso di posta in partenza i destinatari sono descritti in elenchi associati alla minuta del documento e alla registrazione di protocollo si procede secondo le modalità previste dal manuale operativo del software e da quanto espresso nel successivo articolo 9.3.

Anche ai documenti originali plurimi, o in copia per conoscenza, si darà un unico numero di protocollo e, successivamente, gli stessi saranno assegnati ai singoli destinatari.

6.4 Allegati

Tutti gli allegati devono essere trasmessi con i documenti a cui afferiscono alle postazioni di protocollo per la registrazione. Di regola viene apposta la segnatura solo sulla lettera di accompagnamento o sul documento principale. Se richiesto, anche su ogni allegato analogico viene riportato il timbro della segnatura di protocollo. Il sistema informatico provvede automaticamente a registrare gli allegati come parte integrante di un documento elettronico.

6.5 Documenti pervenuti per errore alla SAPNA

Qualora pervengano all'ente documenti di competenza di altre amministrazioni, questi vanno inviati al destinatario. Nel caso in cui il destinatario non sia individuabile, il documento deve essere rimandato al mittente.

6.6 Documenti smistati e assegnati erroneamente

I documenti smistati e assegnati erroneamente devono ritornare all'Ufficio di Protocollo –ove possibile con l'indicazione del nuovo assegnatario. L'ufficio provvederà il più velocemente possibile alla riassegnazione.

6.7 Oggetti plurimi (documento in entrata relativo a procedimenti diversi)

Qualora un documento in entrata presenti più oggetti, relativi a procedimenti diversi, si procede a registrare il documento con unico numero di protocollo ed assegnarlo ai destinatari dei diversi Settori e/o Servizi competenti.

L'originale viene inviato al destinatario indicato nel documento oppure, nel caso di destinatari plurimi, al primo in indirizzo.

6.8 Trasmissioni telematiche

Le trasmissioni telematiche di documenti sono trasmessi/ricevuti dalla SAPNA SpA con immissione diretta dei dati sul server dell'Ente destinatario. I documenti possono essere trasmessi senza firma digitale se inviati tramite linee di comunicazione sicure, riservate, e ad identificazione univoca, attivati con i singoli enti destinatari.

Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

6.9 Gestione della posta elettronica ordinaria

La posta elettronica ordinaria è utilizzata per l'invio di comunicazioni, informazioni e documenti.

In particolare, è sufficiente ricorrere ad un semplice messaggio di posta elettronica per convocare riunioni (interne all'ente), inviare comunicazioni di servizio o notizie dirette ai dipendenti in merito a informazioni generali di organizzazione, diffondere circolari e ordini di servizio (gli originali si conservano nel fascicolo specifico a cura del Settore competente), documenti informatici, copie di documenti cartacei, spedire copie dello stesso documento a più destinatari. A chi ne fa richiesta deve sempre essere data la risposta dell'avvenuto ricevimento.

La posta elettronica ordinaria non può essere utilizzata per la spedizione di documenti con firma digitale, per i quali è prevista l'apposita casella ufficiale di posta elettronica certificata.

Non è possibile inviare messaggi da caselle di posta elettronica ordinaria quando il contenuto di questi impegni la SAPNA SpA verso terzi.

La trasmissione di documenti che necessita di una ricevuta di invio e di consegna è effettuata tramite il sistema di posta elettronica certificata. Per quanto riguarda la gestione della posta elettronica nelle pubbliche amministrazioni si applicano gli articoli 45-49 del D.lgs. 82/05 (CAD) come modificato dal D.lgs. 235/10.

Nel caso di ricezione di messaggi all'indirizzo di posta elettronica ordinaria personale o dell'ufficio di appartenenza, è onere del Responsabile del Procedimento individuare, in base al contenuto, i messaggi rilevanti per l'Ente, da inoltrare per la protocollazione alla casella di posta elettronica ordinaria dell'Ufficio di Protocollo**: ufficio.protocollo@sapnapoli.it**

SEZIONE 7. Assegnazione dei documenti

7.1 Assegnazione

L'assegnazione dei documenti ai destinatari è effettuata, attraverso lo smistamento, per competenza o per conoscenza, dall' Ufficio di Protocollo.

La documentazione indirizzata espressamente all'Unità Operativa (Ufficio) dovrà essere smistata al Responsabile dell'Ufficio. Se indirizzata al Responsabile del Procedimento dovrà essere indirizzata direttamente a quest'ultimo o ad un suo delegato specificamente indicato.

7.2 Modifica delle assegnazioni

Nel caso di assegnazione inesatta dei documenti, il destinatario del settore che ha ricevuto il documento è tenuto a:

- Restituire l'assegnazione informatica tramite la posta elettronica aziendale indirizzata all' Ufficio di Protocollo, specificando le indicazioni necessarie.
- Consegnare immediatamente il documento all'Ufficio assegnante che provvederà alla corretta riassegnazione.

Il sistema di gestione informatica dei documenti tiene traccia delle riassegnazioni e dei loro tempi.

7.3 Consegna dei documenti informatici

I documenti informatici e/o le immagini digitali dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici, o ai responsabili di procedimento, tramite il sistema informatico di gestione documentale. Si rimanda anche alla Sezione 11.

SEZIONE 8. Classificazione e fascicolazione dei documenti

8.1 Classificazione dei documenti

Tutti i documenti ricevuti o prodotti, indipendentemente dal supporto sul quale sono formati, devono essere classificati in base ad uno specifico titolario di classificazione. I dati di classificazione sono riportati su tutti i documenti. Il programma di protocollo informatico dispone di funzioni di verifica dell'avvenuta classificazione dei documenti.
Il Titolario può essere soggetto a successive rivisitazioni secondo necessità.

