



METRO C S.C.p.A.

**MANUALE DI GESTIONE
DOCUMENTALE**

Rev. 0



INDICE

1. SCOPO E CAMPO DI APPLICAZIONE	3
2. ACRONIMI E DEFINIZIONI	3
3. FONTI NORMATIVE	4
4. RUOLI E RESPONSABILITA'	5
5. MODELLO ORGANIZZATIVO	6
6. DESCRIZIONE DEI PROCESSI	7
7. FLOW CHART	17
8. ALLEGATI	18

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Manuale descrive il sistema di produzione e gestione dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali, degli archivi e della conservazione elettronica.

L'obiettivo fondamentale del Manuale è quello di disciplinare le attività di creazione, acquisizione, registrazione, classificazione e archiviazione dei documenti informatici al fine perseguire la massima reperibilità possibile e la trasparenza dei documenti considerati giuridicamente rilevanti.

A tale riguardo, il presente Manuale di gestione documentale descrive il sistema di gestione informatica dei documenti di Metro C sotto diversi profili:

- organizzativo: mediante la previsione delle modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici, l'individuazione dei ruoli e delle funzioni coinvolte con l'indicazione delle regole e dei criteri di assegnazione dei documenti ricevuti;
- documentale: individuando i formati utilizzati per la formazione del documento informatico e le procedure di riversamento;
- di protocollo informatico: riportando le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione, di utilizzo e tenuta del registro di emergenza;
- di assegnazione e classificazione: portante le modalità di aggiornamento.

Il Manuale riporta pertanto il processo di produzione e gestione dei documenti informatici che, in ossequio alla normativa vigente, costituisce un preciso obbligo normativo per le sole Pubbliche Amministrazioni ma a cui Metro C (d'ora in poi "la Società") ha inteso aderire su base volontaria, del tutto facoltativamente, in ottica di massima trasparenza, efficienza e tutela dell'attività aziendale.

Si precisa, infine, che nella medesima ottica, il servizio di Conservazione sostitutiva è affidato ad un outsourcer.

2. ACRONIMI E DEFINIZIONI

2.1. Acronimi

RGD = Responsabile della Gestione Documentale

RSC = Responsabile del Servizio di Conservazione

RSI = Responsabile Sistemi Informativi

DPO = Data Protection Officer

IDM = Integra Document Management (outsourcer responsabile della Conservazione dei documenti)

PA = Pubblica Amministrazione

B2B = Business to business

CAD = Codice dell'Amministrazione Digitale

PCM = Piattaforma Controllo e Monitoraggio

AD = Amministratore delegato

DT = Direttore Tecnico

SIP = Pacchetto di versamento informatico

AIP = Pacchetto di archiviazione

DIP = Pacchetto di distribuzione

2.2. Definizioni

Processo: insieme di attività correlate o interagenti che trasformano elementi in entrata in elementi di uscita.

Conservazione Elettronica Sostitutiva: la conservazione digitale di documenti originariamente analogici.

Manuale di Conservazione: strumento descrittivo del sistema di conservazione dei documenti informatici, adottato ai sensi dell'art. 9 del DPCM 3 dicembre 2013.

Manuale di Gestione: strumento descrittivo del sistema di gestione informatica dei documenti.

Scarto: operazione attraverso cui vengono eliminati documenti privi di valore amministrativo e legale.

Versamento: operazione attraverso la quale Metro C predispone e inoltra i documenti a **IDM**.

Legal Archive: è il sistema informatico utilizzato da **IDM** per la conservazione dei documenti.

3. FONTI NORMATIVE

- **CAD** (D.Lgs 82/2005, modificato dal D.Lgs 217/2017): Linee guida sulle Conservazione Elettronica, nonché la descrizione dettagliata della disciplina con annessi oneri e diritti.
- **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, art. 2215 bis): Documentazione informatica.
- **Circolare AGID del 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.
- **DPCM 3 dicembre 2013:** Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, comma 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.

- **DPCM 13 novembre 2014:** Regole concernenti la formazione dei documenti informatici, in vigore dall'11 febbraio 2015.
- **Regolamento Generale sulla protezione dei dati UE 679/2016 (GDPR):** Introduzione del diritto sulla portabilità dei dati.
- **D.Lgs. 231/2001:** la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.
- **Legge 241/1990 art. 22:** Documento amministrativo.
- **ISO 14721:2012 OAIS (Open Archival Information System),** Sistema informativo aperto per l'archiviazione.
- **ISO/IEC 27001:2013,** Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).

