

# Manuale di Gestione Documentale

Approvato con Determinazione del Presidente  
n. 27 del 21 dicembre 2021

## Indice

1.	GENERALITÀ.....	3
1.1	Manuale di gestione documentale .....	3
1.2	Politiche di gestione, archiviazione e conservazione documentale .....	4
1.3	Politiche di sicurezza.....	4
1.4	Principali norme di riferimento.....	4
1.5	Area organizzativa omogenea e Unità organizzative responsabili.....	5
1.6	Accreditamento all'IPA e Domicilio Digitale .....	5
1.7	Responsabile della gestione documentale.....	6
2.	GESTIONE DOCUMENTALE .....	8
2.1	Tipologie di documenti .....	8
2.1.1	Documento informatico e documento amministrativo informatico.....	8
2.1.2	Documento analogico .....	10
2.2	Formazione dei documenti informatici .....	11
2.2.1	Premessa .....	11
2.2.2	Modalità di formazione del documento informatico.....	12
2.2.3	Metadati.....	13
2.2.4	Formato file .....	14
2.2.5	Validazione temporale .....	15
2.2.6	Firma e assegnazione firma .....	16
2.2.7	Distinzione dei documenti in base allo stato di trasmissione.....	17
2.3	Fascicolo .....	17
2.3.1	Definizione e funzione .....	17
2.3.2	Formazione, implementazione e gestione.....	18
2.4	Piani di classificazione e di conservazione.....	18
2.4.1	Piano di classificazione .....	18
2.4.2	Piano di conservazione.....	20
2.4.3	Procedure di scarto.....	20
2.4.4	Modifiche al piano di classificazione e al piano di conservazione.....	21
3.	PROTOCOLLO INFORMATICO .....	22
3.1	Regole e modalità di protocollazione .....	22
3.1.1	Registrazione di protocollo .....	22
3.1.2	Registrazione di protocollo differito .....	23
3.1.3	Conservazione delle registrazioni.....	24
3.1.4	Segnatura.....	24
3.1.5	Scansione .....	25
3.1.6	Classificazione.....	26

3.1.7	Assegnazione .....	26
3.1.8	Rigetto .....	27
3.1.9	Smistamento.....	27
3.1.10	Annullamento di protocollo .....	27
3.1.11	Documenti soggetti a registrazione particolare .....	29
3.1.12	Documenti esclusi dalla registrazione .....	31
3.2	Registri e Repertori di protocollo .....	31
3.2.1	Registro di protocollo .....	31
3.2.2	Registro di emergenza .....	32
3.2.3	Registri particolari di protocollo .....	33
3.2.4	Repertori .....	34
3.3	Sistema informatico di protocollazione (Docway) .....	38
3.3.1	Sistema di protocollazione di Agenzia delle entrate-Riscossione .....	38
3.3.2	Sistemi di protocollazione delle entità pregresse confluite nell'Ente .....	40
4.	FLUSSI DOCUMENTALI .....	41
4.1	Descrizione dei flussi documentali .....	41
4.2	Flussi documentali in entrata.....	42
4.2.1	Descrizione del flusso di lavorazione dei documenti in entrata .....	43
4.2.2	Modalità operative di registrazione sul sistema di protocollo.....	48
4.3	Flussi documentali in uscita .....	49
4.4	Flussi documentali interni alla AOO .....	52
5.	SISTEMA DI GESTIONE DOCUMENTALE .....	54
5.1	Componenti del sistema di gestione documentale.....	54
5.2	Archivi analogici.....	58
5.2.1	Premessa.....	58
5.2.2	Archivi correnti.....	58
5.2.3	Archivio di deposito e storico .....	59
6.	PIANO DELLA SICUREZZA .....	61
6.1	Premessa .....	61
6.2	Principali misure organizzative di sicurezza .....	61
6.3	Principali misure tecniche di sicurezza .....	62
6.4	Normativa interna.....	64
7.	STORICIZZAZIONE DEL DOCUMENTO .....	66

### 1. GENERALITÀ

#### 1.1 Manuale di gestione documentale

L'Agenzia per l'Italia Digitale (di seguito AgiD) ha pubblicato le nuove Linee Guida sulla Formazione, Gestione e Conservazione del Documento Informatico (di seguito Linee Guida). Le suddette Linee Guida sono state emanate il 9 settembre 2020 e si applicano ai soggetti indicati nell'Art. 2, commi 2 e 3, del Codice dell'Amministrazione Digitale (CAD) prescrivendo, per tali soggetti, la redazione del Manuale di Gestione Documentale. Le Linee Guida sono state modificate da AgiD il 17 maggio 2021, posticipando anche la data di entrata in vigore delle stesse, precedentemente fissata al 7 giugno 2021, al 1° gennaio 2022.

Il presente Manuale - conformemente a quanto disciplinato al punto 3.5 delle Linee Guida - **“descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi”** per Agenzia delle entrate-Riscossione.

Il Manuale costituisce regolamentazione interna di Agenzia delle entrate-Riscossione (di seguito anche “Ente” o “AdeR”) ed è fatto obbligo a tutti i dipendenti e ai collaboratori dell'Ente di attenersi alle disposizioni contenute nello stesso. Inoltre, ai sensi del par. 3.5 delle Linee Guida, lo stesso viene pubblicato nella sezione “Amministrazione Trasparente” del sito istituzionale dell'Ente.

Gli **Allegati**, che costituiscono parte integrante del Manuale, sono i seguenti:

- Allegato 1) Definizioni;
- Allegato 2) Elenco UOR;
- Allegato 3) Elenco Metadati;
- Allegato 4) Piano di classificazione;
- Allegato 5) Piano di conservazione;
- Allegato 6) Format Registro d'emergenza.

**Il Manuale può essere aggiornato, su proposta del Responsabile della gestione documentale, con provvedimento del Responsabile dell'Area Innovazione e Servizi Operativi, qualora gli aggiornamenti da apportare interessino i soli Allegati.** È inoltre funzionalmente connesso al presente Manuale il **Manuale di conservazione**, di cui al par. 4.6 delle Linee Guida Agid, che illustra il sistema di conservazione dei documenti informatici dell'Ente.

### 1.2 Politiche di gestione, archiviazione e conservazione documentale

L'Ente adotta politiche di gestione e conservazione dei documenti coerenti con la normativa vigente e in particolare, con le Linee Guida, il CAD ed il Codice dei Beni Culturali.

La gestione e la conservazione hanno come obiettivo la tutela dei documenti nel loro valore giuridico-probatorio mantenendone nel tempo l'integrità e l'affidabilità.

Al fine di assicurare l'efficace attuazione delle politiche, l'Ente assicura la formazione e l'aggiornamento professionale al personale coinvolto nei processi di gestione documentale, con riferimento alle regole e agli strumenti informatici adottati per la gestione dei documenti e ai processi operativi dell'Ente.

### 1.3 Politiche di sicurezza

L'Ente adotta politiche di Sicurezza che tengono conto delle minacce alla stessa e della relativa evoluzione, in linea con la normativa vigente, anche in tema di protezione dei dati personali, e con le specifiche raccomandazioni, segnalazioni e Linee Guida pubblicate dall'AGID.

Più precisamente, l'Ente promuove le iniziative finalizzate al continuo miglioramento relative a:

- valutazione dei rischi;
- definizione e applicazione di adeguati piani di difesa;
- attivazioni di strumenti tecnici ed organizzativi su tutta la filiera;
- monitoraggio e aggiornamento costante di processi, procedure, prassi e strumenti;
- informazione e formazione del personale.

### 1.4 Principali norme di riferimento

- **Decreto legislativo 7 marzo 2005, n. 82:** Codice dell'amministrazione digitale;
- **Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445:** Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- **Decreto legislativo 22 gennaio 2004, n. 42:** Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137;
- **Decreto del Presidente della Repubblica 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;

- **DPCM 22 febbraio 2013:** Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del Codice dell'amministrazione digitale;
- **DPCM 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, per quanto applicabile a seguito delle abrogazioni introdotte dalle Linee Guida AGID del 9 settembre 2020;
- Regolamento Europeo n. 910/2014: in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS);
- Regolamento Europeo n. 679/2016 (GDPR): protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Linee Guida Agenzia per l'Italia Digitale del 9 settembre 2020 (aggiornate il 17 maggio 2021) sulla formazione, gestione e conservazione dei documenti informatici.

### 1.5 Area organizzativa omogenea e Unità organizzative responsabili

L'Area Organizzativa Omogenea (AOO) è l'insieme delle strutture di una amministrazione che usufruiscono in modo omogeneo e coordinato di servizi informatici comuni per la gestione dei flussi documentali. **Agenzia delle entrate-Riscossione è articolata in un'unica Area Organizzativa Omogenea (AOO).**

Le Unità Organizzative Responsabili (UOR) sono costituite, all'interno della AOO, dalle strutture organizzative dell'Ente che, in relazione alle competenze funzionali assegnate, assumono la responsabilità nella trattazione dei documenti riferiti alle attività e ai procedimenti amministrativi di competenza.

L'elenco delle UOR dell'Ente è riportato all'**Allegato 2**.

### 1.6 Accreditamento all'IPA e Domicilio Digitale

L'Ente è censito, ai sensi di legge, nell'Indice delle Pubbliche Amministrazioni (IPA).

Per l'unica AOO dell'Ente sono pubblicate le diverse Strutture (Direzioni Centrali, Aree e relative Direzioni, Reti Territoriali e Direzioni Regionali) unitamente alle altre informazioni richieste, dal Portale delle Pubbliche Amministrazioni (IPA).

L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet - [indicepa.gov.it](http://indicepa.gov.it) - da parte di tutti i soggetti pubblici o privati.

L'Ente comunica tempestivamente all'IPA ogni successiva modifica intervenuta.

L'Ente è dotato di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'indice delle Pubbliche Amministrazioni (IPA): [protocollo@pec.agenziariscossione.gov.it](mailto:protocollo@pec.agenziariscossione.gov.it). Tale casella costituisce il domicilio digitale dell'Ente. Ai sensi di legge è inoltre pubblicata su IPA la PEC dedicata alla fatturazione elettronica ([fatturazioneelettronica@pec.agenziariscossione.gov.it](mailto:fatturazioneelettronica@pec.agenziariscossione.gov.it)).

### 1.7 Responsabile della gestione documentale

L'Ente nomina il Responsabile della gestione documentale a cui è assegnato il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del DPR n. 445/2000. Il Responsabile si avvale delle strutture organizzative dell'Ente preposte alla gestione documentale e del protocollo (Settore Gestione Documentale e Protocollo, nell'ambito della Direzione Produzione Ruoli e Gestione Documentale).

Il Settore Gestione Documentale e Protocollo governa, a livello di Ente, le attività di gestione e conservazione documentale e di protocollazione, assicurandone l'indirizzo, il coordinamento e il monitoraggio e definendone regole, processi e strumenti.

In particolare, il Responsabile della gestione documentale, conformemente a quanto contemplato al par. 3.4 delle Linee Guida:

- garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi, incluse le funzionalità di accesso e le attività di gestione degli archivi anche in relazione alla selezione e allo scarto;
- vigila sull'osservanza della normativa;
- predispone ed aggiorna il presente Manuale, d'intesa con il Responsabile della conservazione, il Responsabile della transizione digitale e acquisito il parere del Responsabile della protezione dei dati personali (ai sensi del par. 3.4 delle Linee Guida);
- garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgono nel rispetto della normativa vigente;

- garantisce la corretta produzione del registro giornaliero di protocollo e l'invio dello stesso in conservazione;
- autorizza le operazioni di annullamento delle registrazioni di protocollo, ai sensi di legge. Inoltre, il Responsabile della gestione documentale presidia:
  - l'aggiornamento del Piano di Conservazione, allegato al presente Manuale, per l'avvio dei processi di selezione finalizzati allo scarto dei documenti e per il riversamento in conservazione di quelli informatici;
  - il trasferimento periodico (almeno annuale) nell'archivio di deposito dell'Ente dei documenti analogici (dei relativi fascicoli e serie) relativi ai procedimenti amministrativi conclusi;
  - il controllo della movimentazione dei documenti analogici e dei relativi fascicoli;
  - il versamento nella sezione d'archivio dei documenti analogici (e relativi fascicoli e serie) destinate alla conservazione permanente secondo l'ordine originario assunto nella fase di formazione;
  - la predisposizione e l'invio dei pacchetti di versamento dei documenti informatici nel sistema di conservazione.

Tutte le attività in ambito gestione documentale sono svolte in coordinamento con il Responsabile della conservazione (cfr. par. 4.5 delle Linee Guida Agid), con il Responsabile per la Transizione Digitale, con il Responsabile per la Protezione dei Dati personali e con il supporto delle altre figure/strutture dell'Ente (in particolare con la Direzione Tecnologie e Innovazione, per l'implementazione e la gestione degli strumenti a supporto, e con la Direzione Organizzazione e Processi per la definizione dei processi e delle regole da applicare).

## 2. GESTIONE DOCUMENTALE

### 2.1 Tipologie di documenti

#### 2.1.1 Documento informatico e documento amministrativo informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento amministrativo informatico è ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa.

L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono valutabili in giudizio tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Il documento informatico assume la caratteristica di immodificabilità se prodotto in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Il documento informatico può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale: il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme vigenti.

L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione; tuttavia le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Tali considerazioni si estendono al documento amministrativo informatico, fermo restando che le caratteristiche di integrità ed immodificabilità sono garantite anche mediante la registrazione nel protocollo informatico dell'Ente e negli ulteriori registri particolari.

I messaggi di posta elettronica certificata costituiscono di per sé un documento informatico, oltre che un mezzo di scambio di comunicazioni e documenti, in quanto la

relativa trasmissione/ricezione è giuridicamente rilevante e permette di avere prova opponibile dell'invio e della consegna del messaggio di posta.

**Il messaggio e gli allegati trasmessi/ricevuti con PEC assumono lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente, tra l'altro, di ricorrere contro terzi.**

La PEC, a differenza della posta elettronica semplice, ha le seguenti peculiarità:

- identificazione del mittente;
- garanzia dell'integrità e della riservatezza dei messaggi;
- data certa di spedizione e consegna dei messaggi;
- ricevuta di avvenuta consegna o avviso di mancato recapito;
- tracciatura dei messaggi a cura del gestore.

Il **duplicato del documento informatico** è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti. Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originali (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un pubblico ufficiale a ciò autorizzato.

La **copia di documento informatico** è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente.

La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico.

Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta fermo l'obbligo di conservazione dell'originale informatico.

La **copia su supporto informatico di documenti analogici** può essere costituita da:

- copia informatica di documento analogico, avente contenuto identico a quello del documento analogico ma forma diversa;
- copia per immagine su supporto informatico di documento analogico, avente contenuto e forma identici all'originale.

Entrambe le tipologie di documento hanno la medesima efficacia probatoria degli originali analogici solo se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico prodotta secondo le regole tecniche.

I file delle immagini dei documenti analogici, prodotti mediante scansione e archiviati sui sistemi informatici dell'Ente, non assumono quindi la medesima efficacia probatoria dell'originale; rimangono quindi fermi gli obblighi di gestione e di conservazione previsti dalla normativa dei documenti analogici originali.

### 2.1.2 Documento analogico

Il **documento analogico** è la rappresentazione non informatica, di atti, fatti o dati giuridicamente rilevanti. Qualsiasi documento non informatico (ad es., un documento cartaceo) è, dunque, un documento analogico.

Per **documenti analogici originali unici** si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta.

Ai sensi delle norme vigenti, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un pubblico ufficiale a ciò autorizzato.

Pertanto, tutti i documenti cartacei su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa, sono documenti analogici.

Il **duplicato** di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali.