8.2 Formazione e identificazione dei fascicoli

La Fascicolazione ed identificazione dei fascicoli informatici sarà organizzata successivamente nell'ambito delle attività di digitalizzazione della gestione documentale.

SEZIONE 9. Spedizione dei documenti destinati all'esterno

9.1 *Spedizione dei documenti cartacei*

L'Ufficio di Protocollo provvede alla spedizione dei documenti cartacei dopo la loro protocollazione in uscita. Nel caso di raccomandate AR queste dovranno essere complete di modulistica compilata, mentre nel caso di posta inviata per il tramite di servizio postale privato, del "modulo accettazione spedizione postali". Infine, nel caso di posta o pacchi inviati per il tramite di corriere espresso tipo DHL, UPS, TRACO, MAILBOX, etc. della distinta di spedizione.

Le informazioni minime da indicare sono:

- Numero di Protocollo
- Tipo di spedizione richiesto
- Ufficio che ha richiesto la spedizione
- Destinatario
- Indirizzo – Cap - Comune - Provincia
- Numero tracciamento
- Numero di spedizioni
- Tipologia (cittadina, nazionale, internazionale)

9.2 *Spedizione dei documenti informatici*

La spedizione dei documenti informatici avviene all'interno del sistema informatico di gestione dei documenti, dopo essere stati protocollati e comunque secondo i seguenti criteri generali:

1. I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari o pubblicato sull'Indice PA (IPA);
2. Per la spedizione la SAPNA SpA si avvale di una casella di posta elettronica certificata;
3. L'Ufficio di Protocollo provvede a:
   a. Effettuare l'invio telematico utilizzando i servizi di autenticazione;
   b. Verificare l'avvenuto recapito dei documenti spediti per via telematica;
   c. Archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo.

Per la riservatezza delle informazioni contenute nei documenti elettronici, chi spedisce si attiene a quanto prescritto dall'articolo 49 del D.lgs. 82/05 (CAD), come modificato dal d.lgs. 235/10.

La spedizione di documenti informatici al di fuori dei canali istituzionali descritti è considerata una mera trasmissione di informazioni senza che a queste la SAPNA SpA riconosca un carattere giuridico-amministrativo che la impegni verso terzi.

SEZIONE 10. Gestione dei flussi di documenti cosiddetti interni

10.1 *Comunicazioni informali*

Questo genere di informazioni possono essere trasmesse/ricevute per posta elettronica ordinaria purché si tratti di scambio di informazioni e documenti che non impegnino la SAPNA SpA verso terzi o possono far nascere diritti o doveri.

10.2 Scambio di documenti fra gli uffici

Della comunicazione/scambio di informazioni, di documenti o unità archivistiche giuridicamente rilevanti all'interno dell'ente deve essere tenuta traccia nel sistema informatico di gestione dei documenti e degli archivi.

SEZIONE 11. Scansione dei documenti su supporto cartaceo

11.1 Documenti soggetti a scansione

I documenti **su supporto cartaceo** dopo le operazioni di registrazione, e segnatura, possono essere acquisiti, all'interno del sistema di protocollo informatico, in formato immagine con l'ausilio di scanner.

11.2 Processo di scansione

Il processo di scansione si articola nelle seguenti fasi:

- Acquisizione delle immagini in modo che a ogni documento, anche composto da più fogli, corrisponda un unico file in un formato standard abilitato alla conservazione;
- Verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- Collegamento delle rispettive immagini alla registrazione di protocollo, in modo non modificabile;
- Memorizzazione delle immagini, in modo non modificabile.

Il processo di scansione dei documenti cartacei, al fine della loro trasformazione in formato immagine, avviene nella fase di registrazione, esclusivamente a cura del Protocollo per la corrispondenza in entrata.

SEZIONE 12. Conservazione e tenuta dei documenti

12.1 Conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei

La SAPNA ha in fase di attivazione le procedure per la conservazione e memorizzazione dei documenti analogici, informatici e delle rappresentazioni digitali dei documenti cartacei conformemente alla normativa vigente in materia.

12.2 Conservazione dei documenti informatici

La SAPNA ha in fase di attivazione le procedure per la conservazione a norma dei documenti informatici conformemente alla normativa vigente in materia.

Il manuale di gestione e i relativi aggiornamenti devono essere conservati integralmente e perennemente nell'archivio dell'ente.

SEZIONE 13. Accesso

13.1 Accessibilità da parte degli utenti appartenenti alla SAPNA SpA

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili e password. Il sistema applica automaticamente l'inserimento del livello predeterminato.

Per quanto riguarda i documenti riservati si rimanda alla normativa vigente in materia di accesso agli atti amministrativi, che in generale regola tutte le possibilità di accesso, consultazione e riproduzione dei documenti.

SEZIONE 14. Albo Pretorio on-line

E' istituito l'Albo Pretorio on-line disponibile presso il sito telematico istituzionale della SAPNA SpA all'indirizzo www.sapnapoli.it

Per il contenuto ed i requisiti delle richieste di pubblicazione si rimanda alle disposizioni ivi previste.