4. RUOLI E RESPONSABILITA'

Il responsabile interno del processo di creazione, gestione e versamento dei documenti informatici è il **RGD**, coadiuvato nel suo operato dal **RSI** e **DPO**, invero, il **RSC** che è il responsabile del processo di conservazione. In particolare:

- **RGD** ha la responsabilità di:
 - regolare e vigilare il flusso dei documenti e dei dati oggetto di conservazione e la gestione degli stessi;
 - acquisire la documentazione necessaria;
 - predisporre e aggiornare il manuale di gestione dei flussi documentali;
 - rappresentare il referente interno per l'outsourcer (IDM);
 - gestire il processo di versamento dei SIP.
- **RSC** deve:
 - definire le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali;
 - gestire il processo di conservazione e garantire nel tempo la conformità alla normativa vigente;
 - generare e sottoscrivere il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
 - generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

- effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adottare misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adottare inoltre analoghe misure con riguardo all'obsolescenza dei formati;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- provvedere alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione.

4.1 Deleghe e Procure

Il **RGD**, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse ad uno o più soggetti, che all'interno della struttura organizzativa, abbiano competenze ed esperienze idonee. La delega deve indicare le specifiche funzioni e competenze delegate.

5. MODELLO ORGANIZZATIVO

5.1 Manuale di Gestione

Il manuale di gestione, i cui obiettivi sono stati riportati nel paragrafo 1, costituisce il modello organizzativo in materia di conservazione digitale da parte di Metro C ed è redatto dal **RGD**, che procede al suo periodico aggiornamento in ottica di razionalizzazione ed efficientamento della prassi, nonché di compliance con la normativa vigente.

È stato nominato **RGD** in data 15 Gennaio 2021 il Sig. Fabio Aresu con lettera di incarico da parte dell'Amministratore Delegato di Metro C, debitamente controfirmata per accettazione.

In linea con quanto previsto dal DPCM 3/2013, il Manuale deve essere reso noto mediante la sua pubblicazione sul sito internet della società, inoltre una copia è inviata per conoscenza all'Agenzia Italiana del Digitale.

5.2 Struttura Organizzativa

Il modello organizzativo di Metro C relativamente al processo di produzione, gestione e conservazione dei documenti informatici prevede i seguenti attori coinvolti e relative attività:

- Ufficio Amministrativo-Finanziario e dei sistemi generali (**URAFP**), responsabile della produzione gestione e archiviazione della documentazione cartacea e digitale.
- Ufficio Protocollo, responsabile della protocollazione dei documenti ufficiali amministrativi, in coordinazione con la Segreteria Direzionale, del Database di Posta In e Out e della PEC. La PO-MC-01: *Gestione corrispondenza e Document Management* definisce dettagliatamente le classi di riservatezza e i soggetti autorizzati alla gestione delle caselle postali, PEC, documenti e

accessi. Ciò nonostante, si può sintetizzare dicendo che la gestione della PEC è effettuata da AD-DT, Ufficio Protocollo (tramite la propria segreteria), la Segreteria Direzione, e l'Ufficio Acquisti (per la sola spedizione) con eccezione del **RGD** per la conservazione elettronica.

- Segreteria Direzionale, responsabile della gestione della corrispondenza cartacea e digitale. Tuttavia, ogni ufficio possiede la propria Segreteria la quale gestisce autonomamente e internamente la corrispondenza di suo interesse.
- **RSI** unico gestore e responsabile dei sistemi informativi interni della società e degli accessi.
- **DPO** che osserva il rispetto sulla normativa del trattamento dei dati personali, privacy e sicurezza.
- Responsabile della gestione documentale che definisce e assicura criteri uniformi del trattamento del documento informatico e in particolare di classificazione e archiviazione nonché di comunicazione interna tra le aree organizzative coinvolte, si occupa di acquisire i documenti cartacei e digitali prodotti dal **URAFP** e procedere alla sua classificazione e archiviazione in ottica della conservazione elettronica.
- **RSC** che Metro C ha optato per esternalizzare alla società **IDM**, tuttavia all'interno della società è stato nominato un **RGD** il quale collabora con il **RSC** per la corretta ed efficiente promozione del processo di conservazione elettronica.

Il modello organizzativo per la gestione dei documenti informatici prevede che **RGD** si coordini, attraverso comunicazioni interne di varia natura, con i responsabili e le segreterie dell'**URAFP** e con l'Ufficio IT per acquisire i documenti digitali da questi ultimi prodotti e archiviati sulla Piattaforma Informatica *Sharepoint*. Questi documenti cartacei e/o digitali devono aver subito già il processo di protocollazione interno, ed eventualmente di trasformazione digitale, dall'ufficio protocollo in coordinamento con la Segreteria Direzionale.

Una volta reperiti i documenti informatici di cui sopra, questi sono archiviati in cartelle specifiche secondo una definita classificazione e fascicolazione da parte dello **RGD**, supportato dal **RSI** e dal **DPO**, in maniera che si possa procedere con la fase di conservazione con il supporto del **RSC**.