La **copia** di un documento analogico è la trascrizione o riproduzione dell'originale. Si distingue in copia semplice, imitativa e conforme. La copia semplice è la pura trascrizione dell'originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia).

La copia conforme è la copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica").

La **copia analogica di documento informatico** è, di norma, la stampa cartacea dello stesso. La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata o qualificata, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale in tutte le sue componenti da un pubblico ufficiale ovvero deve riportare, apposto a stampa, un contrassegno, ai sensi dell'art. 23 co. 2-bis del CAD.

Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

## 2.2 Formazione dei documenti informatici

### 2.2.1 Premessa

I documenti sono di norma generati in formato informatico, sottoscritti con firma digitale e protocollati nel sistema di protocollo dell'Ente.

L'Ente può generare in modalità analogica documenti, sia esattoriali che non esattoriali, **limitatamente** ai casi per i quali sia necessario adottare tale modalità in relazione alla normativa di riferimento, all'assenza di indirizzo PEC del destinatario o al caso in cui i destinatari, per determinati processi, prevedano esclusivamente la ricezione di documenti in formato analogico (es. notifica a mezzo posta o messo, produzione e consegna allo sportello, ecc.), fino all'implementazione di un sistema di produzione di documenti analogici quali copie conformi di originali di documenti informatici.

Il documento informatico (come peraltro quello analogico, salvo standard specifici, deve, in genere, recare:

- la denominazione e il logo dell'Ente;
- l'indicazione completa della struttura che ha prodotto il documento;
- l'indirizzo completo dell'Ente (via, numero, CAP, città, provincia);
- il numero di telefono della struttura;
- il codice fiscale/p.iva dell'Ente;
- il luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo (sistema di protocollo Docway o registri particolari);

- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento informatico, sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento analogico, sottoscrizione autografa del RPA e/o responsabile del provvedimento finale;
- informazioni complete sul destinatario (nome, cognome, sede legale, C.F. se disponibile, ecc...).

I modelli di riferimento delle principali tipologie di documenti sono presenti sulla intranet dell'Ente.

### 2.2.2 Modalità di formazione del documento informatico

Il documento informatico è formato mediante una delle seguenti modalità:

- **redazione tramite l'utilizzo di appositi strumenti software:** in tal caso il documento informatico assume le caratteristiche di immodificabilità e di integrità con la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con il versamento ad un sistema di conservazione; in caso di formazione attraverso strumenti Office (es. word) il file va prodotto in formato PDF/A per la sottoscrizione con firma digitale;
- **acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- **registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;

- **generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica:** in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

I dati/file prodotti con modalità automatizzata o manuale se privi dei requisiti di immodificabilità, di integrità e di identificazione in modo univoco e persistente (sempre che gli stessi non siano attribuiti ad esempio mediante invio tramite PEC e/o sottoscrizione digitale) **non costituiscono documenti informatici**. In tale tipologia possono essere ricompresi i dati/file inviati tramite sistemi di trasferimento automatico di dati (cooperazione applicativa, web services, applicazioni web, ecc.), laddove non rispettino i requisiti indicati.

### 2.2.3 Metadati

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi "metadati", secondo quanto richiesto dalle Linee Guida.

I metadati costituiscono i dati associati ai documenti, che ne descrivono il contesto, il contenuto e la struttura, così da permetterne la gestione nel tempo in conformità a quanto definito dalla norma. Gli obiettivi fondamentali dei metadati sono:

- garantire l'identificazione permanente dei singoli oggetti informativi, ad es.: identificativo univoco (numero di protocollo, data, autore, ecc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi, ad es.: indici di classificazione;
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi, ad es.: procedimento amministrativo cui il documento è connesso.

In prima istanza i metadati possono essere suddivisi nelle seguenti macrocategorie:

- **Descrittiva:** ha lo scopo di facilitare il recupero e l'identificazione dell'oggetto digitale;
- **Gestionale:** ha lo scopo di supportare la gestione dell'oggetto digitale all'interno di una collezione;
- **Strutturale:** ha lo scopo di collegare fra loro i componenti di oggetti informativi complessi.

Peraltro, il documento una volta formato avrà un suo percorso di esistenza che lo porterà ad essere gestito da diversi sistemi e applicazioni con la contestuale produzione e associazione di ulteriori informazioni.

Un altro aspetto da tenere in considerazione, dunque, è che i metadati non vengono attribuiti ai documenti e in generale agli oggetti digitali tutti nel medesimo tempo, ma **tendono ad accumularsi nel corso della vita degli stessi per tracciarne l'utilizzo**, ad esempio gli accessi, le modifiche, i trasferimenti, le copie, nonché le modalità della sua conservazione.

In **Allegato 3** è riportata l'elenco con il dettaglio dei Metadati previsti dalla normativa vigente.

### 2.2.4 Formato file

Il presente paragrafo fornisce indicazioni sui Formati File accettati e gestiti dall'Ente. I formati descritti, coerentemente ai requisiti definiti dalla normativa vigente, sono stati scelti fra quelli che possono maggiormente garantire il principio di interoperabilità fra i sistemi di gestione documentale e conservazione privilegiando, fra le diverse opportunità, quelli già approvati dagli organismi di standardizzazione internazionale quali ISO e ETSI.

Ciò premesso, dal punto di vista tecnico, le scelte sono state effettuate valutando le seguenti caratteristiche:

- Apertura;
- Sicurezza;
- Portabilità;
- Funzionalità;
- Supporto allo sviluppo;
- Diffusione.

#### **Di seguito si riporta l'elenco dei formati gestiti dall'Ente:**

- **PDF - PDF/A:** Il PDF è stato concepito per rappresentare documenti complessi in modo indipendente dalle caratteristiche dell'ambiente di elaborazione del documento. Un documento PDF può essere firmato digitalmente attraverso il formato ETSI PAdES o CAdES. Il formato è stato ampliato in una serie di sotto-formati tra cui il PDF/A. Il PDF/A è stato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali;

- **TIFF:** di questo formato vi sono diverse versioni, con specifiche pubbliche e non soggette ad alcuna forma di limitazione. Il formato è utilizzato per la conversione in digitale di documenti cartacei;
- **JPG:** tale formato è il più utilizzato per la memorizzazione di fotografie ed è quello più comune su World Wide Web e consente, inoltre, di associare metadati ad un'immagine;
- **Office Open XML (OOXML):** il formato dispone di alcune caratteristiche che lo rendono adatto alla conservazione nel lungo periodo, tra queste l'embedding dei font, la presenza di indicazioni di presentazione del documento, la possibilità di applicare al documento la firma digitale XML. I metadati associabili ad un documento che adotta tale formato sono previsti dallo standard ISO 29500:2008;
- **Open Document Format (ODF):** il formato è uno standard aperto, basato sul linguaggio XML, per la memorizzazione di documenti;
- **Extensible Markup Language (XML):** (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi;
- **TXT:** ai fini della conservazione nell'uso di tale formato, è importante specificare la codifica del carattere adottata;
- **Formati Messaggi di posta elettronica:** ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME. Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui ai precedenti paragrafi.

### 2.2.5 Validazione temporale

I requisiti di immodificabilità e di integrità del documento informatico possono essere assicurati anche con l'apposizione di una validazione temporale:

- realizzata dai certificatori accreditati mediante marche temporali (inclusa la marcatura postale elettronica);
- contenuta nella segnatura di protocollo;
- ottenuta attraverso la procedura di conservazione dei documenti;
- ottenuta attraverso l'utilizzo di posta elettronica certificata.

## 2.2.6 Firma e assegnazione firma

I requisiti di immodificabilità e di integrità del documento informatico possono essere assicurati anche con l'apposizione di una firma elettronica qualificata, di una firma digitale o firma elettronica avanzata, ai sensi del par. 2.1.1 delle Linee Guida.

La sottoscrizione dei documenti informatici prodotti dall'Ente è apposta con un processo di **firma elettronica digitale (qualificata)**, in conformità alle disposizioni dettate dalla normativa vigente.

La firma **digitale** è un particolare tipo di firma elettronica avanzata e qualificata (ai sensi del Regolamento Europeo eIDAS) basata su un certificato qualificato e realizzata mediante un dispositivo sicuro di firma (token, usb, smart card, usb, hsm) con un sistema di chiavi asimmetriche a coppia (una pubblica ed 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 del documento informatico. La firma digitale può essere utilizzata anche in modalità remota e/o automatica.

Il CAD stabilisce anche che "l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria", prevedendo quindi l'onere probatorio a carico del titolare del dispositivo di firma per l'eventuale disconoscimento della stessa.

La firma digitale viene assegnata ai dipendenti dell'Ente, secondo i criteri di attribuzione definiti, in relazione alle responsabilità assegnate, e secondo le procedure di ciascuna certification authority (CA), previo riconoscimento del titolare anche tramite delegati interni all'Ente da parte delle certification authority (Circolare ADER n. 60 – GESTIONE DELLA FIRMA DIGITALE).

La tabella che segue riepiloga i formati gestiti con firma digitale:

<b>CADES</b>	<b>PAdES</b>	<b>XAdES</b>
CMS Advanced Electronic Signature	PDF Advanced Electronic Signature	XML Advanced Electronic Signature
Qualsiasi File .doc, .xls, .exe, .pdf, etc.	Solo file .pdf	Solo file .xml
L'estensione del file firmato è p7m	L'estensione del file firmato è pdf	L'estensione del file firmato è xml

La firma elettronica "semplice" invece garantisce l'identificazione informatica dell'utilizzatore esclusivamente in forma di PIN o insieme di Username e Password (come nel

caso delle e-mail); tale firma non assume valore di sottoscrizione e la relativa efficacia probatoria è liberamente valutabile dall'autorità giudiziaria.

La verifica della validità della firma digitale associata ad un documento informatico deve essere effettuata tramite le funzionalità dei servizi/piattaforme disponibili ([Documento Tecnico Operativo n. 44 – Istruzioni per la verifica della Firma Digitale](#)).

La **firma autografa** può essere apposta sui documenti analogici e sulle copie analogiche di documenti informatici.

### 2.2.7 Distinzione dei documenti in base allo stato di trasmissione

I documenti, analogici o informatici, in base allo stato di trasmissione si distinguono in:

- **documenti in arrivo:** si intendono tutti i documenti di rilevanza giuridico probatoria acquisiti dall'Ente nell'esercizio delle proprie funzioni e provenienti da un diverso soggetto pubblico o privato;
- **documenti in partenza:** si intendono i documenti di rilevanza giuridico probatoria prodotti dall'Ente nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato ed anche ai propri dipendenti come persone fisiche e non nell'esercizio delle loro funzioni;
- **documenti interni scambiati tra UOR;** si intendono i documenti scambiati tra le diverse UOR afferenti alla AOO.

## 2.3 Fascicolo

### 2.3.1 Definizione e funzione

Il *fascicolo* è l'unità di base dell'archivio e aggrega documenti che afferiscono allo stesso procedimento.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che il diritto di accesso. Si possono distinguere cinque tipologie di fascicolo:

- di **"Affare"**, conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme;
- di **"Attività"**, conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;

- di **“Procedimento amministrativo”**, conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento finale;
- di **“Persona fisica” o “Persona giuridica”**, **conserva i documenti relativi a diversi procedimenti amministrativi, legati da un vincolo archivistico interno, relativo a una persona fisica (e.g. fascicolo del personale) o una persona giuridica.**

### 2.3.2 Formazione, implementazione e gestione

Per ogni tipologia, l'Ente può conservare in un *fascicolo informatico* gli atti, i documenti e i dati da chiunque siano stati formati. Il *fascicolo informatico* deve recare l'indicazione:

- dell'AOO titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti;
- dell'indice di classificazione (e.g. titolo, classe, sottoclasse, etc.);
- del numero del fascicolo, che è identificativo di una catena numerica relativamente alla classe di riferimento dell'anno di creazione;
- della data di apertura e di chiusura del fascicolo.

L'indicazione dell'UOR e del Responsabile del Procedimento Amministrativo (RPA) concorrono all'identificazione del fascicolo e al riconoscimento del responsabile. La UOR, l'RPA e la classe devono essere gli stessi per il documento e per il fascicolo.

## 2.4 Piani di classificazione e di conservazione

### 2.4.1 Piano di classificazione

Il piano di classificazione (c.d. titolario) è il sistema sul quale si basa la classificazione dei documenti costituito da voci articolate su più livelli gerarchici (es. titoli, classi, sottoclassi, ecc.) e definito sulla base delle attività, dei processi e dei servizi gestiti dall'organizzazione.

La voce di I livello del piano di classificazione individua per lo più processi/servizi primari dell'organizzazione, mentre le sotto-articolazioni della voce corrispondono a specifiche attività/processi di maggiore dettaglio che rientrano concettualmente nei processi/servizi primari a cui il titolo si riferisce.

Il piano di classificazione documentale dell'Ente è articolato in titoli, a loro volta suddivisi in classi, sulla base della tipologia dei documenti prodotti e ricevuti dall'Ente, in relazione alle diverse attività, processi e servizi dallo stesso gestiti.

Il piano di classificazione documentale dell'Ente è stato definito e introdotto a decorrere dal 1° luglio 2017, a seguito dell'avvio in operativo – ai sensi del D.L. n. 193/2016 – di Agenzia delle entrate-Riscossione, tenendo conto anche delle esigenze di continuità con il pregresso assetto societario della riscossione. Il piano è stato oggetto di successive integrazioni in relazione al consolidamento e allo sviluppo dei servizi e dell'operatività dell'Ente, anche in coerenza con l'evoluzione del contesto normativo di riferimento. Il piano riporta pertanto anche titoli e classi che sono stati posti "in disuso" (non utilizzabili per la classificazione di nuovi documenti) in quanto riferite a documenti relativi a procedimenti, attività e servizi dismessi o riferiti al pregresso assetto societario della riscossione.

Il piano è di riferimento per la classificazione di tutti i documenti prodotti e ricevuti dall'Ente, sia informatici che analogici, indipendentemente dai registri di protocollazione e dagli archivi utilizzati.

Il piano prevede i seguenti titoli:

- I. Governance – Organi;
- II. Governance - Affari Istituzionali e Relazioni Esterne;
- III. Governance - Attività di Governance;
- IV. Core business - Relazioni Enti;
- V. Core business - Produzione ruoli;
- VI. Core business – Riscossione;
- VII. Core business - Relazioni con i contribuenti;
- VIII. Core business - Procedure cautelari;
- IX. Core business - Procedure esecutive;
- X. Core Business - Procedure concorsuali;
- XI. Affari Legali;
- XII. Risorse Umane;
- XIII. Amministrazione e Finanza;
- XIV. Approvvigionamenti e Logistica;
- XV. Sistemi Informativi;
- XVI. Attezionati (in disuso);
- XVII. Riservati (in disuso);
- XVIII. Non contenzioso (in disuso);

Il piano di classificazione documentale dell'Ente è contenuto **nell'Allegato 4**.

### 2.4.2 Piano di conservazione

Il piano di conservazione documentale dell'Ente costituisce il punto di riferimento per la gestione del ciclo di vita dei documenti indicando la tempistica di riferimento ai fini dello scarto degli stessi (c.d. massimario di scarto) e i termini per il passaggio nel sistema di conservazione dei documenti informatici.

Il piano di conservazione è riportato **in Allegato 5**.

La tempistica individuata per ciascuna classe del piano di classificazione, definita in ragione delle caratteristiche e della natura dei documenti (quali di governance, contabili-amministrativi, negoziali, riferiti alla riscossione esattoriale, al contenzioso, al personale, ecc.), costituisce il riferimento per l'avvio, come definito al paragrafo 3.5.3, del processo di selezione dei documenti, dall'archivio di gestione documentale e/o dall'archivio di conservazione, che potrebbero essere oggetto di scarto.