SEZIONE 15. Pubblicazione

15.1 *Pubblicazione e divulgazione*

In ottemperanza all'art. 5, comma 3, del DPCM 3 dicembre 2013, il presente Manuale di gestione viene reso accessibile nelle seguenti forme:

- Per il personale della SAPNA SpA, mediante diffusione interna, con qualsiasi mezzo;
- Per il pubblico, mediante pubblicazione sul sito internet della S.A.P.NA. SpA (www.sapnapoli.it);
- Tramite la pubblicazione nel settore di corrispondenza sul sito istituzionale della SAPNA SpA, degli atti di adozione e revisione.

ALLEGATO N. 1-

DEFINIZIONI E NORME DI RIFERIMENTO (GLOSSARIO)

Ai fini del presente Manuale si intende:

- **Amministrazione, l a S . A . P . N A . S p A**
- **D o c u m e n t o ,** le informazioni o l'insieme delle stesse - rese disponibili su supporto analogico o digitale - che l'Amministrazione è in grado di produrre, utilizzare, acquisire e gestire in ambito burocratico amministrativo, tecnico e giuridico, al fine di conseguire il proprio scopo sociale;
- **Testo Unico,** il decreto del Presidente della Repubblica 20 dicembre 2000 n.445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Regole tecniche,** il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428 e al DPCM del 3 dicembre 2013 inerente regole tecniche per il protocollo informatico;
- **"CAD",** il Decreto Legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale modificato dal Decreto Legislativo 30 dicembre 2010, n. 235.
- **Segnatura di protocollo:** l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti la protocollazione del documento stesso;
- **Classificazione:** l'attività che consente di organizzare tutti i documenti correnti prodotti dall'Amministrazione, secondo uno schema articolato di voci (il cd. titolario) che descrive l'attività del soggetto produttore identificandone funzioni e competenze;
- **Assegnazione:** l'operazione d'individuazione dell'ufficio competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
- **Titolario di classificazione:** un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Amministrazione, che consente di classificare, in maniera logica, sistematica e coerente, la documentazione archivistica, che venga prodotta o comunque acquisita dall'Amministrazione, durante lo svolgimento dell'attività amministrativa;
- **Fascicolo:** l'unità archivistica che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare.
- **Casella PEC:** casella di posta elettronica, istituita da un'AOO, per la ricezione dall'esterno e per la spedizione all'esterno dei documenti da registrare a protocollo.
- **Firma digitale:** particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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.
- **Registro giornaliero di protocollo - RGP:** registro su cui si memorizzano quotidianamente i documenti ricevuti e spediti da SAPNA; è atto pubblico di fede privilegiata.

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- **AOO** Area Organizzativa Omogenea: insieme definito di unità organizzative di una amministrazione, che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali. h particolare una AOO utilizza per il servizio di protocollazione un'unica sequenza numerica, rinnovata ogni anno solare. La SAPNA costituisce un'unica AOO.

- **MdG** Manuale di Gestione del protocollo informatico e gestione documentale
- **RPA** Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **UOP** Unità Organizzativa Operativa di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** Unità Operative Responsabili - un insieme dì risorse umane e strumentali (di solito un ufficio) cui è affidata una competenza omogenea, nell'ambito della quale i dipendenti assumono la responsabilità nella trattazione di affari o procedimenti amministrativi.
- **SdP** Sistema di protocollazione informatica e gestione documentale – il software utilizzato per la protocollazione dei documenti e per la gestione dei flussi documentali.
- **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;
- **Duplicato informatico:** il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza dì valori binari del documento originario;

ALLEGATO N. 2-

PRINCIPALI RIFERIMENTI DEGLI UFFICI e/o UNITA' OPERATIVE DELLA S.A.P.NA. SPA

- DIREZIONE TECNICA - AREA TECNICA

  Segreteria Tecnica, Settore Area Tecnica, Siti, Discariche, Flussi, Ingegneria, Contabilità Industriale, Servizi, TMB Giugliano, TMB Tufino

- UFFICIO AMMINISTRAZIONE DEL PERSONALE
- UFFICIO AMMINISTRAZIONE E FINANZA
- UFFICIO GARE E CONTRATTI
- UFFICIO AFFARI GENERALI

  Segreteria Generale, Protocollo, Legale, ITC

ORGANI DI CONTROLLO E PREVENZIONE

- RESPONSABILE PREVENZIONE DELLA CORRUZIONE
- ORGANISMO DI VIGILANZA

ALLEGATO N. 3-

ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONI PARTICOLARI

(inserimento a Repertorio)

I documenti sottoelencati non vengono registrati sul sistema di protocollazione informatica perché già soggetti a registrazione particolare da parte dell'Amministrazione:

- le Determinazioni dell'Amministratore Unico,
- le Determinazioni dirigenziali (se adottate)
- le Disposizioni Organizzative
- i contratti verso fornitori

ELENCO DEI DOCUMENTI NON SOGGETTI A REGISTRAZIONE

(già soggette a identificazione e tracciabilità)

- le pubblicazioni all'Albo Pretorio (assegnazione progressivo di pubblicazine)
- le Fatture elettroniche (assegnazione da sistema)
- altri tipi di verbalizzazioni previsti dalla legge o da regolamenti.

ALLEGATO N. 4-

DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

- le gazzette ufficiali;
- i bollettini ufficiali e notiziari della pubblica amministrazione,
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste, i libri, i materiali pubblicitari;
- gli inviti a manifestazioni;
- tutti i documenti non sottoscritti o sottoscritti con firma apocrifa;
- i documenti erroneamente indirizzati alla SAPNA (da trasmettere a chi di competenza, se individuabile, o, altrimenti, da restituire al mittente);
- la corrispondenza interna esclusa quella che in modo diretto o indiretto ha contenuto probatorio e comunque attiene alla gestione dei procedimenti amministrativi.