Questo iter è dettagliatamente descritto nel successivo paragrafo.

6. DESCRIZIONE DEI PROCESSI

Il ciclo di vita del documento informatico è articolato in tre processi:

- **Creazione:** acquisizione di documenti cartacei, informatici e/o telematici o nella creazione degli stessi;
- **Gestione:** dalla registrazione del documento alla classificazione, assegnazione e archiviazione;
- **Conservazione:** trasferimento dei documenti dall'archivio corrente all'archivio di deposito.

6.1. Creazione e Gestione Documentale

Per creazione si intende il processo di produzione dei documenti cartacei ed informatici.

Ogni documento è di fatto l'output di un processo ben preciso che viene dettagliatamente descritto nella sua procedura di riferimento e a cui fa capo uno specifico responsabile **URAFP**. In particolare, le PO-MC-21: *Flussi Amministrativi e gestione della Tesoreria*, PO-MC-31: *Amministrativo-Contabile* ciclo attivo e la PO-MC-33: *Adempimenti fiscali, tributari e previdenziali*, illustrano il processo di produzione cartacea e digitale dei documenti di interesse oggetto del manuale di gestione (paragrafo 6.2.2).

In merito alla gestione dei documenti informatici, come evidenzia la PO-MC-41: *Infrastrutture sistemi Informativi*, Metro C procede al salvataggio e archiviazione dei documenti informatici con cadenza variabile a seconda della significatività dei dati generati. Il **RSI** è l'unico soggetto responsabile della gestione dei sistemi informatici. Per l'archiviazione digitale Metro C prevede l'utilizzo della piattaforma *Sharepoint* nella quale vengono salvati e archiviati, così come descritto dalla PO-MC-25: *Piattaforma Controllo e Monitoraggio*, i documenti informatici prodotti.

Questi ultimi devono successivamente essere acquisiti dal **RGD** il quale procede, sotto la sua responsabilità e con il supporto del **RSI** e **DPO**, alla loro classificazione, registrazione e archiviazione digitale, coerentemente con quanto accordato dall'outsourcer per la conservazione elettronica.

Per la descrizione del processo di acquisizione occorre differenziare il documento originariamente cartaceo da quello informatico.

Nel caso di documenti cartacei, il **RGD** deve:

- accettarsi che sia stato scansionato e protocollato dall'Ufficio competente, il quale deve verificarne la conformità con l'originale;
- verificare la presenza di categorie particolari di dati personali sensibili;
- classificare e archiviare il documento nell'apposita forma richiesta dall'Outsourcer, supportato dall'Ufficio IT.

Nel caso di documenti informatici, il **RGD** deve:

- Accettarsi che sia stato protocollato dall'Ufficio competente;
- Verificare la presenza di dati Sensibili;
- Classificare e archiviare il documento nell'apposita forma richiesta dall'Outsourcer; supportato dall'Ufficio IT.

Al termine di tale processo l'**RGD** si deve accertare che il documento informatico sia in possesso delle seguenti cinque caratteristiche fondamentali:

- staticità, il documento informatico deve essere redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione e non deve contenere macroistruzioni o codice eseguibile tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati;
- integrità;

- immutabilità, attraverso l'apposizione della firma digitale da parte dei responsabili di processo;
- leggibilità;
- autenticità.

Il documento informatico creato è quindi identificato in modo univoco e durevole ed è memorizzato in un sistema di gestione informatica dei documenti. L'art. 3, comma 9, del DPCM 13 novembre 2014 stabilisce, infatti, che *“al documento informatico immutabile vengono associati i metadati che sono stati generati durante la sua formazione”*. I metadati altro non sono che un insieme di dati (informazioni) associati ad un documento informatico o a un fascicolo informatico o ad un'aggregazione documentale informatica al fine di identificare e descrivere: contesto, contenuto e struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

L'art. 9, comma 7, dello stesso DPCM, prevede che i metadati *“minimi”* da associare ad un documento amministrativo informatico di cui all'art. 53 del D.P.R. 28 ottobre 2000 n. 445 sono:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

6.2. Conservazione

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di conservazione che ha lo scopo di assicurare: autenticità, integrità, affidabilità, legalità e reperibilità.

Le modalità di conservazione della documentazione versata dal **RGD** sono descritte in dettaglio nel Manuale del Responsabile di Conservazione (Allegato 1- Allegato E, Manuale di Conservazione di IDM).