I documenti che devono essere conservati, per il periodo temporale previsto dal Piano di conservazione, sono oggetto di:

- riversamento, in caso di documento informatico, in coerenza con la normativa di riferimento, nel sistema di conservazione dell'Ente. In sede di riversamento viene anche valutata l'esigenza operativa dell'Ente, sotto la supervisione del Responsabile della gestione documentale e con il coinvolgimento delle Strutture centrali competenti, di mantenere i documenti versati anche nei rispettivi archivi correnti;
- trasferimento, in caso di documento analogico, all'archivio di conservazione dell'Ente (CGD) da parte delle Strutture organizzative quando i documenti abbiano esaurito la propria utilità nel processo di lavorazione e con cadenza almeno annuale.

### 2.4.3 Procedure di scarto

Il processo di scarto comprende la propedeutica procedura di selezione dei documenti mediante definizione dell'approccio, dei criteri e dei requisiti specifici per lo scarto, a cura delle strutture competenti dell'Ente per i diversi titoli/classi di documenti, con il coordinamento e la supervisione del Responsabile della gestione documentale. Per la selezione dei documenti da sottoporre alla procedura di scarto sono adottati i seguenti criteri:

- che siano trascorsi i termini minimi previsti nel piano di conservazione;

- che non possiedano più alcuna rilevanza sul piano amministrativo e giuridico, in quanto riferiti a procedimenti conclusi e non più suscettibili di ulteriori interventi di ordine amministrativo o giurisdizionale.

La selezione in archivio dei documenti da sottoporre a scarto può avvenire con logica massiva/aggregata o puntuale in coerenza con i criteri e i requisiti definiti. I documenti oggetto di scarto sono sottoposti alla preventiva autorizzazione della competente Soprintendenza Archivistica e Bibliografica del MIBAC ai sensi della normativa vigente, nonché eventualmente allocati nell'archivio storico.

#### 2.4.4 Modifiche al piano di classificazione e al piano di conservazione

Il piano di classificazione e il piano di conservazione devono essere costantemente aggiornati in relazione ai procedimenti amministrativi e alle attività svolte dall'Ente. A tal fine il Responsabile della gestione documentale ne verifica periodicamente la rispondenza e ne assicura l'aggiornamento come di seguito indicato.

Le modifiche al piano di classificazione documentale (introduzione di nuovi titoli o classi o messa "in disuso" di quelle esistenti) e al piano di conservazione documentale dell'Ente possono essere adottate con provvedimento del Responsabile della gestione documentale, acquisita la preliminare condivisione della Direzione Organizzazione e Processi.

### 3. PROTOCOLLO INFORMATICO

L'Ente organizza e gestisce il servizio per la tenuta del protocollo informatico e della gestione dei flussi documentali, come previsto dall'art. 61 del DPR n. 445/2000, cui è attribuita la competenza sulla tenuta del sistema di gestione analogica e informatica dei documenti, dei flussi documentali e degli archivi, nonché il coordinamento degli adempimenti previsti dalla normativa vigente.

Ogni qualvolta venga emanata o modificata una delle normative interne dell'Ente che direttamente o indirettamente contenga delle disposizioni in merito alla protocollazione è necessario un previo coinvolgimento dell'Ufficio Protocollo.

Ogni operatore è responsabile della corrispondenza dei dati desunti dal documento protocollato rispetto a quelli immessi nel sistema di protocollo. Il sistema di protocollo assicura la tracciabilità di tutte le registrazioni effettuate e dei relativi flussi documentali.

A supporto delle attività operative i singoli operatori possono avvalersi del Servizio di Help Desk ICT dell'Ente.

Di seguito sono indicate le regole e le modalità adottate dall'Ente per la protocollazione dei documenti, i Registri di protocollo previsti e l'illustrazione del sistema informatico di protocollazione (Docway) utilizzato dall'Ente.

#### 3.1 Regole e modalità di protocollazione

##### 3.1.1 Registrazione di protocollo

Per registrazione si intende l'insieme delle procedure e degli elementi attraverso i quali i documenti vengono trattati sotto il profilo strettamente giuridico - probatorio, assumendo l'addetto al protocollo la funzione certificativa della effettiva ricezione e spedizione dei documenti.

La registrazione deve essere effettuata, di norma, **entro la giornata di arrivo o comunque entro 24 ore dal ricevimento del documento**. I documenti che arrivano il venerdì dopo l'orario di chiusura dell'Ente o di sabato e nei festivi, sono protocollati il giorno lavorativo successivo.

Dopo l'avvenuta registrazione gli elementi del documento protocollato sono riconducibili a due tipologie:

- elementi immodificabili;
- elementi modificabili.

Gli **elementi immodificabili** servono ad attribuire a ciascun documento data, forma e provenienza certa attraverso la registrazione delle informazioni rilevanti sul piano giuridico - probatorio. Pertanto, il sistema informatico impedisce la loro modifica una volta registrati.

Essi sono:

- 1) data di registrazione;
- 2) numero di protocollo;
- 3) corrispondente (mittente per documento in arrivo; destinatario per documento in partenza);
- 4) oggetto;
- 5) impronta del documento informatico;
- 6) numero degli allegati;
- 7) descrizione degli allegati.

Gli **elementi modificabili obbligatori** sono:

- 1) UOR;
- 2) responsabile del procedimento amministrativo;
- 3) classificazione archivistica in base al Titolare;
- 4) fascicolo (ove applicabile).

Gli **elementi modificabili non obbligatori** sono:

- 1) Recapito del mittente;
- 2) Collegamenti ad altri documenti diversi da quello di inserimento;
- 3) Tipologia di documento;
- 4) Durata della conservazione;
- 5) Altri tipi di annotazione.

### 3.1.2 Registrazione di protocollo differito

La registrazione differita di protocollo in entrata è consentita solo nel caso:

- di pervenimento della corrispondenza nei giorni non feriali;
- di pervenimento della corrispondenza nei giorni feriali ma al di fuori dell'orario di lavoro;
- di eccessivo carico di lavoro;

non sia possibile effettuare la protocollazione nel medesimo giorno in cui è pervenuta la corrispondenza. Tale facoltà è comunque limitata ai casi in cui non venga pregiudicato il

diritto del terzo; in tale ultima ipotesi sarà comunque garantita la registrazione della data effettiva di ricezione della corrispondenza informatica o analogica.

### 3.1.3 Conservazione delle registrazioni

Ogni registrazione di protocollo informatico produce un "record" nel sistema di gestione documentale. Ogni operazione di inserimento e modifica viene registrata su un file di log. In tal modo si è in grado di ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolatura ecc.).

Al fine di garantire l'immodificabilità delle registrazioni, il registro informatico di protocollo giornaliero viene trasmesso in conservazione entro la giornata lavorativa successiva.

### 3.1.4 Segnatura

La segnatura di protocollo è l'apposizione o l'associazione al documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile.

La registrazione e la segnatura costituiscono un'operazione unica e contestuale aventi entrambe la natura di atto pubblico.

L'operazione di segnatura deve consentire l'identificazione univoca e certa nel formato previsto dalle norme vigenti.

Gli elementi della segnatura devono essere apposti sui documenti prodotti da registrare in partenza, sui documenti in ingresso e sui documenti scambiati tra le UOR dell'Ente (protocollo tra uffici).

Per il **documento analogico**, la segnatura può avvenire con stampa di apposite etichette adesive, sulle quali vengono riportate le informazioni con i dati della segnatura, da applicare sulla prima pagina del documento originale. L'acquisizione dell'immagine è eseguita solo dopo l'operazione di segnatura, in modo da inserire nel Protocollo Informatico il documento scansionato contenente i dati della segnatura.

Per i documenti in partenza materializzati la segnatura consiste nell'apposizione del numero e della data di protocollo, generate dal sistema informatico, ovvero dal registro particolare utilizzato per lo specifico documento in partenza.

Le informazioni da associare al documento analogico desunte dal sistema di protocollo sono:

- l'identificazione in forma sintetica o estesa dell'amministrazione e dell'AOO individuata ai fini della registrazione e della gestione del documento;
- il numero progressivo di protocollo;
- la data di protocollo;
- la classificazione in base al Piano di classificazione vigente;
- l'identificativo UOR a cui il documento è assegnato per competenza e responsabilità (RPA);
- le eventuali UOR in copia conoscenza.

Per il **documento informatico**, qualora lo stesso sia pervenuto tramite PEC, la ricevuta di protocollazione è rilasciata direttamente dal sistema di gestione documentale.

Se il documento informatico è pervenuto tramite *e-mail*, la ricevuta, se richiesta, sarà generata in formato pdf o pdf/a e inviata via *e-mail* al mittente. Le informazioni minime da associare sono:

- codice identificativo dell'amministrazione;
- codice identificativo dell'AOO;
- codice identificativo del registro;
- numero di protocollo,
- data di protocollo;
- anno solare di riferimento del registro di protocollo.

Oltre alle informazioni minime la segnatura deve prevedere:

- classificazione in base al Piano di classificazione vigente;
- codice identificativo dell'ufficio a cui il documento è assegnato;
- ogni altra informazione utile o necessaria, già disponibile al momento della registrazione.

### 3.1.5 Scansione

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura di protocollo sono acquisiti in formato immagine mediante il processo di scansione. Tale processo si articola nelle seguenti fasi:

- Acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file in formato pdf/a standard abilitato alla conservazione;

- Verifica della leggibilità, accessibilità e qualità delle immagini acquisite;
- Verifica piena corrispondenza del documento scansionato con l'originale analogico;
- Collegamento delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile.

### 3.1.6 Classificazione

Tutti i documenti ricevuti e prodotti, indipendentemente dal supporto sul quale sono formati, sono classificati in base al Piano di classificazione.

Il protocollo informatico non permette la registrazione di documenti non classificati, inoltre garantisce la storicizzazione delle variazioni del Titolare e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei documenti in relazione al Titolare vigente al momento della produzione degli stessi.

### 3.1.7 Assegnazione

Gli operatori abilitati alla protocollazione in ingresso provvedono ad assegnare i documenti acquisiti tramite il sistema di gestione documentale alle aree/strutture competenti per materia/funzione (UOR), quali RPA, in coerenza con l'organigramma, il funzionigramma e il sistema di normativa interna dell'Ente. Ciascun Responsabile di struttura organizzativa presidia i documenti assegnati nel sistema di protocollazione, anche con riferimento alle eventuali ulteriori strutture logiche collegate alla propria UOR e dedicate a processi/tematiche di competenza, così come definito dalla normativa interna dell'Ente.

Il medesimo documento può essere reso disponibile nel sistema di gestione documentale ad altre aree/strutture usando il tasto funzione "nuovo cc" ovvero attraverso la funzione "conferenza di servizi" per competenza e per conoscenza.

L'ufficio assegnatario può a sua volta condividere i documenti alle aree/strutture ad essa afferenti attraverso l'apposita funzione del sistema di gestione documentale. Qualora sia necessario consegnare un documento analogico originale, questo dovrà essere consegnato all'ufficio che risulta assegnatario ed eventuali assegnazioni per conoscenza devono essere sempre effettuate tramite il sistema di gestione documentale.

Nel caso di un'assegnazione errata, la struttura che riceve il documento è tenuta al rigetto dello stesso, ai sensi del par. 3.1.8, ovvero, se ne ha conoscenza, alla riassegnazione alla struttura competente.

Il sistema di gestione informatica dei documenti tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'operatore agente, data e ora di esecuzione.

I documenti analogici, protocollati e assegnati, e la posta che non necessita di protocollazione, sono resi disponibili ai destinatari (RPA) dalle strutture protocollanti.

L'indicazione per l'ulteriore eventuale inoltro dei documenti verso altre amministrazioni; è contenuta nella normativa interna per la gestione del Protocollo informatico.

### 3.1.8 Rigetto

Il RPA se ritiene che il documento assegnatogli non è di propria competenza e non conosce il RPA corretto, deve utilizzare la funzione "Rigetta" unitamente alla esplicazione puntuale delle motivazioni nel campo "Annotazioni". In tal caso il documento protocollato viene automaticamente restituito alla struttura protocollante che, a sua volta, sulla base delle indicazioni ricevute nell'annotazione, provvede a riassegnare correttamente il documento protocollato al competente Responsabile per l'espletamento dei relativi adempimenti.

### 3.1.9 Smistamento

Lo smistamento dei documenti all'interno dell'Ente avviene, di norma, attraverso il sistema di assegnazione del Protocollo Informatico coerentemente all'organigramma e funzionigramma dell'Ente.

Gli originali dei documenti cartacei - preventivamente scansionati ed inseriti nel protocollo informatico (come previsto nel par. 3.1.5) sono trasmessi alla struttura Responsabile del procedimento (RPA) o eventualmente collocati negli archivi dell'Ente, secondo le indicazioni fornite dalla stessa.

### 3.1.10 Annullamento di protocollo

L'annullamento di una registrazione di protocollo è un'operazione del tutto eccezionale, consentita solo nei casi previsti dalla vigente normativa in materia, con autorizzazione del Settore Gestione Documentale e Protocollo. In particolare, l'annullamento è previsto per errori materiali nell'inserimento di dati obbligatori quali ad esempio:

- a) errata indicazione del canale di acquisizione del documento nell'Archivio dell'Ente (entrata, uscita, interno);
- b) protocollazione di un documento già protocollato;

c) errore di battitura nel campo oggetto la cui modifica non comporti il cambiamento del significato dello stesso oggetto;

d) errata indicazione del mittente (se in entrata) o del destinatario (se in uscita).

Nei casi citati si deve obbligatoriamente procedere con la richiesta di annullamento dell'intera registrazione.

Non è mai consentito l'annullamento o la modifica di un campo modificabile di un documento che è già stato spedito al destinatario.

È consentita la modifica (autorizzata dal Responsabile della gestione documentale) al campo oggetto di registrazione solo se la modifica non comporta un sostanziale cambiamento della registrazione stessa.

La richiesta di annullamento deve essere effettuata, tramite mail indirizzata al protocollo centrale ([protocollo@agenziariscossione.gov.it](mailto:protocollo@agenziariscossione.gov.it)) e per conoscenza al Responsabile della gestione documentale, dall'operatore che ha effettuato la registrazione nel protocollo informatico.

La richiesta deve essere motivata e tipiche motivazioni "standard" di una richiesta di annullamento sono:

- per errata compilazione di campo non modificabile (oggetto, mittente, destinatario);
- in quanto documento registrato come interno anziché in entrata;
- in quanto documento registrato come interno anziché in uscita;
- in quanto documento registrato in entrata anziché in uscita;
- in quanto documento registrato in uscita anziché in entrata;
- in quanto documento registrato in entrata anziché come interno;
- in quanto documento registrato in uscita anziché come interno;
- per assegnazione di numero a documento già protocollato (esclusivamente per il registro di emergenza);
- per registrazione di protocollo effettuata senza inserimento dei relativi allegati;
- per errore nella redazione del documento informatico principale rilevato dopo la registrazione di protocollo;
- per errore nella redazione del documento informatico allegato rilevato dopo la registrazione di protocollo;
- perché è venuto a meno il motivo amministrativo per il quale il documento era stato prodotto;
- per registrazione di protocollo generata per errore durante una fase di prova (test).

Se è stata prodotta una nuova registrazione in sostituzione di quella da annullare, nella richiesta di annullamento deve essere indicato anche il nuovo numero di protocollo.

In definitiva, la procedura di annullamento deve riportare una dicitura o un segno in posizione visibile comunque da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore e agli estremi del procedimento di autorizzazione.