Vengono altresì esclusi dall'obbligo di protocollazione i seguenti documenti cartacei/digitali interni:

- Richieste ferie
- Richieste permessi
- Le ricevute di ritorno delle raccomandate A.R.
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura
- Corsi di aggiornamento, Convocazioni ad incontri o riunioni interne e corsi di formazione interni

Sono esclusi dalla registrazione di protocollo tutti i documenti già soggetti a registrazione particolare dell'Amministrazione di cui all'allegato n° 3. I documenti di cui al presente articolo possono, se ritenuto necessario, essere inseriti nel registro degli atti generici.

ALLEGATO N. 5-

Amministratore del sistema di protocollo:

Ufficio Affari Generali

Operatore di protocollo:

abilitato a tutte le funzioni di registrazione (ingresso, uscita, interno), ricerca e consultazione

I dipendenti abilitati

Operatore di Protocollo in uscita:

abilitato alla registrazione dei documenti in uscita, interni e alla consultazione

I dipendenti autorizzati alla registrazione di documenti in uscita in servizio presso le Unità operative dell'Area Organizzativa Omogenea

Utente di protocollo:

abilitato alla consultazione dei documenti in relazione al flusso di assegnazione

Tutti i dipendenti della SAPNA che trattano o accedono alla documentazione amministrativa

ALLEGATO N. 6-

PROTOCOLLO DI EMERGENZA (ART. 63 D.P.R. 445/ 00)

Per attivare il registro di protocollo di emergenza si deve verificare almeno una delle seguenti tre condizioni, non necessariamente dipendenti una dall'altra:

1. guasto al software di protocollazione informatica;
2. guasto al sistema informatico di gestione;
3. mancanza di energia elettrica.
4. guasto alla rete di connessione

Quando una di queste si verificasse, si dovrà attivare un protocollo di emergenza su supporto cartaceo o informatico. La gestione del protocollo di emergenza comporterà la protocollazione sia in entrata che in uscita da parte dell'Ufficio di Protocollo.

Per l'attivazione del protocollo di emergenza si deve:

A) Redigere il verbale di attivazione (modulo n. 1);
B) Compilare il registro di emergenza (modulo n. 2);
C) Dare comunicazione alla struttura organizzativa dell'amministrazione della attivazione dell'emergenza ;

Al termine dell'emergenza si deve:

A) Revocare l'autorizzazione al protocollo di emergenza (modulo n. 3);
B) Inserire manualmente le registrazioni di emergenza nel protocollo informatico;
C) Dare comunicazione alla struttura organizzativa dell'amministrazione della revoca dell'emergenza;
D) Conservare il registro di emergenza;

La numerazione del registro di emergenza è unica per l'intero anno, ricominciando dal numero successivo all'ultimo utilizzato per ogni attivazione. Per i relativi dettagli si fa riferimento ai paragrafi 5.13, 5.14, 5.15.

Modulo n. 1

AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE

DI PROTOCOLLO SUL REGISTRO DI EMERGENZA

(art. 63 DPR 445/2000)

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445:

- preso atto che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

non è possibile utilizzare la normale procedura informatica;

- si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Il Responsabile del servizio archivistico per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Modulo n. 2

Numero Registro. emergenza	Data	Tipo	Mittente/ Destinatario	Oggetto	Titolo	Classe	Sottoclasse	n. Fascicolo

Modulo n. 3

REVOCA AUTORIZZAZIONE ALLO SVOLGIMENTO DELLE OPERAZIONI DI REGISTRAZIONE DI PROTOCOLLO SUL REGISTRO

DI EMERGENZA

(art. 63 DPR 445/2000)

Ai sensi dell'art. 63 del dPR. 28 dicembre 2000 n. 445:

- ricordato che, per le cause sotto riportate:

Data interruzione	
Ora interruzione	
Causa della interruzione	

non essendo possibile utilizzare la normale procedura informatica, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

preso atto che, dalla data e ora sotto riportate:

Data ripristino	
Ora ripristino	

È stato ripristinato il normale funzionamento della procedura informatica

- si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

- si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Il Responsabile del Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

PO.07.2016
APPENDICE 2

GESTIONE DOCUMENTAZIONE
SEDE OPERATIVA
FLUSSO PROTOCOLLO E DISTRIBUZIONE POSTA

MANUALE SULLA CONSERVAZIONE DEI DOCUMENTI

PRODOTTI DA SAPNA SPA.

– ENERJ-

Manuale di Conservazione

di Enerj S.r.l.

EMISSIONE DEL DOCUMENTO

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

REGISTRO DELLE VERSIONI

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

INDICE DEL DOCUMENTO

1 INTRODUZIONE

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

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

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

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

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

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

2 SCOPO E AMBITO DEL DOCUMENTO

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

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

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

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

Il presente documento sostituisce le versioni precedenti.