6.2.1. Descrizione dei rapporti con l'Outsourcer

La Società Metro C ha affidato, tramite contratto (Allegato 2- Allegato B, Contratto di affidamento del servizio di conservazione di documenti Informatici), alla società **IDM** il compito di conservare in formato elettronico, così come previsto dalla legge, i documenti riportati al paragrafo 6.2.2. Nello specifico **IDM**, in virtù della nomina di **RSC**, ha il compito di:

- produrre tutta la documentazione interna (procedura operativa/manuale) prevista dalla normativa;
- apporre la propria firma digitale e la marca temporale sul pacchetto di archiviazione, necessaria per la corretta tenuta dello stesso;
- mantenere presso di sé copia dell'archivio digitale;
- garantire l'esibizione del **DIP** alla comunità di riferimento, ovvero agli Utenti autorizzati.

Qualora si debbano gestire eventuali anomalie o modificare e/o aggiornare il contratto con **IDM** è responsabilità del **RGD** coordinarsi e contattare **IDM** per risolvere suddette problematiche.

6.2.2. Documenti oggetto del contratto

Metro C ha affidato a **IDM** la conservazione elettronica e/o sostitutiva dei seguenti documenti:

- Libro Giornale;
- Libro Inventari;
- Registro IVA acquisti;
- Registro IVA vendite;
- Riepilogo IVA;
- Fattura Passiva;
- Fattura Attiva;
- Fattura Attiva PA e B2B;
- Registro Corrispettivi.

Ogni documento gode di peculiarità specifiche, si rimanda all'Allegato 2 per la descrizione dettagliata dell'iter della conservazione di ciascun documento.

6.2.3. Modalità di Versamento

Per modalità di versamento si intende il metodo utilizzato da Metro C per inviare i documenti a **IDM** così da poter essere archiviati e conservati da quest'ultimo.

Metro C ha optato per una modalità di tipo **SFTP** per tutti i documenti di cui sopra, eccezione fatta per la Fattura Attiva PA e B2B, per la quale è prevista una gestione automatica attraverso l'Invoice Channel (si rimanda alla PO-MC-68: *Fatturazione elettronica e conservazione sostitutiva*).

Tale modalità prevede che i documenti possono essere versati nel sistema di conservazione mediante protocollo **SFTP** (modalità binaria). Per le specifiche si rimanda all'Allegato 3-Manuale Operativo DB2CSV, che illustra dettagliatamente e tecnicamente tutte le fasi per il versamento del **SIP**.

A titolo esemplificativo, il processo di versamento è così sintetizzato:

Al **RGD** viene assegnata una cartella (Home-SP) in cui è suo compito versare i file da conservare.

A tale scopo è necessario che tutti i file PDF dei documenti siano stati preventivamente depositati, divisi per tipologia, in diverse cartelle e con nomenclatura standardizzata.

Il **RGD** supportato dall'ufficio IT versa i documenti informatici di ciascuna tipologia documentaria nelle omonime cartelle: ad esempio, i file PDF delle fatture attive nella cartella "Fatture Attive", le quali compongono un **SIP** che, una volta completo, viene versato nel sistema dal **RGD**.

Le credenziali per l'accesso alla cartella **SFTP** sono inviate da **IDM** all'indirizzo e-mail: metroc@casellapec.com così da poter essere reperite dal **RGD**

Un pacchetto di versamento (SIP) completo è costituito da:

- Un numero <n> di file (con n>=1);
- Numero 1 indice di conservazione (così come descritto nel paragrafo 6.2.1.).

Ogni attività del **RGD** è soggetta al controllo del **RSI** e **DPO** i quali si accertano del rispetto della prassi con le procedure e la normativa vigente.

6.2.4. Validazione Versamento e Accettazione/ Rifiuto

Il sistema di versamento mette a disposizione di Metro C una serie di funzionalità di validazione che gli consentono, se necessario, di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del conservatore. Il sistema di conservazione prevede la possibilità di eseguire verifiche sulla composizione del pacchetto di versamento, sull'integrità dei file e sull'insieme dei metadati forniti. Le validazioni sono concordate nel contratto di affidamento del servizio di conservazione, tuttavia i diversi tipi di validazione previsti sono:

- Validazioni del pacchetto di versamento: il sistema di conservazione verifica la congruità delle informazioni contenute nell'indice dei metadati con il numero di documenti presenti nel pacchetto di versamento: per superare la validazione il pacchetto di versamento deve contenere tutti i documenti elencati nell'indice di conservazione (Controllo Obbligatorio).
- Validazioni sul singolo documento: il sistema di conservazione permette di verificare che:
 - il mime type del documento in elaborazione appartenga alla lista dei mime type per i quali il sistema conserva i viewer;
 - il mime type di un file corrisponda a quanto dichiarato (Controllo Obbligatorio); o la firma di un file sia valida (impostabile solo nel caso p7m o pdf);
 - la marca temporale di un file sia valida (impostabile solo nel caso tsd o p7m);
 - nel caso in cui il file dei metadati, prodotto e versato da **RGD**, includa anche un campo contenente l'hash di ciascun file, il sottosistema di validazione ricalcola l'hash di ogni documento e lo confronta con quello dell'indice verificando l'integrità del file versato.
- Validazioni sui metadati: il sistema di conservazione definisce per ciascuna descrizione archivistica il set di metadati previsti e oggetto dell'accordo tra SP e conservatore. Per ciascun metadato è possibile configurare:
 - nel campo "Tipo metadato": la tipologia di dato (stringa, numero, data ...);

- nel campo “Espressione di Validazione”: l’espressione regolare con la quale il valore del metadato dovrà coincidere;
- nel campo “Pattern di Conversione”: il tipo di pattern accettato per il tipo di metadato;
- una volta validato il versamento, **IDM** procede all’accettazione del **SIP** rilasciando a Metro C il rapporto di versamento. Questo è un file in formato XML contenente:
 - l’identificativo univoco del rapporto, ovvero l’identificativo univoco del processo che l’ha generato;
 - il riferimento temporale relativo alla sua creazione (specificato con riferimento al tempo UTC);
 - gli identificativi univoci dei documenti versati;
 - gli identificativi univoci dei file versati;
 - le impronte degli oggetti-dati che ne fanno parte;
 - la lista dei metadati versati suddivisi per documento.

Il rapporto di versamento è reso disponibile attraverso un versamento via **SFTP**, ciò implica che è restituito nello stesso folder di input dove Metro C ha trasferito il pacchetto di versamento. Come ulteriore feedback il file di indice viene rinominato con estensione “OK” in caso di processo di conservazione eseguito con successo o in “KO” in caso di processo di conservazione in errore. Nel caso di KO viene fornito tramite mail una notifica dettagliata sul motivo di errore così che il **RGD** tempestivamente procede alla sua rettifica. Nel pacchetto di versamento, archiviato e approvato, deve essere posta la firma digitale da **IDM** così che non possa essere modificato e dunque avere efficacia di legge.

6.2.5 Archiviazione, Distribuzione e Scarto

Il Legal Archive, di proprietà di Ifin Sistemi S.r.l., trasforma i pacchetti di versamento in **AIP** secondo un sistema ben definito nell’Allegato 1. La durata dell’archiviazione digitale deve essere permanente per quei documenti obbligati dalla legge alla conservazione elettronica, invero, cambia a seconda del documento. Nel caso specifico dei documenti che Metro C affida a **IDM** l’archiviazione digitale prevista è di 10 anni per ciascuno, tuttavia si rimanda all’Allegato 2 per i dettagli di ciascun file oggetto della conservazione. La visualizzazione dei documenti è autorizzata solamente ai soggetti definiti “Utenti” i quali possono accedere ad un formato visibile degli **AIP**, noto come pacchetto di distribuzione, le cui caratteristiche tecniche sono consultabili nell’Allegato 1, attraverso delle credenziali rilasciate da **IDM**.

Alla scadenza del termine di conservazione il sistema di archiviazione genera una notifica automatica al **RSC**, il quale, dopo averla notificata alla **RGD**, procede allo scarto dei suddetti pacchetti di archiviazione. **IDM** è altresì dotata di server locali nei quali vengono registrati e archiviati automaticamente, mediante back-up, tutti i documenti ricevuti. Ciò comporta che, nell’eventualità di modifica o cancellazione di pacchetti informatici ottenuti, **IDM** è capace di mantenerli presso i propri server locali per un periodo non superiore a tre mesi.

6.2.6. Visualizzatori Conservazione

I visualizzatori (*viewer*) associati ai formati file rappresentano lo strumento che garantisce nel tempo la leggibilità dell'oggetto digitale conservato. Per soddisfare la normativa vigente in materia di conservazione, nel pacchetto di distribuzione vengono inseriti i *viewer* associati ai file che lo compongono, siano questi documenti principali o loro allegati.

Il sistema di conservazione archivia al proprio interno e mantiene aggiornati i *viewer* indicati in tabella:

Viewer	Formati file accettati associato
Notepad++	File testuali e XML (*. ex, *.xml)
Thunderbird	File di posta elettronica (*.eml)
AdobeReader*	File PDF/A, PDF (*.pdf)
Firefox	File HTML (*.htm, *.html)
7zip	File ZIP, TAR (*.zip, *.tar)
FileProtector	File P7M (*.p7m)
GIMP	File TIFF (*.tiff)

6.2.7. Gestione Accessi Utenti

Sono stati richiesti le creazioni di tre account utenti che possono accedere al sistema di conservazione "Legal Archive". Ogni account è associato ad una singola persona fisica la quale è l'unica autorizzata ad accedere al sistema. Le credenziali non sono cedibili a terzi. Il **RGD** è responsabile della corretta tenuta e gestione dell'accesso degli utenti.