### 3.1.11 Documenti soggetti a registrazione particolare

Conformemente alle policy dell'Ente per utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati, con particolare riferimento agli obblighi di riservatezza nel trattamento delle informazioni, sono riportate di seguito le modalità operative per la protocollazione e gestione di particolari tipologie di documenti in ingresso; più precisamente per i documenti analogici:

- **Corrispondenza personale:** la corrispondenza che riporta come destinatario soltanto il nominativo di una persona - senza alcun riferimento alla funzione, all'ufficio di appartenenza, a un progetto, a un prodotto oppure che riportano in chiaro la dicitura "riservata" o "personale", "confidenziale" o simili - non viene aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli alla struttura protocollante di riferimento;
- **Corrispondenza indirizzata agli Organi dell'Ente:** tutta la corrispondenza indirizzata, anche solo genericamente, agli Organi dell'Ente non deve essere mai aperta. L'addetto alla funzione di protocollo si limiterà a scansionare la busta che verrà protocollata in modalità "riservato" e consegnata al Settore Segreteria Tecnica che provvederà a riportare sul documento il numero di protocollo presente sulla busta;
- **Corrispondenza indirizzata all'Area Risorse Umane, alla Direzione Internal Audit ed al Responsabile della prevenzione della corruzione:** l'addetto all'attività di protocollo si limiterà a scansionare la busta che verrà protocollata e consegnata ai Responsabili destinatari che provvederanno a riportare sul documento il numero di protocollo presente sulla busta;
- **Lettere anonime:** le lettere anonime vanno protocollate con indicazione di "anonimo" nel campo mittente ed in modalità "riservato". L'operatore di protocollazione dovrà inserire come RPA il Responsabile del Settore Segreteria Tecnica;

- **Lettere prive di firma o con firma illeggibile:** le lettere prive di firma o con firma illeggibile vanno protocollate con indicazione di "privo di firma" o "firma illeggibile" nel campo mittente ed in modalità "riservato". L'operatore di protocollazione dovrà inserire come RPA il Responsabile del Settore Segreteria Tecnica;
- **Buste di gara:** la corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso", "procedura", "avvisi pubblici di indagine di mercato per la ricerca di immobili" o simili o comunque dalla cui confezione si evinca la partecipazione ad una gara, non viene aperta ma viene protocollata in entrata con l'apposizione del numero di protocollo direttamente sulla busta (plico o simili). Il responsabile (RPA) ovvero un suo delegato provvederà entro la giornata di assegnazione a ritirare la busta (plico o simili), ed una volta aperta a riportare il numero di protocollo e la data di registrazione già assegnati al documento, conservando la busta (plico o simili) come allegato a comprova della provenienza, della data e dell'orario di ricezione e contestuale protocollazione.

Per taluni documenti analogici o informatici dell'Ente, connessi principalmente alle attività di riscossione e prodotti con modalità massiva e da sistemi informatici centralizzati, è previsto l'utilizzo di "registri particolari di protocollo" (cfr. par. 3.2.3).

I documenti e le comunicazioni ricevuti via **posta elettronica (e-mail) non certificata** privi di sottoscrizione possono, a discrezione della UOR, essere oggetto di protocollazione. Laddove gli stessi siano sottoscritti con firma digitale (o con altro mezzo idoneo ad accertarne la fonte di provenienza) sono da considerarsi originali a tutti gli effetti di legge e nel caso in cui **il contenuto sia rilevante al fine giuridico-probatorio sono soggette a protocollazione.**

I documenti informatici prodotti o gestiti da applicativi e procedure informatizzate, anche di altri Enti/Autorità, a supporto di specifici processi dell'Ente, possono essere soggetti a registrazione particolare, anche tramite gli applicativi di altri Enti/Autorità laddove consentito dalla specifica normativa vigente.

Per i documenti informatici classificati come "riservati" (ai sensi dell'art. 38 Disciplinare per l'utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati di AdeR), in quanto contenenti "*informazioni e dati che possono essere trattati esclusivamente da un ristretto numero di persone, sulla base di specifiche indicazioni del/dei vertice/direttori/responsabili dell'Ente*", la protocollazione deve essere fatta nel sistema Docway con modalità "riservato" che consente la visibilità e l'intervento sul protocollo ai soli assegnatari dello stesso.

### 3.1.12 Documenti esclusi dalla registrazione

L'art. 53, comma 5 del DPR 445/2000 prescrive l'esclusione dalla registrazione a protocollo delle seguenti tipologie:

- bollettini ufficiali P.A.;
- notiziari P.A.;
- materiali statistici;
- atti preparatori interni;
- giornali e riviste;
- libri;
- materiali pubblicitari;
- gazzette ufficiali;
- inviti a manifestazioni che non attivino procedimenti amministrativi.

## 3.2 Registri e Repertori di protocollo

### 3.2.1 Registro di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso ed è idoneo a produrre effetti giuridici nei confronti dei terzi.

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

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

La produzione del documento avviene dopo la chiusura del registro di protocollo e prima della riapertura nel giorno successivo in modo che nessun altro documento possa essere protocollato nel registro della giornata precedente né tramite operatore né in modalità automatica.

All'avvio del processo di creazione del pacchetto di versamento, vengono elaborati i dati presenti nel registro di protocollo al fine di:

- ottenere i metadati di profilo specifici da inviare al sistema di conservazione (Numero iniziale, Numero Finale, Data inizio registrazione, Numero di documenti registrati, Numero di documenti annullati);

- effettuare la registrazione del file PDF nel registro/repertorio stabilito e memorizzare tra gli attributi estesi del documento quelli calcolati precedentemente;
- predisporre il documento all'invio in conservazione;
- inviare, in caso di anomalia durante il flusso, una notifica.

Il trasferimento del pacchetto di versamento al sistema di conservazione avviene tramite un processo automatico che si occupa di creare il pacchetto di versamento, inviarlo al sistema di conservazione e registrare lo stato del versamento stesso.

### 3.2.2 Registro di emergenza

Nelle situazioni di emergenza nelle quali non sia possibile utilizzare il protocollo informatico a causa di eventi quali, a titolo meramente indicativo:

- un guasto all'applicativo utilizzato per le attività di protocollazione;
- un guasto al sistema informatico;

il documento deve essere registrato comunque su un supporto alternativo, denominato registro di emergenza (RE).

L'attivazione del registro di emergenza è autorizzata dal Responsabile dell'Ufficio Protocollo, ovvero suo delegato, che ha anche il compito di:

- redigere il modello di autorizzazione per l'attivazione del registro di emergenza attivazione utilizzando il modello **A** di cui **all'Allegato 6**;
- dare comunicazione alle strutture protocollanti della attivazione della procedura di emergenza.

Al termine dell'emergenza il Responsabile dell'Ufficio Protocollo, o suo delegato, devono:

- formalizzare la revoca dell'autorizzazione per l'attivazione del registro di emergenza utilizzando il modello **B** di cui **all'Allegato 6**;
- dare comunicazione alle strutture protocollanti della revoca della procedura di emergenza.

Sul registro, utilizzando il modello **C** di cui **all'Allegato 6**, devono essere riportate la causa, la data e l'ora di inizio dell'interruzione, nonché la data e l'ora del ripristino della piena funzionalità del sistema.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile autorizza l'uso del registro di emergenza fino al ripristino del protocollo informatico.

Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate.

La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti; più precisamente:

- la numerazione del registro di emergenza è distinta da quella del protocollo ufficiale, è unica per l'intero anno e ricomincia dal numero successivo all'ultimo generato per ogni attivazione;
- ogni documento è individuato dal numero assegnato nel registro di emergenza a partire dal n. 1 e preceduto dal codice della propria struttura;
- ogni foglio deve essere numerato in modo che più operatori possano lavorare contemporaneamente.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dati.

Durante la fase di ripristino a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

Il registro di emergenza si rinnova ogni anno solare; inizia pertanto il 1° gennaio e termina il 31 dicembre di ogni anno.

Il Responsabile dell'Ufficio Protocollo, o suo delegato, deve annotare i periodi di attivazione del registro di emergenza; qualora nel corso di un anno non si sia fatto ricorso allo stesso ne annota il mancato uso.

### 3.2.3 Registri particolari di protocollo

L'Ente, oltre ai registri di cui ai punti precedenti, la cui istituzione è obbligatoria, utilizza Registri particolari di protocollo destinati alla registrazione di determinate fattispecie di documenti tra loro omogenee per contenuto, finalità o modalità di gestione, quali:

- cartelle di pagamento;
- avvisi di intimazione;
- preavvisi di fermo amministrativo;
- comunicazioni preventive iscrizione ipotecaria;

- pignoramenti presso terzi;
- proposte di compensazione ex art. 28-ter del D.P.R. 602/1973;
- comunicazioni relative alla definizione agevolata, alle procedure concorsuali, alle eccedenze di pagamento;
- comunicazione richieste di rimborso agli enti;
- certificazioni uniche ai professionisti;
- conti di gestione digitali;
- piani di rateizzazione;
- fatture elettroniche.

I Registri particolari assicurano modalità di registrazioni analoghe a quelle assicurate dalla segnatura di protocollo dei documenti. In particolare, è assicurata la consequenzialità dei numeri di registrazione attribuiti in forma automatica e la non modificabilità delle registrazioni: è infatti lo stesso sistema, che produce queste tipologie di documenti, che genera e appone la segnatura su ciascun documento.

### 3.2.4 Repertori

Il repertorio è una aggregazione documentale che raccoglie documenti identici per forma e provenienza, ma difformi per contenuto, disposti in sequenza cronologica. Ciascun documento, in base a tale ordine, è identificato con un numero progressivo cui viene riconosciuta una valenza probatoria.

I repertori che costituiscono mere aggregazioni sono:

<b>Corrispondenza del Presidente IN</b>	<b>Corrispondenza del Presidente OUT</b>
<b>Curriculum Vitae</b>	<b>Deleghe AFC</b>
<b>Determinazioni del Presidente</b>	<b>Determinazione Responsabile Area ISO</b>
<b>Disposizioni Direzione Approvvigionamenti Partenza</b>	<b>Disposizioni Direzione Approvvigionamenti fra Uffici</b>
<b>Disposizioni Settore Acquisti Partenza</b>	<b>Disposizioni Settore Acquisti fra Uffici</b>

Oltre a quelli citati, nell'Ente sono definiti e gestiti particolari fattispecie per le quali è prevista una più ampia raccolta informativa che riguardano:

- 1) Contenzioso - atti introduttivi al giudizio,
  - 2) Contenzioso – atti successivi (relativi a sentenze, precetti e pignoramenti)
- Il **repertorio degli atti introduttivi** si compone di tutti i documenti (citazioni, ricorsi, etc.) relativi alla costituzione in giudizio. Le informazioni trattate sono riportate nel seguente schema:

REPERTORIO CONTENZIOSO - ATTI INTRODUTTIVI - INSERIMENTO	
TIPO	Nessuna <input type="text"/>
DATA SCADENZA	<input type="text"/>
<b>CONTENZIOSO</b>	
* TIPO ATTO INTRODUTTIVO	- <input type="text"/>
* AUTORITÀ GIUDIZIARIA ADITA	<input type="text"/>
* CODICE FISCALE CONTROPARTE	<input type="text"/>
<b>ATTO IMPUGNATO</b>	
ULTERIORI ATTI IMPUGNATI	- <input type="text"/>
* NUMERO ATTO IMPUGNATO	<input type="text"/>
ELENCO ULTERIORI ATTI IMPUGNATI	<input type="text"/>
DATA PRIMA UDIENZA	<input type="text"/>
* DATA NOTIFICA RICORSO	<input type="text"/>
ESTREMI NOTIFICA ATTO	<input type="text"/>
STATO DI LAVORAZIONE	- <input type="text"/>
STATO DI LAVORAZIONE AL	<input type="text"/>
NUMERO PRATICA AL	<input type="text"/>
<b>BARCODE</b>	
BARCODE	<input type="text"/>

Il **secondo repertorio** riguarda gli atti successivi relative al contenzioso esattoriale. Le informazioni trattate per le **sentenze** sono riportate nel seguente schema:

 **REPERTORIO CONTENZIOSO - ATTI SUCCESSIVI - INSERIMENTO**

**SCADENZA**

TIPO  ▼

**ATTI SUCCESSIVI**

\* TIPO ATTO SUCCESSIVO ⓘ  ▼  
Comunicazione del dispositivo della sentenza  
Sentenza/ordinanza

\* AUTORITÀ GIUDIZIARIA ADITA DEL RICORSO/SENTENZA  Q

\* R.G. ATTO INTRODUTTIVO NUMERO/ANNO

\* NUMERO SENTENZA/ANNO

\* CODICE FISCALE CONTROPARTE

\* NUMERO ATTO ESATTORIALE IMPUGNATO ⓘ

\* DATA NOTIFICA ATTO PERVENUTO ⓘ  📅

\* CONDANNA ALLE SPESE  ▼

STATO DI LAVORAZIONE  ▼

STATO DI LAVORAZIONE AL ⓘ

NUMERO PRATICA AL ⓘ

Le informazioni trattate per i **precetti e pignoramenti** sono riportate nel seguente schema:

 **REPERTORIO CONTENZIOSO - ATTI SUCCESSIVI - INSERIMENTO**

**DATI DEL DOCUMENTO**

SIGLA STRUTT.  ANNO

\* MITTENTE  Q A MEZZO  ▼

FIRMATARIO  Q RUOLO

DATA DOC.  📅 PROT. MITTENTE

VOCE DI INDICE  Q

\* OGGETTO

\* ALLEGATO  - +

\* CLASSIF.  Q 📄 XI/3 - Sentenza con precetto, precetto e pignoramento

VISIBILITÀ  ▼

**ATTI SUCCESSIVI**

\* TIPO ATTO SUCCESSIVO

\* AUTORITÀ GIUDIZIARIA ADITA DEL RICORSO/SENTENZA

\* R.G. ATTO INTRODUTTIVO NUMERO/ANNO  /

\* NUMERO SENTENZA/ANNO  /

\* CODICE FISCALE CONTROPARTE

\* DATA NOTIFICA ATTO PERVENUTO

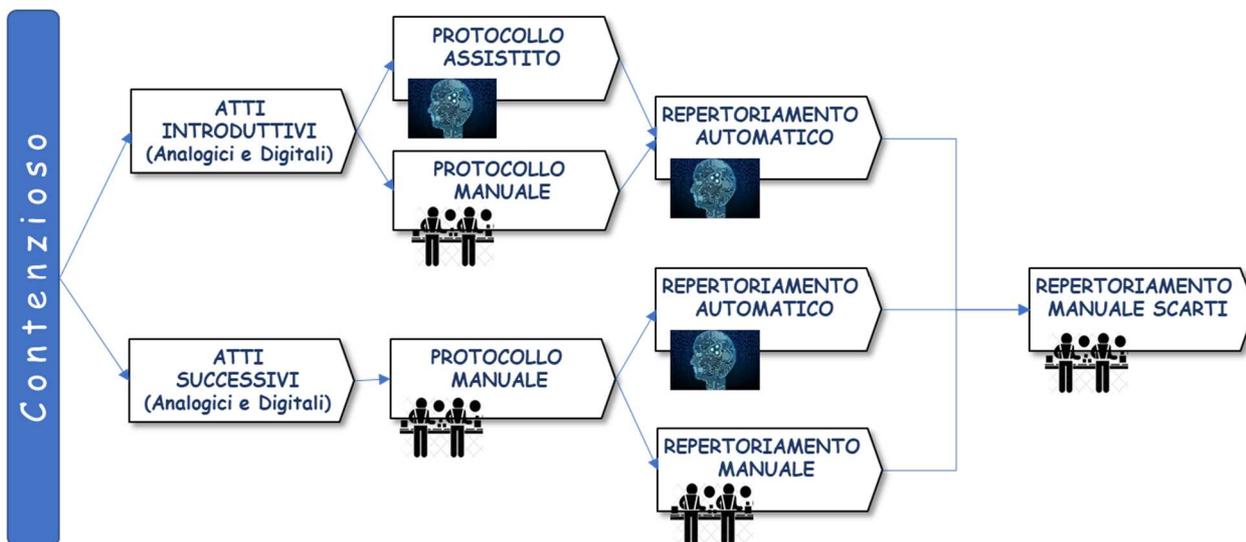
STATO DI LAVORAZIONE

STATO DI LAVORAZIONE AL

NUMERO PRATICA AL

I principi di riservatezza, le politiche di sicurezza, la tutela delle informazioni e la tracciabilità delle modifiche adottate per il protocollo informatico si estendono alla gestione dei repertori.