2.1 Specificità di contratto

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

Torna al sommario

3 TERMINOLOGIA

3.1 GLOSSARIO

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

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

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

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

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

certificatore accreditato	soggetto, pubblico o privato, riconosciuti dall' Agenzia per l'Italia Digitale che emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia Digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia Digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Contratto di Servizio	Documento contrattuale stipulato tra il Cliente (Produttore) ed Enerj (Conservatore) che contiene la descrizione analitica del servizio. Gli accordi di dettaglio sono riportati negli specifici allegati
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

fascicolo informatico	aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del CAD.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di *hash*	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Hardware Security Module	dispositivi per la gestione sicura delle firme digitali che ne velocizzano l'apposizione e ne permettono la completa gestione in remoto
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione

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

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

pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

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

staticità	caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

3.2 ACRONIMI

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

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

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

4 NORMATIVA E STANDARD DI RIFERIMENTO

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

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

4.1 Normativa inerente per la conservazione - Legislazione Italiana

- **Codice Civile** – "Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica.";
- **Legge 7 agosto 1990, n. 241 e s.m.i.** – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i.** – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **Decreto Legislativo 11 febbraio 2005 n. 68** . Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3;
- **Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **Decreto del 2 novembre 2005** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (Gazzetta Ufficiale n. 266 del 15-11-2005) del Ministro per l'Innovazione e le Tecnologie;
- **Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009** - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;
- **Deliberazione Cnipa del 21 maggio 2009, n. 45** (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010). Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;

- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- **Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013** - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- **Circolare AGID 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- **Decreto del Ministero dell'Economia e delle Finanze 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

4.2 Altre normative

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

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

4.3 Standard tecnici internazionali di riferimento

4.3.1 ISO/IEC

- **UNI EN ISO 9000:2005** - Sistemi di gestione per la qualità - Fondamenti e vocabolario;
- **UNI EN ISO 9001:2008** - Sistemi di gestione per la qualità - Requisiti;
- **UNI EN ISO 9004:2009** - Gestire un'organizzazione per il successo durevole: L'approccio della gestione per la qualità;
- **UNI EN ISO 19011:2012** - Linee guida per audit di sistemi di gestione;
- **ISO 14721:2012** - Space data and information transfer systems - Open archival information system (OAIS) - Reference model; Sistema informativo aperto per l'archiviazione;
- **UNI ISO 31000:2010** - Gestione del rischio - Principi e linee guida;
- **ISO/IEC 27000:2012** - Overview and vocabulary;
- **ISO/IEC 27001:2013** - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ISO/IEC 27002:2013** - Code of practice for information security controls;
- **ISO/IEC 27005:2011** - Information technology -- Security techniques -- Information security risk management;
- **UNI ISO 15489-1:2006** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management;
- **UNI ISO 15489-2:2007** - Informazione e documentazione - Gestione dei documenti di archivio - Linee Guida sul record management;
- **UNI 11386:2010** - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.
- **ISO 15836:2009** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

4.3.2 ETSI (European Telecommunications Standards Institute)

- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** - Electronic Signatures and

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

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

4.3.3 OAIS (Open Archival Information System)

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

Torna al sommario

5 RUOLI E RESPONSABILITÀ

5.1 Ruoli esterni al SdC

5.1.1 Produttore

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

5.1.2 Fruitore

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

5.1.3 Certification Authority e fornitori di servizi di Firma Digitale

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

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

5.1.4 Time Stamping Authority

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

5.2 Ruoli interni al SdC

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

5.2.1 Responsabile del Servizio di Conservazione (RSC)

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

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

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

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

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

5.2.3 Responsabile funzione archivistica di conservazione (RFA)

- Definisce e gestisce il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- Definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici;
- Monitora il processo di conservazione e attua analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- Collabora con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

5.2.4 Responsabile del Trattamento dei Dati personali (DIR)

- Garantisce il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;
- Garantisce che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza

5.2.5 Responsabile sistemi informatici per la conservazione (RSI)

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

5.2.6 Responsabile sviluppo e manutenzione del sistema (RSM)

- Coordina lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione;
- Pianifica e monitora i progetti di sviluppo del sistema di conservazione;
- Monitora gli SLA relativi alla manutenzione del sistema di conservazione;
- Si interfaccia con il produttore in relazione alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche;
- Gestisce lo sviluppo degli applicativi software connessi al servizio di conservazione.

Di seguito vengono riportati i nominativi attualmente in carica.