Ogni utente possiede un profilo differente il quale concederà funzionalità specifiche. I tipi di utente sono:

Utente Avanzato	Può effettuare ricerche tra i documenti conservati, richiedere il download dei file relativi e richiedere pacchetti di distribuzione con valore legale. Può caricare documenti nel sistema di conservazione da interfaccia web.
Utente Base con esibizione (Utente predefinito)	Può effettuare ricerche tra i documenti conservati, richiedere il download dei file relativi e richiedere pacchetti di distribuzione con valore legale.
Utente Base senza esibizione	Può effettuare ricerche tra i documenti conservati, richiedere il download dei file relativi. Non può richiedere pacchetti di distribuzione con valore legale.

Nello specifico Metro C prevede due “Utenti Avanzati” ed un “Utente Base”:

- **RGD** (Utente Avanzato);
- Responsabile dell’Ufficio di Amministrazione (Utente Avanzato);
- Responsabile Cespiti dell’Ufficio Acquisti (Utente Base).

È possibile aggiornare e/o modificare l’anagrafica degli utenti in qualsiasi momento. A tal proposito, il **RGD** scarica e modifica il modulo di anagrafica degli utenti autorizzati all’accesso (presente nell’Allegato 1) e lo invia al Legale Rappresentante di Metro C per l’apposizione della firma. Successivamente, questo modulo aggiornato e firmato viene inviato tramite PEC al Rappresentante Commerciale di **IDM** che procede a modificare e/o aggiornare gli utenti e conseguentemente le credenziali di accesso. Nei casi più urgenti, ulteriormente alla PEC è possibile contattare telefonicamente IDM per sollecitare e velocizzare il procedimento.

L’accesso al **DIP** deve essere consentito inoltre alle Autorità di Controllo nel corso delle loro verifiche e ispezioni. L’Autorità di Controllo potrà servirsi di un profilo temporaneo per accedere che deve essere preventivamente richiesto dall’Amministratore Delegato e/o dal **RGD** a **IDM** e da lei prodotto in un arco temporale non eccedente le 24 ore.

6.3 Misure di sicurezza e Trattamento dei dati personali

RGD definisce le misure tecniche e organizzative al fine di assicurare la sicurezza applicativa ed infrastrutturale del protocollo informativo e del sistema gestione documentale. Tali strategie coerenti con la policy di sicurezza della società, sono finalizzate a garantire una corretta gestione dei dati e documenti sensibili.

Coerentemente con suddette policy, Metro C realizza un sistema di misure volte a garantire integrità e disponibilità dei dati (Modello Organizzativo Privacy approvato dal CdA di Metro C in data 23 maggio 2018, che ha sostituito la previgente procedura PO-MC-15: *Documento Programmatico sulla sicurezza e tutela dei dati personali e della privacy*).

Tale attività si fonda su una fitta rete di soggetti interconnessi che procedono sistematicamente alla revisione, aggiornamento, archiviazione e monitoraggio dei documenti trattati. Estrema attenzione viene posta sulla gestione degli accessi ai dati sensibili, sul backup, salvataggio e ripristino dei dati.

Ulteriore aspetto fondamentale sulla compliance della sicurezza è la tutela dei dati personali con implicita gestione del processo di cancellazione e del Data Breach (PO-MC-65: *Portabilità dei dati, cancellazione e Data Breach*).

Così come previsto dal Regolamento generale sulla protezione dei dati personali UE 679/2016 (**GDPR**) nonché dal D. Lgs. n. 196/2003 (**Codice Privacy**), come modificato dal D. Lgs. n. 101/2018 e dal D.Lgs 231/2001, in relazione alla prevenzione di reati incidenti su sistemi e dispositivi informatici, Metro C tutela il diritto dei soggetti interessati ad ottenere i dati personali che li riguardano, con eventuale cancellazione degli stessi ove richiesto e ricorrendone le condizioni di legge.

In caso di violazione dei dati personali (Data Breach), Metro C assicura la notifica all’Autorità Garante per la Protezione dei dati personali entro 72 ore della violazione documentando tutte le violazioni nell’apposito Registro.

Tali controlli sono dettagliati nel Modello Organizzativo Privacy di Metro C sopra citato e, in relazione alle fattispecie qualificabili come reati, nel Modello di Organizzazione, Gestione e di Controllo ex D. Lgs. 231/2001 di Metro C.