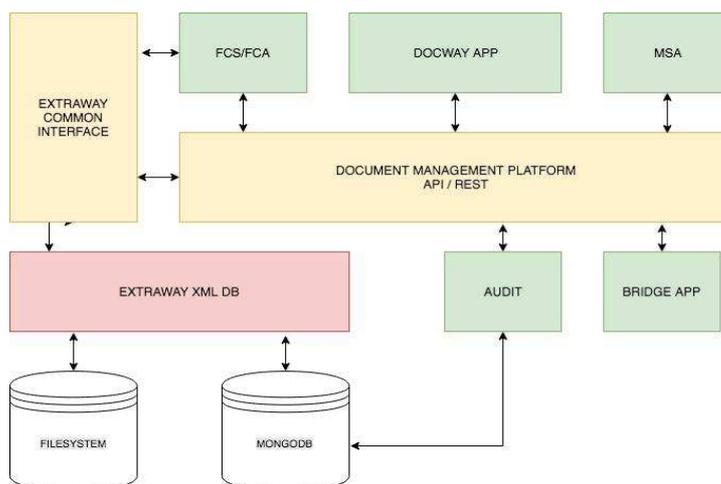
Il processo di repertoriamento può essere manuale o assistito da intelligenza artificiale e può avvenire contestualmente alla protocollazione, ovvero costituirsi in fasi e tempi successivi. Gli scarti (record che non soddisfano le soglie di qualità attese) sono gestiti dall'Ufficio Protocollo. La figura che segue rappresenta sinteticamente l'operatività descritta.



### 3.3 Sistema informatico di protocollazione (Docway)

#### 3.3.1 Sistema di protocollazione di Agenzia delle entrate-Riscossione

Il Protocollo Informatico in uso presso l'Ente è DOCWAY® XML Ver. 4RE la cui architettura è riportata nello schema che segue:



Detto sistema è una full web application sviluppata in Java in ambiente J2EE in architettura three-layer.

La soluzione gestisce e supporta la modalità multi-Ente e multi-AOO senza alcuna limitazione, né tecnologica, né funzionale, né commerciale (software a riuso per le PP.AA.) in quanto consente di configurare più ambienti virtuali e fisici al fine di bilanciare l'esigenza di performance con la massima separazione delle informazioni ed autonomia dei sottosistemi.

DOCWAY® XML Ver. 4RE è una soluzione:

- aperta basata sulla piattaforma tecnologica EXTRAWAY® XML DATABASE di 3D Informatica, realizzata adottando gli Open Standard di riferimento (XML, JEE, SOA), per garantire l'espandibilità della soluzione e per accogliere una eventuale futura razionalizzazione e automazione di altri flussi applicativi;
- risponde a stringenti requisiti in termini di sicurezza, sia per quanto concerne l'accesso al sistema, sia per quanto concerne l'autenticità e la sicurezza dei documenti gestiti. Il sistema può avvalersi di sistemi di autenticazione forte per l'accesso e di una architettura PKI per quanto concerne la firma e la crittografia dei documenti, nonché la loro archiviazione digitale a norma.

Il sistema di Protocollo informatico Docway, in riferimento alle misure di sicurezza previste (cfr. capitolo 6), è configurato in modo da consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti e assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate, nonché l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate. Ciascun utente del Protocollo Informatico può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli UO ad esso subordinati. In deroga alle regole sopra definite, è possibile ampliare gli accessi in funzione di specifiche e comprovate esigenze lavorative ed in ogni caso attraverso le autorizzazioni dei responsabili.

I livelli di autorizzazione per l'accesso alle funzioni del protocollo informatico sono definiti e gestiti secondo regole approvate dal Responsabile della gestione documentale. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione ai diritti di intervento sul documento (modifica e annullamento delle informazioni).

Esistono diversi profili dei diritti di accesso, sia in termini di visibilità dei documenti che per possibilità di inserimento, modifica e annullamento delle informazioni di protocollo.

Ad ogni utente censito nell'anagrafe del sistema di protocollo viene assegnato, attraverso IGI, un profilo di default che prevede la gestione dei documenti ad esso assegnati e di quelli in carico al proprio ufficio di appartenenza identificato sulla base dell'organigramma.

L'estensione del profilo dei diritti di accesso viene effettuata attraverso IGI su specifica richiesta del Responsabile del soggetto proprietario del profilo o del soggetto stesso.

La "Visibilità" dei documenti è condizionata, oltre che dal profilo abilitativo assegnato all'utente, anche dalla modalità con la quale è stata eseguita la registrazione. In particolare, il documento può essere registrato come:

- "Pubblico": visibile a tutti gli utenti che abbiano assegnato il diritto di visione del relativo documento;
- "Riservato": visibile solo agli utenti assegnatari del protocollo.

Il RPA dei documenti protocollati ha la possibilità di riassegnare gli stessi a nuovi utenti assegnatari coinvolti nel processo amministrativo. Gli eventuali diritti di intervento o di nuova assegnazione di un documento, protocollato in forma riservata, altamente confidenziale o segreta, sono fruibili dai soli assegnatari o dall'utente che ha protocollato il documento se inserito tra gli assegnatari dello stesso. Se l'utente abilitato all'inserimento che ha protocollato il documento, in forma riservata, non è inserito tra gli assegnatari, successivamente alla registrazione, perde i diritti di visibilità e quindi anche di intervento sul

documento. Ogni operazione di inserimento, assegnazione, lettura, intervento sui documenti (modifica e annullamento) viene storicizzata dal sistema.

Ogni profilo abilitativo istituito può essere integrato da ulteriori specifiche abilitazioni/diritti per l'utilizzo di funzioni che non mutano le caratteristiche principali del profilo stesso. Ci si riferisce in questo caso all'abilitazione per la fascicolazione e la archiviazione dei documenti (in raccoglitori), ai diritti di visibilità di particolari Repertori e ai diritti di inserimento e intervento in relazione ai documenti protocollati in essi contenuti.

### 3.3.2 Sistemi di protocollazione delle entità pregresse confluite nell'Ente

Il sistema di protocollo garantisce altresì la possibilità di ricercare documenti pregressi alla costituzione dell'Ente (ante 1° luglio 2017), atteso che lo stesso nasce da un percorso di progressivo accorpamento, tramite molteplici operazioni societarie, delle precedenti diverse società del Gruppo Equitalia nonché dall'avvio, dal 1° luglio 2017, di Agenzia delle entrate-Riscossione.

Tali funzionalità sono realizzate mediante ambienti dedicati di Docway, per garantire la continuità operativa delle attività trasferite, secondo le regole di cui al presente Manuale (laddove compatibili) in riferimento sia ai documenti analogici che a quelli informatici.

## 4. FLUSSI DOCUMENTALI

### 4.1 Descrizione dei flussi documentali

Il presente capitolo fornisce indicazioni per lo scambio di documenti all'interno ed all'esterno dell'Ente. La corrispondenza in ingresso può essere acquisita dall'Ente con diversi mezzi e modalità in base al canale di invio utilizzata dal mittente.

La protocollazione della corrispondenza in ingresso è curata dalle strutture protocollanti presenti su ciascuna sede dell'Ente; per la corrispondenza in ingresso tramite PEC non istituzionale è, invece, protocollata dalle strutture assegnatarie delle PEC stesse. La protocollazione della corrispondenza in uscita è curata, in modo distribuito, dalla struttura mittente dell'Ente.

Il processo di protocollazione dell'Ente prevede, dal punto di vista funzionale, diverse modalità di protocollazione (manuale, automatica e assistita da sistemi di intelligenza artificiale).

Nell'ambito del processo di gestione documentale, il documento amministrativo, in termini operativi, è classificabile in:

- Entrata;
- Uscita;
- Interno;

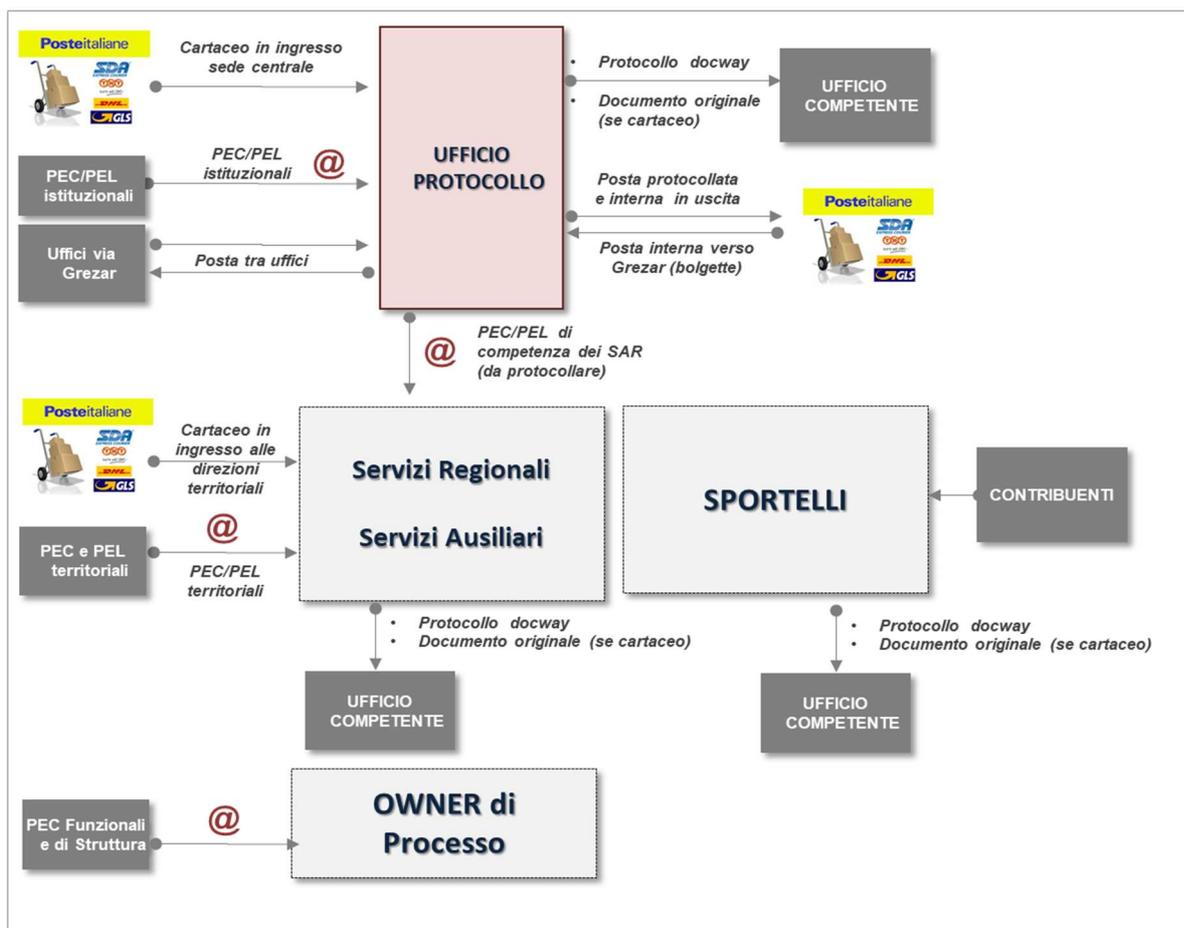
I documenti analogici sono ricevuti (in entrata) o trasmessi (in uscita) mediante posta ordinaria, posta raccomandata, notifica postale/messo ovvero con consegna "brevi manu".

I documenti informatici sono ricevuti (in entrata) o trasmessi (in uscita) mediante posta elettronica certificata (PEC), posta elettronica ordinaria (PEL), canali web, sportello "on line", con servizi di interoperabilità tra sistemi applicativi (cooperazione applicativa), ovvero, ove previsto, su supporto rimovibile (Cd ROM, DVD, ecc.).

I documenti informatici interni sono trasmessi tra UOR mediante sistema di protocollo Docway, con registrazione come "protocollo interno" e utilizzando la funzione di assegnazione alla UOR destinataria. Eventuali documenti analogici interni devono essere comunque protocollati e deve essere caricato il relativo file per immagine (scansione) sul sistema di protocollo, mentre il documento originale deve essere trasmesso al destinatario tramite i servizi di spedizione interna.

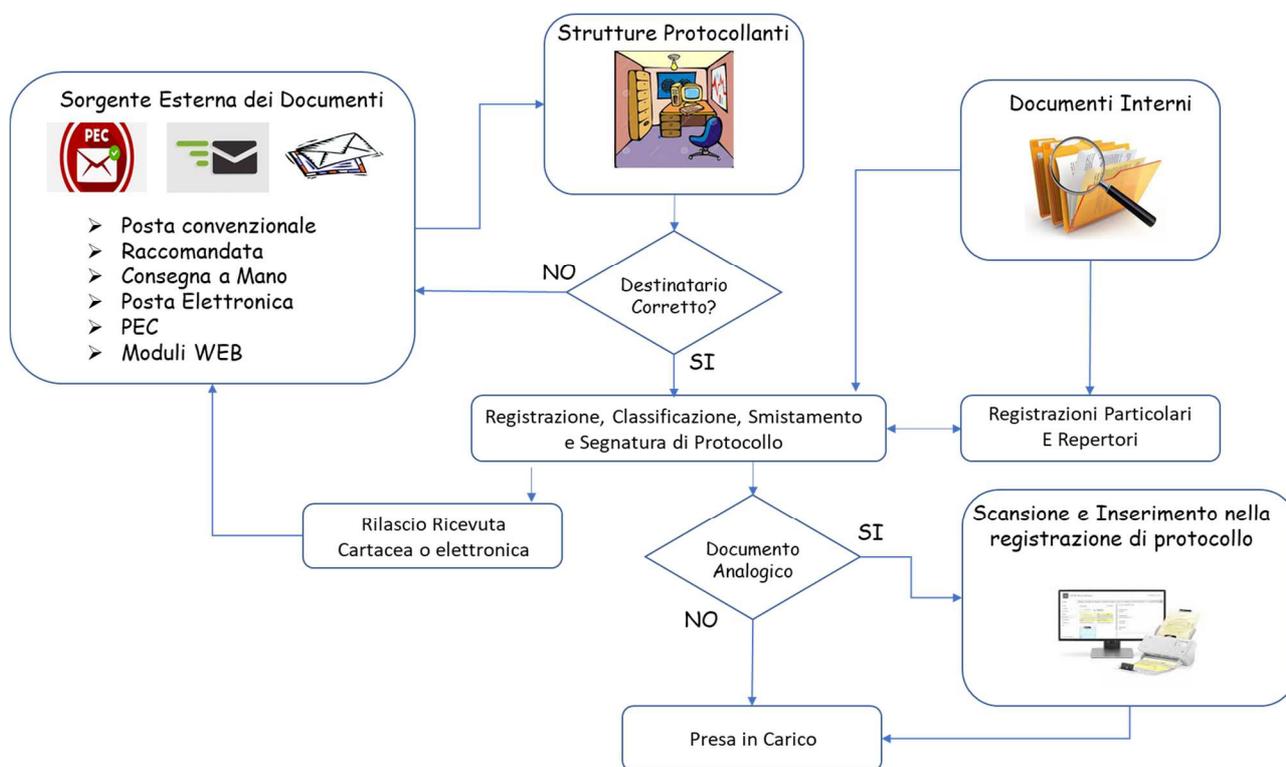
## 4.2 Flussi documentali in entrata

La figura che segue descrive il contesto di riferimento relativo alla gestione dei flussi in entrata individuando l'oggetto documentale da trattare, le strutture organizzative coinvolte ed i canali di pervenimento.