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

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

Torna al sommario

6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 Organigramma

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

6.2 Strutture organizzative

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

6.2.1 Attività proprie di ciascun contratto di servizio di conservazione

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

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

6.2.2 Attività proprie di gestione dei sistemi informativi

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

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

Torna al sommario

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE

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

7.1 Oggetti conservati

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

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

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

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

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

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

7.2 Formati

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

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

7.3 Pacchetto di versamento

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

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

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

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

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

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

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

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

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

7.4 Pacchetto di archiviazione

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

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

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

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

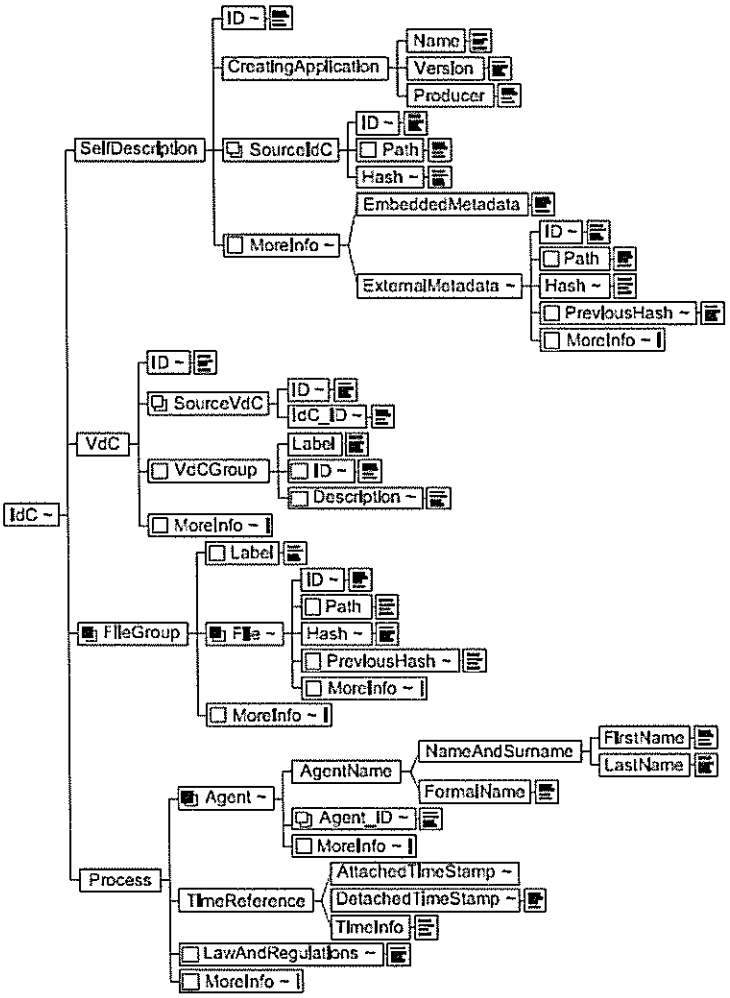


Figura 1 - Rappresentazione UML del contenuto del PdA

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

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

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

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

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

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

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

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

7.5 Pacchetto di distribuzione

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

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

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

Il PdD è corredato da ulteriori informazioni quali:

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

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

soggetti autorizzati dal Cliente.

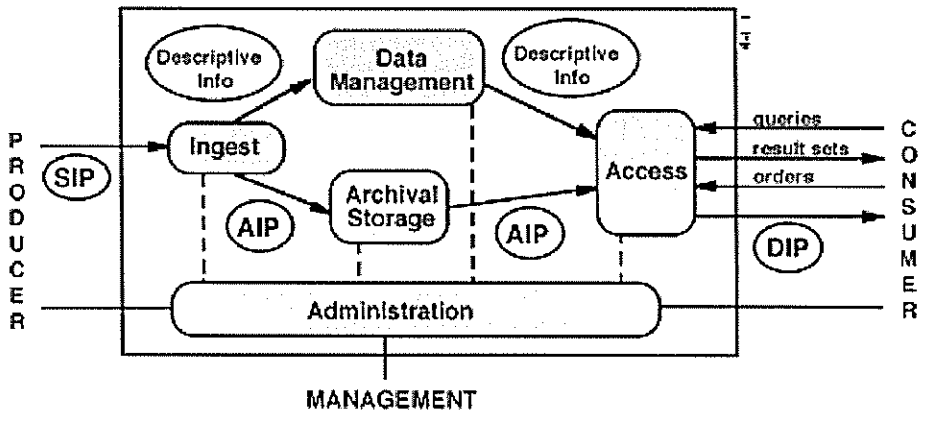
Torna al sommario

8 IL PROCESSO DI CONSERVAZIONE

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

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

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



Schema 1 - **Modello funzionale OAIS**

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

Le principali modalità di trasmissione del pacchetto di versamento sono:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.4 Rifiuto dei PdV e modalità di comunicazione delle anomalie

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

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

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

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

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

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

8.5 Preparazione e gestione del PdA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

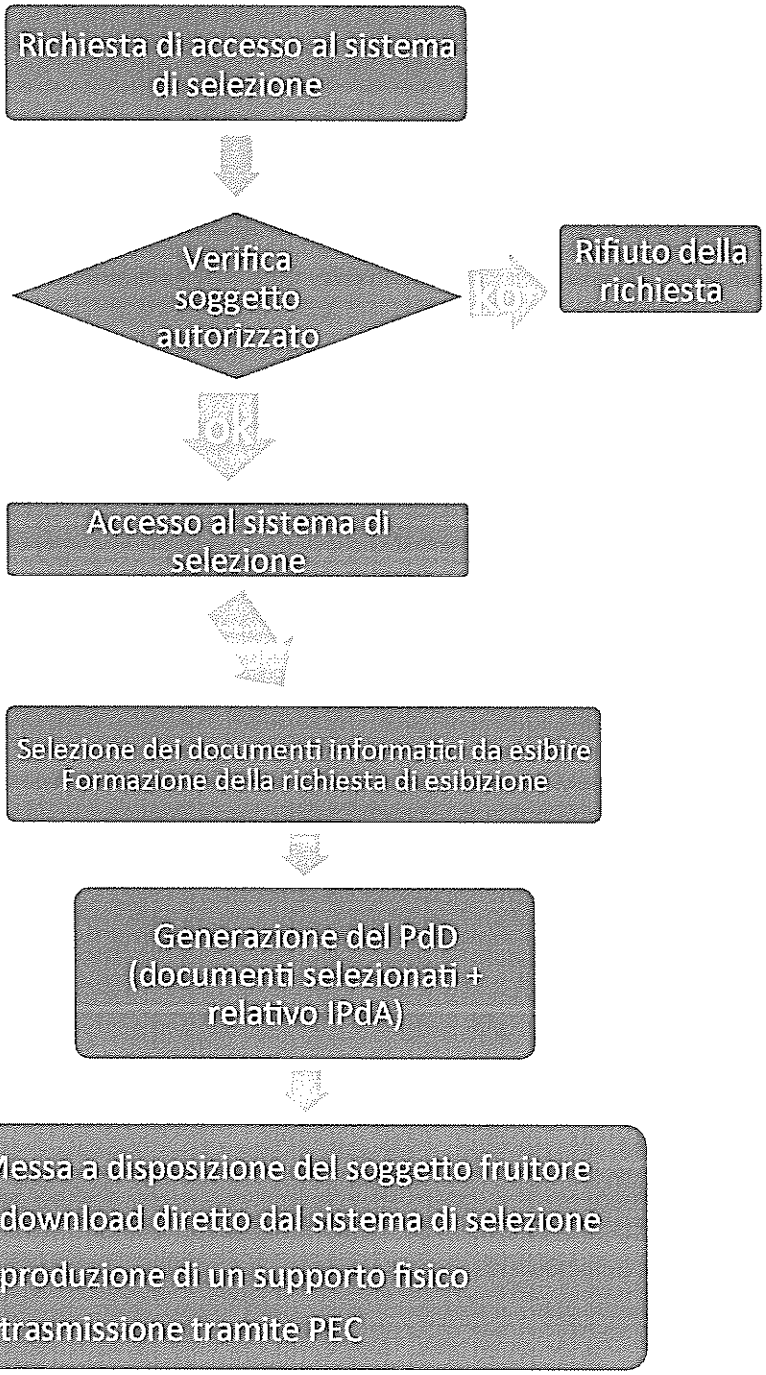
I supporti fisici sono trasportati a cura e responsabilità di personale Enerj o