6.4 Documento Amministrativo

Per documento amministrativo si intende, ex art. 22 Legge 241/1990, ogni rappresentazione grafica, elettromagnetica o di qualunque altra specie concernenti attività di pubblico interesse indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale.

Tutti i documenti amministrativi di Metro C emessi, così come previsto dalla PG-MC-01 recante il *Controllo dei documenti e delle registrazioni*, vengono identificati mediante una codifica definita dalla “Procedura di codifica degli elaborati di progetto”. Ogni documento emesso deve inoltre riportare in copertina le seguenti fattispecie: nome e firma del responsabile della redazione, verifica e approvazione.

La distribuzione dei suddetti documenti può essere interna o esterna alla società, a supporto cartaceo o digitale. La descrizione della gestione della corrispondenza affidata alla PO-MC-01: *Gestione della corrispondenza/Document Management*, prevede il seguente iter:

- In riferimento alla documentazione cartacea in entrata questa deve essere ricevuta, protocollata, scansionata e inserita nell’archivio digitale della società Piattaforma Controllo e Monitoraggio (**PCM**), la cui gestione in dettaglio è consultabile tramite la PO-MC-25: *Piattaforma Controllo e Monitoraggio*, ad opera dell’Ufficio Protocollo e Segreteria.
- La corrispondenza cartacea in uscita viene protocollata dalla Segreteria, la quale una volta firmata provvede a scansionarla e ad inserirla nella **PCM**. L’ufficio Protocollo invia copia di tutta la corrispondenza in uscita all’**AD-DT** per conoscenza.
- Stesso iter per i documenti digitali con l’esclusione della scansione che non è necessaria.

6.5 Punti di controllo

L’**RGD** deve redigere e tenere aggiornato il presente manuale periodicamente e rivederlo almeno una volta l’anno, secondo quanto regolato dalla normativa e verificare la corretta applicazione dello stesso, controllando la corretta creazione dei documenti e prendendo visione dei rapporti di versamento al sistema di conservazione sostitutiva.

Egli deve, inoltre, supervisionare l’attività del responsabile della conservazione “delegato” e coordinarsi con quest’ultimo e con tutti gli altri responsabili coinvolti nei processi documentali, come ad esempio il **DPO** nel caso in cui i documenti contengano dati personali.

Le verifiche sono svolte mensilmente a campione dal **RGD** il quale procederà nel redigere un report contenente le conclusioni su tali verifiche. Inoltre, L’**RGD** verifica a campione periodicamente il corretto inserimento dei documenti sullo *Sharepoint*.

Nello specifico svolge dei controlli a campione sui documenti caricati dagli uffici competenti come ad esempio:

- I file PDF presenti nelle cartelle di tutte le categorie ad eccezione delle Fatture Attive, Passive e Libri Inventari devono avere all'inizio del nome il numero del mese di riferimento (da 1 per gennaio a 12 per dicembre) seguito da uno spazio;
- Per le Fatture Attive e Passive il nome del file deve corrispondere al numero univoco della fattura.
- Per tutte le categorie (ad eccezione delle Fatture Attive e Passive) è necessario compilare il campo "Anno di riferimento" che di default propone l'anno corrente.

6.6 Registro Delle Emergenze

Nel caso di interruzione del funzionamento della rete internet, sarà attivata la procedura di emergenza mediante ricorso al Registro di Protocollo di Emergenza. Ogni Responsabile dell'Ufficio competente è incaricato della registrazione manuale del documento di pertinenza che ad emergenza cessata verrà digitalizzato con lo stesso procedimento descritto nel paragrafo 6.1. Per attivare il Registro di Protocollo di Emergenza si deve verificare almeno una delle seguenti condizioni:

- guasto al software di protocollazione informatica;
- guasto al sistema informatico di gestione;
- mancanza di energia elettrica.

Inoltre, il RGD dovrà:

- redigere il verbale di attivazione;
- comunicare al responsabile della propria "struttura" l'attivazione del Protocollo di Emergenza.

Sul Protocollo di Emergenza dovranno essere riportate le seguenti informazioni necessarie:

- numero progressivo di Protocollo di Emergenza;
- data di protocollazione;
- tipo di protocollo;
- oggetto;
- mittente / destinatario;
- classificazione del documento;
- numero di riferimento del documento;
- data di riferimento del documento;
- numero eventuali allegati.

Potranno inoltre essere riportate le seguenti informazioni accessorie:

- eventuali note;
- tipo di documento.

A ciascun documento registrato in emergenza dall'Ufficio viene attribuito, per ciascun anno solare, un numero progressivo a partire dal numero 1, e a seguire dall'acronimo del Responsabile dell'Ufficio da cui è stato prodotto.