#### 4.2.1 Descrizione del flusso di lavorazione dei documenti in entrata

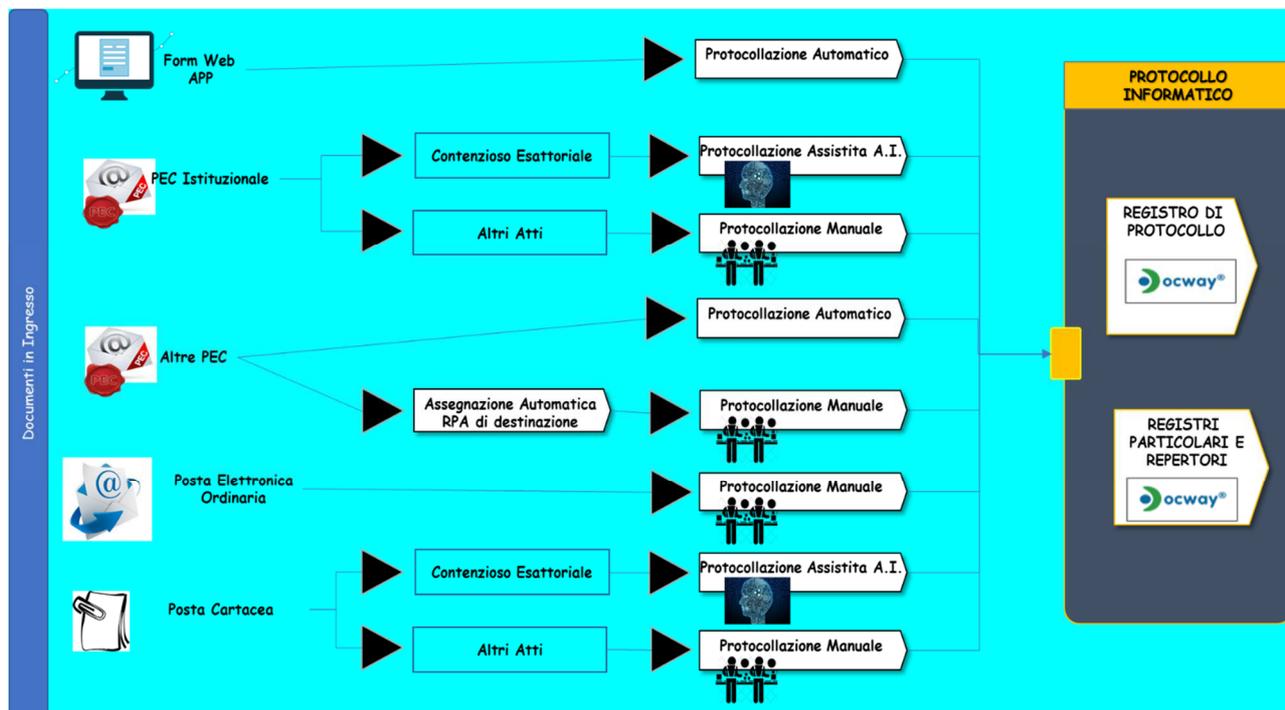
La figura che segue descrive il processo di lavorazione dei documenti in ingresso coprendo l'intero ciclo di lavorazione, dalla ricezione alla conservazione.



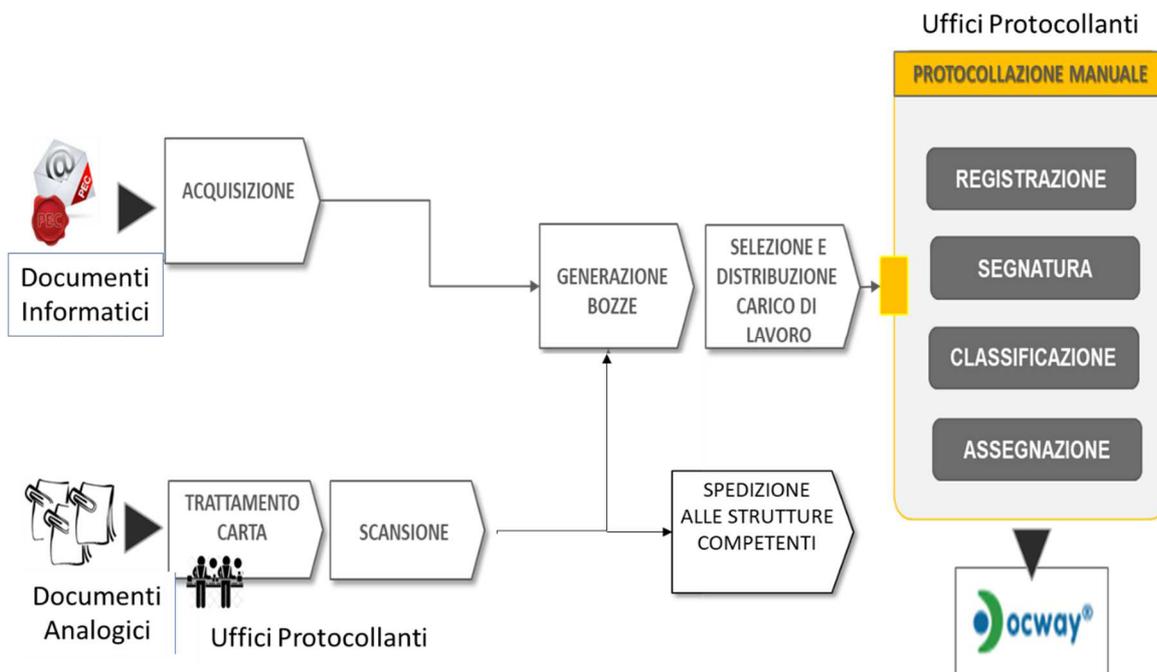
I documenti informatici in arrivo vengono protocollati e assegnati per competenza al RPA; l'informativa dell'assegnazione è resa immediatamente disponibile attraverso un messaggio e-mail che il sistema informatico di protocollazione invia automaticamente alla casella di posta elettronica del RPA.

I documenti in entrata, in funzione del grado di automazione delle diverse classi documentali, possono essere sottoposti, nel rispetto delle regole definite, ad una protocollazione con modalità:

- Manuale;
- Automatica;
- Assistita da sistemi di intelligenza artificiale (I.A.);



Per la **protocollo manuale** il processo è contenuto nello schema a seguire.



Con riferimento ai **documenti analogici**, le principali fasi di lavorazione riguardano:

- **Tattamento carta:**
  - i) **Controllo radiogeno dei plichi cartacei:** conformemente a quanto previsto dal Manuale Unico ADER n. 4 "La Sicurezza", i plichi sono preventivamente sottoposti al controllo radiogeno presso specifici Poli di controllo;
  - ii) **Ricezione e controllo plichi cartacei:** si provvede alla ricezione dei plichi pervenuti presso la sede dell'Ente;
  - iii) **Tracciatura plichi cartacei (per la sede centrale):** si provvede al tracciamento della corrispondenza tramite acquisizione del codice a barre (barcode), apposto dal vettore, sullo specifico applicativo "ancillare" a disposizione dell'Ufficio Protocollo della sede centrale, così da consentire la verifica e quadratura delle distinte di postalizzazione.
- **Scansione documenti cartacei:** i documenti cartacei opportunamente suddivisi in lotti, vengono digitalizzati dagli operatori, per le successive fasi di protocollazione;
- **Spedizione documenti cartacei alle strutture competenti:** successivamente alla fase di scansione i relativi documenti vengono etichettati ed inoltrati agli RPA di competenza;
- **Generazione bozze di protocollo (per la sede centrale):** attraverso procedure automatiche dell'applicativo "ancillare" a disposizione dell'Ufficio Protocollo della sede centrale, vengono generate le bozze di protocollo alle quali sono coerentemente allegati i documenti scansionati.

Con riferimento ai **documenti informatici**, le principali fasi di lavorazione riguardano:

- **Acquisizione:** ricezione attraverso canali telematici (PEC dell'Ente) dei documenti informatici;
- **Generazione bozze di protocollo:** i documenti ricevuti vengono elaborati con procedure automatiche generando, come nel caso dei documenti analogici, le bozze di protocollo.

A seguire si procede con la finalizzazione della protocollazione, ovvero con la **registrazione, segnatura, classificazione ed assegnazione** del documento, come specificato nei paragrafi precedenti.

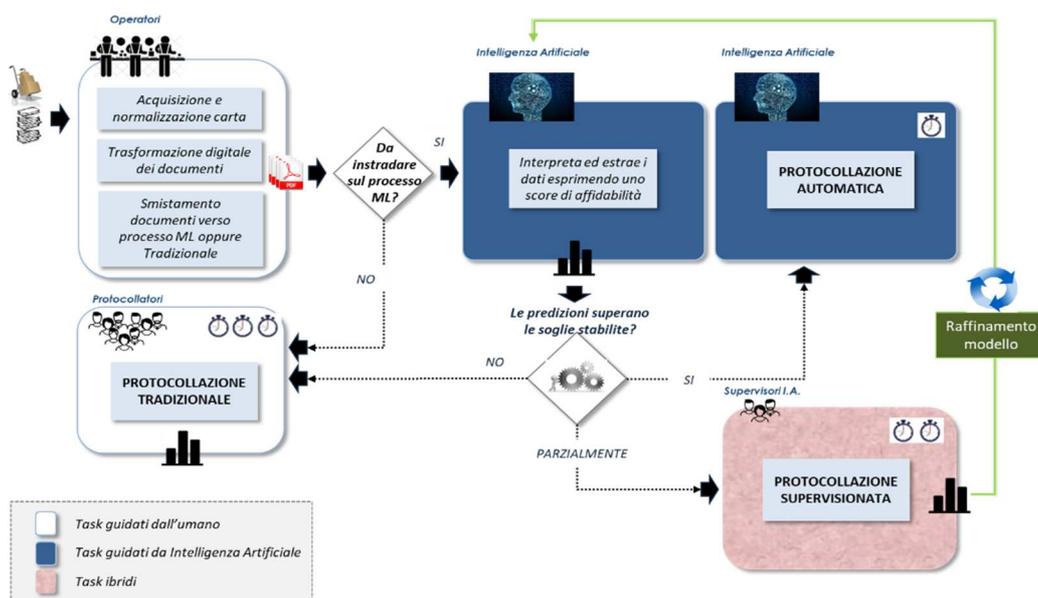
Per alcuni procedimenti amministrativi, con documenti in ingresso ricevuti via PEC a specifici indirizzi basati su istanze standardizzate nel formato e nel contenuto è stata implementata la **protocollazione automatica**. A titolo esemplificativo, tale modalità di protocollazione è stata attivata per le istanze di rateizzazione, le istanze di adesione agli istituti agevolativi (es. definizione agevolata, saldo e stralcio) e le istanze di accesso agli atti. La protocollazione

automatica garantisce il rispetto di tutti i requisiti di sicurezza e di riservatezza nonché di quelli essenziali di gestione dei documenti informatici (immodificabilità, etc.) previsti dalle norme vigenti.

Oltre alla protocollazione manuale e automatica, l'Ente ha attivato e sta progressivamente estendendo modalità innovative di protocollazione **assistite da un sistema di intelligenza artificiale**. Tale sistema permette di incrementare la capacità di protocollazione dell'Ente, in termini di quantità, tempestività e correttezza, nonché di controllo della protocollazione. I paradigmi caratterizzanti il sistema sono basati:

- sulla conoscenza (Knowledge Management System): codifica a mano di grammatiche e lessici da parte di esperti;
- sull'apprendimento automatico supervisionato (Machine Learning): addestramento con modelli statistici su grandi quantità di dati, annotati o non annotati (testi originali o arricchiti con informazioni linguistiche a diversi livelli: categorie morfologiche, sintattiche, semantiche, etc.).

Il sistema, attraverso la conoscenza acquisita, consente di individuare all'interno di ciascun documento le informazioni (in toto o in quota parte) necessarie per la classificazione, l'assegnazione, la protocollazione (con eventuale repertoriamento) del documento stesso. Il ricorso all'intelligenza artificiale permette di **modulare il livello di automazione** della protocollazione, integrando quindi percorsi di lavorazione alternativi, in virtù dei risultati (ovvero dell'accettabilità delle «predizioni») prodotti dal modello di Machine Learning.



In caso di **ricezione di e-mail**, solo laddove sia valutata la necessità di procedere alla relativa protocollazione (cfr. par. 3.1.11), il corpo della mail e l'eventuale documento allegato alla stessa vanno trasformati in file con formato PDF/a (mediante PDF creator) e allegati al protocollo da assegnare all'RPA competente, che verifica la provenienza della mail e valuta se accettare o meno la firma elettronica leggera.

Gli indirizzi di **posta elettronica certificata (PEC)** utilizzati dall'Ente in ricezioni sono collegati al sistema informatico di protocollazione (Docway), al fine di permettere la generazione a sistema delle bozze di protocollo, da finalizzare a cura delle strutture protocollanti ovvero dalla struttura owner della PEC (titolare).

Il sistema di gestione documentale acquisisce tutte le ricevute (file a corredo del messaggio PEC ricevuto) previste dalla normativa in materia di posta elettronica certificata. La verifica della validità della firma digitale è a cura del RPA del documento. Il documento allegato alla PEC, indipendentemente dal formato (anche non PDF o PDF/a) e dalla presenza della firma digitale, viene registrato in allegato al protocollo.

In caso di ricezione di documenti mediante **consegna "brevi manu"** va rilasciata, se richiesta, una ricevuta con le informazioni sul protocollo acquisito (data, numero, ecc.). Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento consegnato "brevi manu", l'ufficio ricevente rilascia al mittente una ricevuta di consegna (anche apponendo timbro di ricevuta sulla fotocopia della prima pagina del documento), fermo restando l'eventuale successivo rilascio al mittente (ad es. tramite invio informatico - e-mail, etc.) delle informazioni di protocollo.

I documenti digitali non possono di norma pervenire all'Ente su **supporti rimovibili**; in caso di esigenze specifiche o a fronte di documenti comunque pervenuti con tale modalità va coinvolto il Responsabile della gestione documentale, prima di procedere all'acquisizione sui sistemi dell'Ente dei documenti.

Qualora pervengano erroneamente all'Ente documenti indirizzati a soggetti diversi dall'Ente, gli stessi dovranno essere restituiti al mittente secondo le seguenti modalità:

- per i documenti informatici pervenuti a mezzo PEC/PEL, l'operatore di protocollo rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore – non di competenza di questo Ente" protocollandolo sia in entrata che in uscita;
- per i documenti cartacei, il relativo plico viene restituito ai servizi postali. Se il plico viene aperto per errore, il documento è protocollato sia in entrata che in uscita inserendo nel campo oggetto la dicitura tipo "documento pervenuto per errore".

#### 4.2.2 Modalità operative di registrazione sul sistema di protocollo

Per procedere alla protocollazione dei documenti in entrata l'addetto al protocollo accede al sistema di protocollo.