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

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

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

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



Schema 2 - Processo di preparazione e gestione del PdD

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

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

8.7.1 Produzione di duplicati informatici

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

Il procedimento di produzione di duplicati si attiva automaticamente:

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

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

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

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

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

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

8.7.3 Produzione di copie informatiche di documenti analogici

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

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

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

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

8.8 Scarto dei pacchetti di archiviazione

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

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

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

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

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

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

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

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

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

Torna al sommario

9 IL SISTEMA DI CONSERVAZIONE

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

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

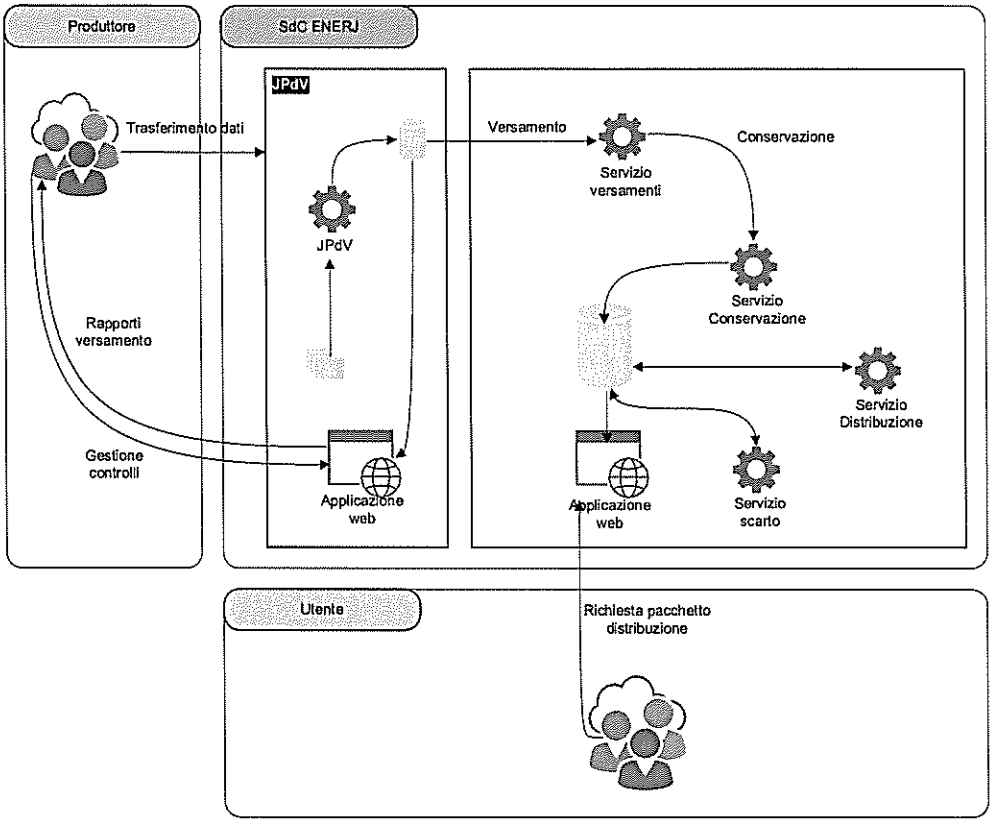
9.1 Componenti Logiche

Il SdC è composto dai seguenti oggetti:

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

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

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



Schema 3 - Schema delle componenti logiche del SdC

9.2 Componenti Tecnologiche

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

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

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

9.3 Componenti Fisiche

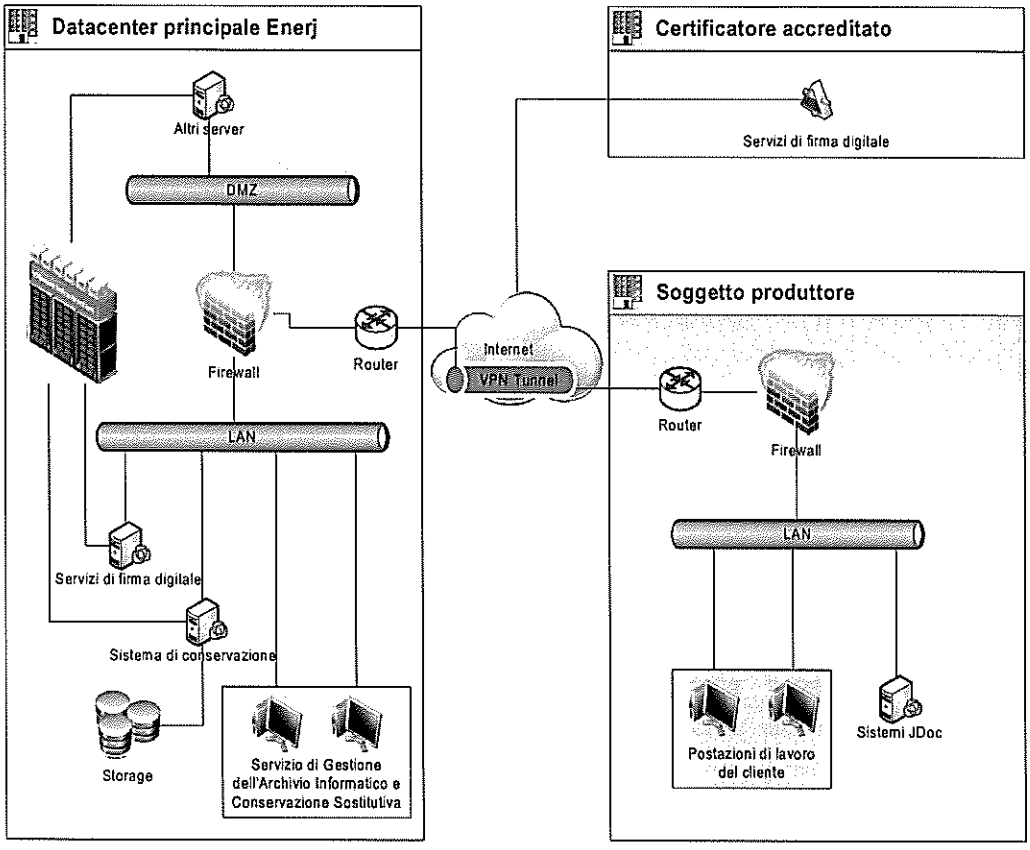
Le componenti fisiche utilizzate nell'infrastruttura di Enerj sono definite e descritte nel dettaglio nei seguenti documenti afferenti al ISMS:

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

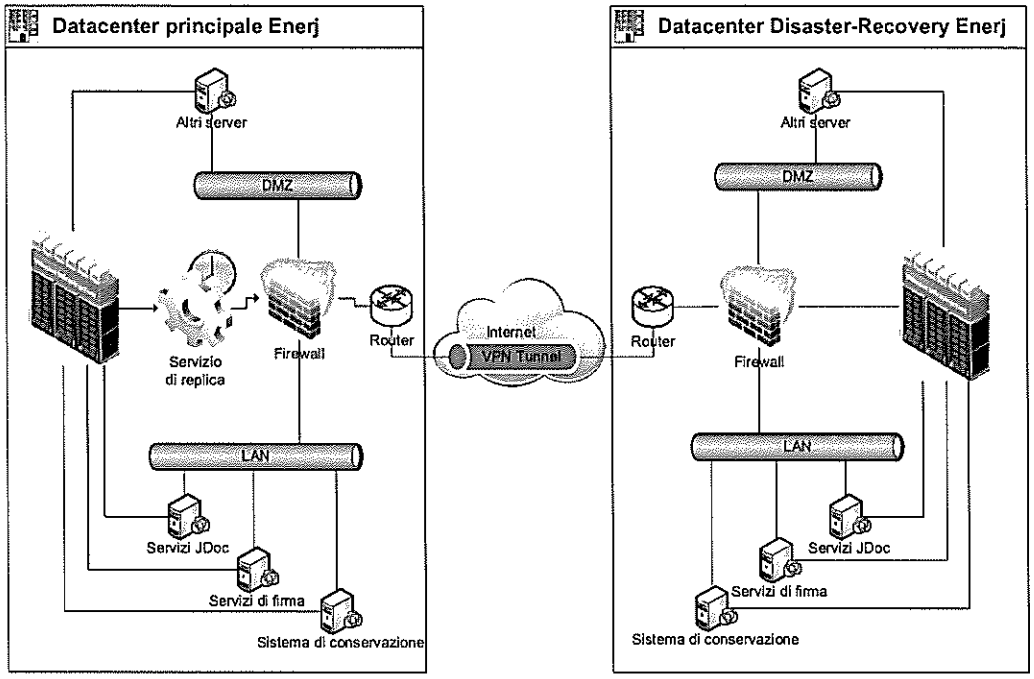
Il SdC si compone di due siti: uno primario situato presso la sede di Enerj ed uno secondario presso il sito di Disaster Recovery. I due datacenter sono connessi mediante una connessione sicura (VPN).

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

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



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



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

9.4 Procedure di gestione e di evoluzione

9.4.1 Conduzione e manutenzione del sistema di conservazione

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

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

9.4.2 Gestione e conservazione dei log

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

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

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

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

9.4.3 Change management

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

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

9.4.4 Verifica periodica di conformità a normativa e standard di riferimento

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

Torna al sommario

10 MONITORAGGIO E CONTROLLI

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

10.1 Procedure di monitoraggio applicativo

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

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

10.2 Procedure di monitoraggio infrastrutturale

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

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

10.3 Verifica dell'integrità degli archivi

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

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

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

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

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

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

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

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

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

informazioni di sicurezza.

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

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

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

10.4 Soluzioni adottate in caso di anomalie

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

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

10.5 Sicurezza del SdC

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

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

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

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