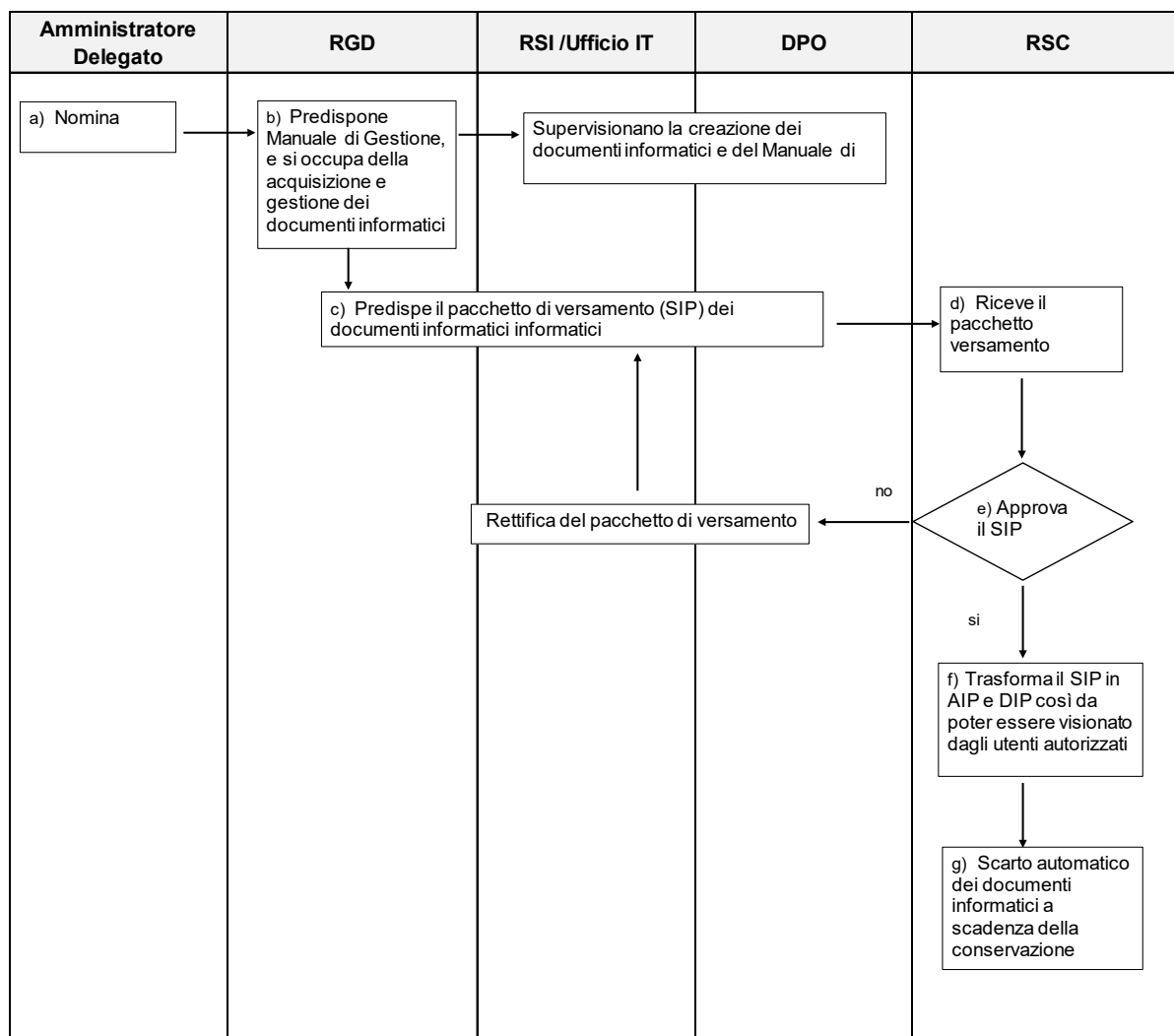
Al termine dell'emergenza, l'RDG deve:

- revocare l'autorizzazione al Protocollo di Emergenza;
- comunicare la revoca del Protocollo di Emergenza.

Una volta riattivato il sistema informatico, l'Ufficio Protocollo procede alla protocollazione dei documenti sul sistema informatico ordinario il quale provvederà a mantenere stabilmente la correlazione con il numero di protocollo utilizzato in emergenza.

È possibile conservare in formato digitale il Registro di Protocollo di Emergenza presso IDM.

7. FLOW CHART



8. ALLEGATI

Alla presente Procedura si allegano i seguenti documenti:

Allegato 1 – Allegato E, Manuale di Conservazione di IDM;

Allegato 2 – Allegato B, Contratto di affidamento del servizio di conservazione di documenti Informatici;

Allegato 3 – Manuale Operativo DB2CSV.