In particolare, deve:

- a) accedere dal Menu principale nella scheda di protocollazione in Entrata;
- b) ai fini della registrazione del documento, compilare i campi obbligatori, utilizzando – laddove previsto – le relative voci di indice;
- c) al fine di una corretta identificazione del documento, inserire nel campo “oggetto”, oltre a quanto riportato nel documento in originale, ogni altro elemento utile (es., ove presente, il codice fiscale del mittente, autorità Giudiziaria, ecc.);
- d) effettuare una accurata verifica della tipologia del documento pervenuto ai fini della classificazione dello stesso all'interno del Titolare;
- e) assegnare la responsabilità del documento al RPA della struttura competente;
- f) accertarsi che sia selezionato il flag di invio della e-mail di notifica;
- g) inserire eventuali note (campo non obbligatorio);
- h) se documento analogico, inserire la scansione del documento con l'apposita segnatura del numero di protocollo;
- i) inserire le informazioni relative ai repertori, laddove richiesto.

Gli RPA e le rispettive strutture devono costantemente monitorare l'eventuale assegnazione di documenti protocollati in entrata, indipendentemente dalla ricezione dell'e-mail di notifica.

Se viene assegnato un documento non di propria competenza, il relativo RPA, qualora conosca l'esatta individuazione della struttura competente, deve procedere, direttamente, alla relativa assegnazione avendo cura di:

- usando il tasto funzione “Annotazione”, inserire nell'apposito spazio le motivazioni del rigetto e indicare la struttura competente alla trattazione del documento;
- usare il tasto funzione “Nuovo RPA” e inserire il nominativo.

In tal modo, il documento protocollato viene automaticamente assegnato al nuovo RPA competente per l'espletamento dei successivi adempimenti.

Qualora, invece, il RPA competente non sia conosciuto, si deve utilizzare la funzione “Rigetta” unitamente alla esplicazione puntuale delle motivazioni nel campo “Annotazioni”. In tal caso il documento protocollato viene automaticamente restituito

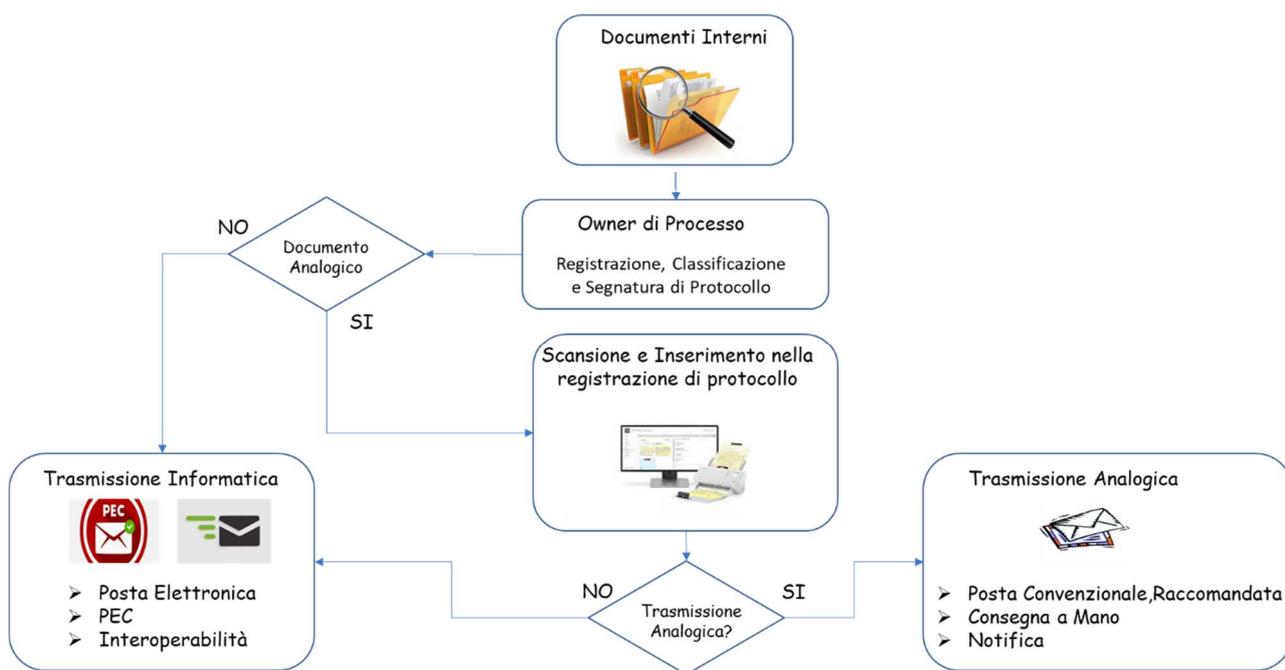
all'Operatore di Protocollo che, a sua volta, anche sulla base delle indicazioni ricevute nell'annotazione, provvede a riassegnare correttamente il documento protocollato al competente RPA per l'espletamento dei relativi adempimenti.

Se, inoltre il RPA ritiene necessario l'interessamento di ulteriori Responsabili, lo stesso dovrà utilizzare la funzione "conferenza di servizi".

Se, infine il RPA ritiene necessario l'interessamento di ulteriori Responsabili e/o risorse solo per opportuna informazione, lo stesso RPA dovrà, usando il tasto funzione "nuovo cc", inserire i nominativi dei relativi RPA/Risorse.

### 4.3 Flussi documentali in uscita

Le comunicazioni verso l'esterno avvengono sia attraverso i canali analogici che informatici, le comunicazioni verso le altre Pubbliche Amministrazioni avvengono di norma mediante l'uso dei canali informatici.



Ogni singola struttura dell'Ente è autorizzata a svolgere attività di registrazione di protocollo per la corrispondenza in uscita di competenza. Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dalle singole strutture.

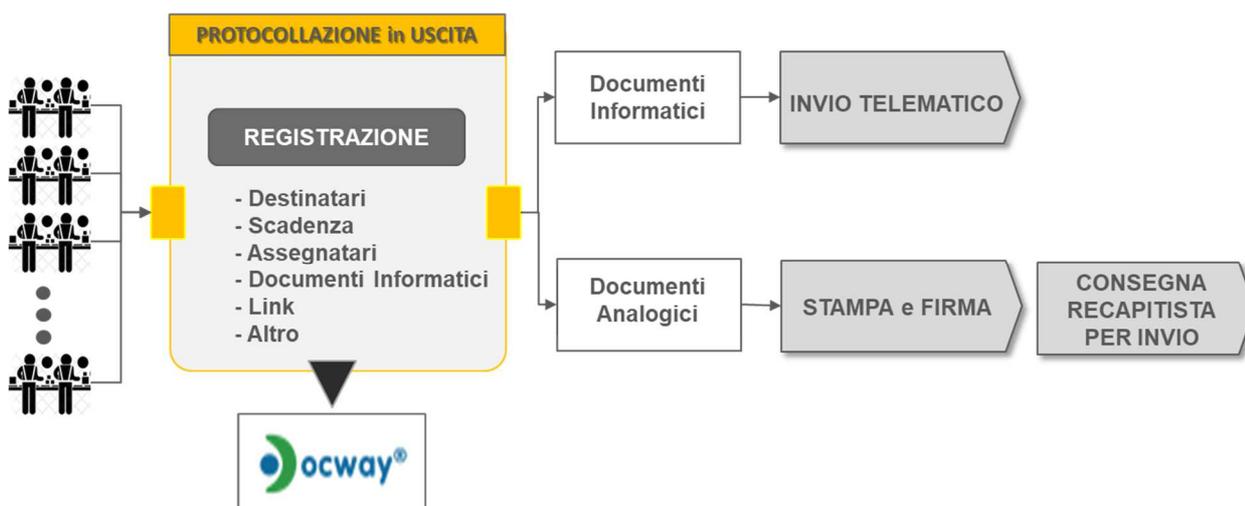
Per procedere alla protocollazione dei documenti in partenza ed assicurarne pertanto la successiva gestione degli stessi, è necessario accedere al sistema di protocollo. In particolare:

- accedere dal Menu principale alla scheda di protocollazione in partenza;
- ai fini della registrazione del documento, compilare i campi obbligatori;
- effettuare una accurata classificazione sulla base del Piano di Classificazione (Titolario);
- assegnare la responsabilità del documento al Responsabile (RPA) della struttura che ha la gestione dello stesso;
- accertarsi che sia selezionato il flag di invio della e-mail di notifica;
- inserire eventuali note (campo non obbligatorio);
- nel caso di documento cartaceo inserire la scansione del documento con l'apposita segnatura del numero di protocollo.

Le informazioni che devono essere valorizzate, sia per i documenti analogici che per quelli informatici, in sede di protocollazione in uscita riguardano le seguenti sezioni:

- il destinatario;
- la scadenza;
- gli assegnatari;
- i documenti informatici;
- gli eventuali link;
- eventuali ulteriori informazioni (Note).

La figura che segue schematizza ed esemplifica il relativo processo.



Il canale preferenziale ai fini dell'invio del documento in partenza è la PEC. Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla normativa vigente.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO). Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al D.P.R. n. 68/2005, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.

Gli incaricati alla trasmissione, anche in via telematica, di atti, dati e documenti sono comunque tenuti al rispetto degli obblighi di riservatezza dell'Ente.

Il protocollo informatico consente la configurazione delle caselle di posta elettronica certificata della AOO e quelle funzionali delle singole UOR, al fine di inviare attraverso il canale telematico i documenti protocollati in partenza e pre-indirizzare nel sistema di protocollo le comunicazioni in ingresso da protocollare in arrivo.

Perché l'invio telematico dei documenti in partenza vada a buon fine è necessario che l'indirizzo PEC dichiarato dai destinatari sia censito e registrato nella relativa anagrafica del protocollo informatico. Pertanto, nel caso in cui il destinatario non sia censito, si deve procedere alla preventiva registrazione dei dati del destinatario e della relativa PEC.

Se l'invio è relativo a documenti analogici, le singole strutture trasmettono all'ufficio addetto allo smistamento della posta abilitato alla spedizione "fisica" il documento in partenza, di norma il giorno lavorativo in cui è stato protocollato.

La struttura addetta allo smistamento della posta provvede alle operazioni necessarie per l'invio della corrispondenza in partenza, secondo i servizi e le modalità previste dall'Ente.

Per le copie dei documenti di riscossione e per gli output prodotti dagli applicativi e dai sistemi informativi dell'Ente consegnati al contribuente allo sportello ovvero tramite recapito PEL dallo stesso indicato non è necessaria la protocollazione sul sistema Docway, fatte salve le eventuali specifiche previsioni contenute nella normativa interna dell'Ente.

#### 4.4 Flussi documentali interni alla AOO

La trasmissione fra UOR di documenti informatici può avvenire o meno tramite il protocollo informatico in funzione del valore e della rilevanza dello stesso determinata dal mittente. Non sono oggetto di protocollazione interna i documenti ad esclusivo uso interno e che non abbiano rilevanza giuridica (quali ad esempio bozze di documenti in lavorazione, e-mail interne, ecc.).

In caso di protocollazione, il documento è registrato nel sistema come protocollo interno e viene trasmesso alla UOR destinataria tramite la funzione di assegnazione; non deve, pertanto, essere registrato dalla UOR destinataria.

La registrazione di un documento interno si compone infatti di una parte relativa alla MINUTA e di una parte relativa all'ORIGINALE come riportato nella figura che segue. Nella sezione "DATI DEL DOCUMENTO" la registrazione dei metadati è dettata dalle regole di assegnazione della responsabilità, ovvero:

- il **MITTENTE** del documento è responsabile della minuta; ha l'obbligo di compilare i campi relativi alla minuta ma non quelli relativi all'originale;
- il **DESTINATARIO** del documento è responsabile dell'originale e deve provvedere alla compilazione dei relativi dati.

Restano invariate le altre sezioni relative alla scadenza, ai documenti informatici, ai link ed altro.



## 5. SISTEMA DI GESTIONE DOCUMENTALE

Il sistema di gestione documentale è l'insieme di tutte le componenti logiche e fisiche a supporto degli utenti per lo svolgimento delle loro attività sia dal punto di vista di gestione ed erogazione del servizio che di fruizione dello stesso. Nel seguito, si evidenziano le componenti applicative che caratterizzano il sistema nel suo complesso.

### 5.1 Componenti del sistema di gestione documentale

Oltre al Protocollo Informatico, il sistema di gestione documentale dell'Ente è rappresentato da una serie di componenti applicative che si sono evolute nel tempo per garantire la gestione di tutti i documenti e la loro conformità alle specifiche norme di settore. Di seguito sono riportate le principali componenti applicative che costituiscono il sistema di gestione documentale dell'Ente, volte a produrre, protocollare, archiviare o conservare i documenti.

<b>Componente applicativa</b>	<b>Processo/funzioni</b>
Docway (Protocollo Informatico)	<p>Costituisce il sistema di protocollo informatico del sistema di gestione documentale, secondo le norme vigenti. In Docway vengono protocollati i documenti in ingresso, sia analogici (presso gli sportelli o via posta) che informatici (via PEC/posta elettronica ordinaria o tramite form web), in uscita e tra le strutture dell'Ente. Inoltre, l'applicativo assolve, per i documenti protocollati, anche le funzioni di archivio corrente e di archivio di deposito. Il sistema permette, tra l'altro, la produzione del registro giornaliero di protocollo.</p> <p>Tramite applicativo "ancillare" vengono predisposti per la protocollazione i documenti analogici che pervengono alla sede centrale dell'Ente.</p>
Infrastruttura PEC	<p>È l'infrastruttura per l'invio tramite PEC dei documenti esattoriali prodotti in modalità "massiva centralizzata", nei casi previsti dalla normativa di riscossione. L'infrastruttura assume anche le funzioni di registro particolare, di archivio corrente e di deposito per le PEC e per le relative ricevute complete (inclusive dei documenti),</p>

	<p>sia per quelle inviate tramite Infrastruttura PEC che tramite IPOL, con funzionalità a disposizione degli utenti per la ricerca dei documenti.</p>
IPOL (Invio PEC On-Line)	<p>È l'infrastruttura per l'invio tramite PEC di documenti, sia esattoriali che di altra natura, prodotti in modalità non "massiva centralizzata" da parte delle Strutture regionali o centrali. IPOL è connesso ed utilizza i servizi di Infrastruttura PEC, in particolare per l'archiviazione delle PEC inviate.</p>
Open CMS	<p>È il componente utilizzato per l'interazione sul web da parte di contribuenti/enti, ai fini della produzione e trasmissione all'Ente di documenti di richiesta/istanza, ecc.. Con tale componente sono pubblicati i form web a disposizione dei soggetti terzi.</p>
Servizi web Enti (Informatizzazione)	<p>È la piattaforma informatica web attraverso la quale viene resa possibile l'interazione diretta e digitale tra l'Ente e gli Enti impositori per i servizi erogati agli stessi, quali la produzione dei frontespizi digitali (tramite il sistema Frontespizio Ruoli) e l'acquisizione di minute e provvedimenti.</p>
Sistema informativo della riscossione	<p>Contiene i dati relativi ai contribuenti e agli enti che sono utilizzati per la produzione dei documenti di riscossione. Il sistema è costituito principalmente dagli applicativi SET, COATTIVO e LAMPO.</p>
Piattaforme di elaborazione documenti (CSF, PCS, ecc.)	<p>Tali Piattaforme consentono la produzione in modalità massiva accentrata dei documenti esattoriali (cartelle, piani di rateizzazione, altri atti), sulla base delle informazioni presenti nel Sistema informativo della riscossione. I file predisposti vengono, in relazione alle modalità di notifica previste dalla normativa di riscossione, destinati:</p> <ul style="list-style-type: none"> <li>• alla stampa per l'invio a mezzo posta (raccomandata A/R) ovvero messo notificatore (documenti analogici);</li> <li>• all'invio tramite PEC (documenti informatici).</li> </ul>
GEDO (Gestione Documenti Ottici)	<p>È la banca dati che contiene i file delle immagini di alcuni documenti dell'Ente (quali notifiche effettuate a livello locale tramite messo interno, ecc.).</p>

	<p>La banca dati è alimentata dalle strutture dell'Ente, regionali e centrali, mediante processo <b>puntuale</b> eseguito online (con data entry da parte degli utenti dei metadati e caricamento della relativa immagine) ovvero <b>massivo</b> eseguito offline. Il componente consente agli utenti abilitati anche la visualizzazione, la ricerca e la stampa dei file.</p>
Portale Immagini	<p>È la banca dati centralizzata che contiene i file con le immagini dei documenti prodotti nei processi di notifica tramite raccomandata A/R e tramite messo esterno.</p> <p>L'applicativo consente agli utenti abilitati la consultazione e la visualizzazione <i>on line</i> delle immagini delle cartoline di raccomandata A/R (per le notifiche tramite raccomandata) e dei documenti della notifica tramite messo (Relata di Notifica, Busta Atto, Certificato Anagrafico/Camerale, Distinta Postalizzazione, A/R ex art.140 c.p.c./Plico Mancato Recapito, Elenco di Affissione ex art.60 del D.P.R. 600/1973/Elenco di Deposito ex art.140 c.p.c.), nonché la richiesta dell'originale.</p>
Documenti Web	<p>È un componente che consente di memorizzare in un archivio corrente alcune tipologie di documenti esattoriali (Cartelle, Entrate patrimoniali e GIA). Il componente è dedicato all'archiviazione e alla consultazione dei documenti prodotti in via massiva dall'Ente.</p>
Piattaforma Conti di Gestione	<p>È il componente attraverso il quale sono generati, sulla base delle informazioni presenti nel sistema informativo della riscossione, i conti di gestione.</p>
ERP-AX	<p>È il sistema ERP dell'Ente che permette anche la produzione di documenti contabili (registri civilistici e fiscali, ...). Nell'ambito del sistema di gestione documentale contiene in particolare i dati dei flussi telematici relativi al processo di fatturazione elettronica.</p>
Piattaforma di Interscambio (Service notifica)	<p>È l'infrastruttura che consente lo scambio, in modalità massiva, di documenti/dati tra l'Ente ed i soggetti terzi incaricati della stampa e della notifica o spedizione degli atti esattoriali. L'infrastruttura quindi supporta:</p>

	<ul style="list-style-type: none"> <li>• la trasmissione ai service dei documenti da stampare, imbustare e recapitare ai contribuenti;</li> <li>• l'acquisizione degli esiti delle operazioni e i file immagine delle relate di notifica/ricevute di ritorno delle raccomandate, depositati poi nei sottosistemi di archiviazione/consultazione.</li> </ul>
Firma Digitale	<p>È il componente che consente di apporre la firma digitale sui documenti informatici prodotti dall'Ente. In relazione alla tipologia di documento e alla modalità di produzione sono previste diverse modalità di firma digitale (con dispositivo fisico OTP o CNS, HSM automatica massiva, HSM remota). Per la firma HSM (High Secure Module) effettuata in modalità massiva e remota il componente utilizzato è COSIGN.</p>
GEA (Gestione Archivi)	<p>È il componente che supporta l'invio all'archivio di deposito (Centro di Gestione Documentale), da parte delle strutture regionali e centrali dell'Ente, dei documenti analogici; include le funzionalità per la gestione delle richieste di copie digitali e di originali dei documenti da parte degli utenti.</p>
SIRFIN	<p>È il sistema di gestione amministrativa del personale dipendente dell'Ente. Il sistema produce e archivia i documenti connessi all'amministrazione del personale (tra cui il Libro Unico del Lavoro).</p>
Cassetto Documentale, Fascicolo del contribuente e Scrivania di sportello	<p>Sono componenti che permettono agli utenti abilitati, anche tramite l'applicativo Scrivania di sportello, la:</p> <ul style="list-style-type: none"> <li>• consultazione on-line di alcuni documenti esattoriali (cartelle di pagamento, avvisi d'intimazione, ...) prodotti centralmente in un arco temporale delimitato e organizzati per codice fiscale del Contribuente (Cassetto Documentale)</li> <li>• visione complessiva della situazione di un contribuente con evidenza degli atti emessi e possibilità di recupero dei documenti di notifica (collegamento con Portale Immagini, GEDO, ...)</li> </ul>
Time Archive	<p>È il componente dedicato alla conservazione (quale archivio di deposito e storico) dei documenti informatici.</p>

Per ciascun componente l'Ente adotta specifici manuali operativi o Documenti Tecnico-Operativi (DTO) che dettagliano le funzionalità previste e le pratiche di utilizzo degli strumenti a supporto della realizzazione dei processi operativi.

## 5.2 Archivi analogici

### 5.2.1 Premessa

I documenti in corso di lavorazione sono riposti nel mobilio (scrivania, cassetiera, armadio, ecc.) in dotazione all'ufficio assegnato a ciascun dipendente. L'ufficio o il mobilio in cui sono riposti i documenti contenenti dati personali devono, in relazione ai rischi connessi alla violazione dei dati trattati, essere resi non accessibili a soggetti (interni o esterni) non autorizzati al trattamento dei dati contenuti, di norma mediante chiusura a chiave. Le chiavi sono affidate ai singoli utilizzatori o al Responsabile della struttura organizzativa di riferimento.

L'Ente per l'archiviazione dei documenti analogici prevede un sistema diffuso di archivi correnti sul territorio nazionale, ad uso delle Direzioni Centrali e delle Direzioni Regionali, nei quali vanno conservati, fino al trasferimento nell'archivio di deposito, i documenti che non sono più in corso di lavorazione o necessari per le successive fasi.

L'Ente si è dotato di un unico archivio di deposito, che svolge anche le funzioni di archivio storico, ove occorra.

### 5.2.2 Archivi correnti

I locali dedicati ad archivio corrente dei documenti delle diverse strutture organizzative dell'Ente sono individuati e allestiti, con riferimento a ciascuna sede, dal Settore Logistica, Infrastrutture e Security della Direzione Approvvigionamenti e Logistica.

Alle Direzioni Centrali e alla Direzione Regionale Lazio sono invece assegnati gli archivi correnti ubicati nella sede di Via Grezar 14, Roma.

I documenti da archiviare presso gli archivi correnti sono raccolti in faldoni e in scatole, e sono indicizzati, in modo che siano reperibili per la consultazione, sia nel periodo di loro giacenza presso l'archivio corrente che dopo il loro trasferimento all'archivio di deposito.

Per taluni documenti analogici l'Ente prevede che, prima dell'archiviazione, si proceda alla scansione degli stessi e al caricamento delle relative immagini nei sistemi di archiviazione informatica.

Restano ferme le specifiche previsioni previste dai contratti di servizi di notifica e recapito o le modalità di archiviazione di determinate tipologie di documenti, in quanto oggetto di specifica disciplina dell'Ente.

Le strutture responsabili delle attività, ai quali i documenti sono sottesi, hanno la diretta responsabilità del trasferimento degli stessi, non appena ne ricorrano i presupposti, all'archivio corrente nonché di attivare il relativo trasferimento all'archivio di deposito.

Gli archivi correnti presenti nelle sedi dell'Ente sono presidiati dalle strutture qualificate come "referente per la sicurezza della sede" in cui il locale è situato, in particolare quando la documentazione contenuta è riferibile a più strutture presenti nella sede. Tali strutture:

- presidiano gli accessi agli archivi, anche mediante – ove valutato opportuno – l'utilizzo di un registro dedicato;
- verificano che vi sia un uso appropriato della documentazione archiviata a cui viene consentito l'accesso;
- monitorano la capienza degli archivi (anche rispetto alla capienza massima consentita dalla normativa di riferimento) e la funzionalità dei dispositivi di sicurezza previsti;
- coordinare i trasferimenti dei documenti all'archivio di deposito dell'Ente.

**Archivio di Deposito** Le strutture responsabili delle attività, ai quali i documenti sono sottesi, sono deputate, sotto la supervisione della struttura referente, a posizionare i faldoni da archiviare negli archivi correnti e a prelevare e riposizionare gli stessi, laddove necessario.

Gli archivi correnti sono accessibili unicamente mediante chiave (o badge), conservata dalla struttura referente.

L'Ente ha anche la gestione in outsourcing, presso la Sikeliarchivi, dell'archiviazione dei documenti analogici della ex-Riscossione Sicilia S.p.A., presso via XVI Strada Giuseppina Virlinzi 70/74 - Catania (CT), assorbita dal 1° ottobre 2021 in Agenzia delle entrate-Riscossione, per effetto dell'art. 76 del D.L. n. 73/2021, convertito con L. n. 106/2021.

### 5.2.3 Archivio di deposito e storico

L'Archivio di deposito dell'Ente è il Centro di Gestione Documentale (CGD) sito in Roma, Via Osvaldo Licini, n. 12.

Per il trasferimento delle scatole, contenenti i faldoni, all'archivio di deposito viene applicata una codifica univoca prodotta dall'applicativo GeA. Il dettaglio delle modalità

di trasferimento dei documenti all'archivio di deposito è descritto nella normativa interna dell'Ente.

Il Settore Gestione Documentale e Protocollo assicura che le scatole trasferite presso l'archivio di deposito siano archiviate nelle apposite celle dell'archivio, registrandone l'ubicazione nell'applicativo GeA, per consentirne il successivo reperimento. Il prelievo delle scatole o dei faldoni ed il loro riposizionamento avviene sempre con il supporto dell'applicativo GeA, che ne registra le movimentazioni.

L'accesso al Centro di Gestione Documentale è garantito da un apposito servizio di guardiania. L'accesso dei dipendenti dell'Ente viene altresì monitorato tramite il sistema di controllo presenze. L'accesso del personale delle imprese addette a servizi di facchinaggio, trasporto e spedizione, gestione archivi, pulizie, manutenzione impianti ed immobili, ecc. è registrato su appositi registri ed è comunque vietato l'accesso ai locali adibiti ad archivio per il personale non autorizzato, incluso quello addetto ai servizi di trasporto e spedizione. Gli archivi del CGD sono dotati delle necessarie misure di sicurezza in ragione dei volumi di documenti archiviati, quali:

- Impianto antincendio – rilevazione fumi;
- Impianto di videosorveglianza;
- Impianto di areazione.

Il perimetro dell'archivio di deposito è recintato ed è dotato di impianti antintrusione.

L'estrazione dei documenti archiviati è limitata ai soli casi in cui ne sia ravvisata l'esigenza da parte delle strutture dell'Ente responsabili per tipologia di documenti. Le richieste di documenti in copia o in originale, ed i relativi riscontri, sono gestiti e tracciati tramite l'applicativo GeA.

I documenti contenenti particolari categorie di dati personali sono gestiti assicurando che l'accesso alle informazioni sia limitato alle sole strutture responsabili.

Il Settore Protocollo e Gestione Documentale assicura che le attività di ricerca e produzione di documenti avvenga nel rispetto della normativa interna dell'Ente e monitora le attività di restituzione dei documenti in originale richiesti, assicurandone il riposizionamento nella medesima ubicazione originaria, tramite l'applicativo GeA.

Il medesimo archivio è altresì dedicato ad archivio storico, per determinate tipologie di documenti.

## 6. PIANO DELLA SICUREZZA

### 6.1 Premessa

Il **Piano della sicurezza** del sistema di gestione informatica dei documenti è costituito dalle misure organizzative e tecniche adottate dall'Ente per garantire, tempo per tempo, un livello di sicurezza dei documenti adeguato alle esigenze di funzionamento dello stesso e il rispetto della normativa esterna di riferimento, quali ad esempio le misure minime di sicurezza ICT emanate dall'AgID (Circolare del 18 aprile 2017, n. 2/2017) e le disposizioni in tema di protezione dei dati personali (Regolamento Europeo n. 679/2016).

L'obiettivo del Piano è quello di garantire che i documenti e le informazioni, inclusi i relativi dati personali, gestiti dall'Ente siano disponibili, integri e riservati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il Piano della sicurezza della gestione documentale si inserisce nel più ampio quadro delle misure organizzative e tecniche di sicurezza informatica e fisica adottate da Agenzia delle entrate-Riscossione, attraverso i presidi organizzativi specificamente dedicati alla sicurezza e mediante la regolamentazione interna dei relativi processi di gestione.

### 6.2 Principali misure organizzative di sicurezza

L'Ente presidia i rischi connessi alla sicurezza attraverso le figure istituzionali di compliance (Responsabile della gestione documentale, Responsabile della conservazione, Responsabile della protezione dei dati - DPO, Responsabile Transizione Digitale, ecc.) e le strutture centrali di governance (Internal Audit, Legale, ecc.). Inoltre, sono istituite strutture organizzative con responsabilità diretta e presidi costanti sulla gestione della sicurezza (cybernetica e fisica):

- nell'ambito della **Direzione Tecnologie e Innovazione**, per la sicurezza degli archivi digitali e dei flussi documentali dei documenti informatici;
- nell'ambito della **Direzione Approvvigionamenti e Logistica** e della **Direzione Produzione Ruoli e Gestione Documentale**, per la sicurezza fisica degli archivi e dei flussi documentali dei documenti analogici.

L'Ente inoltre si è dotato di un **Sistema di gestione della sicurezza delle informazioni (SGSI)**, rispondente alla norma internazionale ISO 27001, e di un **Sistema di gestione della protezione dei dati personali (SGPD)**, per il presidio e la salvaguardia dei diritti degli interessati, nel trattamento dei dati personali, in riferimento alle prescrizioni e agli adempimenti previsti nel Regolamento Europeo sulla protezione dei dati 679/2016 (GDPR). Tale impostazione permette quindi l'adozione di approcci, coerenti agli standard metodologici di riferimento, basati sulla valutazione dei rischi al fine di orientare efficacemente le azioni di risposta alle minacce.

Le strutture dedicate alla sicurezza informatica peraltro collaborano e interagiscono, attraverso il NAIT (Nucleo Accreditato IT) interno all'Ente, con gli enti nazionali deputati alla sicurezza per il tramite del CERT-MEF, sia nell'ambito della "struttura di governo" che in quello del "Nucleo Tattico Operativo". Tali strutture presidiano tutti i processi di gestione della sicurezza, sia in logica proattiva che reattiva, curando l'attuazione delle misure di sicurezza previste (quali la gestione degli incidenti di sicurezza, la gestione degli amministratori di sistema, la protezione della configurazione dei dispositivi, la gestione delle copie di sicurezza, l'inventariazione dell'hw e del sw, il patching dei sistemi, le difese contro i malware, la valutazione e la correzione delle vulnerabilità, la protezione delle reti, il controllo degli accessi fisici/logici, ecc..

Per gli aspetti che regolano i comportamenti dei dipendenti l'Ente ha adottato, quale misura generale di sicurezza, il "**Disciplinare per l'utilizzo degli strumenti elettronici, per gli accessi alle risorse e ai dati di AER**" che contiene le regole e le indicazioni di riferimento a cui ciascun dipendente deve attenersi per l'uso degli strumenti tecnologici (informatici e di comunicazione) al fine di contenere i connessi rischi di sicurezza informatica e di protezione dei dati personali.

Le misure richiamate sono naturalmente nel quadro regolamentare e nel sistema di controllo dell'Ente, costituito, tra l'altro, dal Codice etico, dal Codice Disciplinare, dal Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. n. 231/2001 e dal Piano triennale di prevenzione della corruzione e della trasparenza ai sensi della L. n. 190/2012.

### 6.3 Principali misure tecniche di sicurezza

L'**assegnazione/revoca dei profili abilitativi** (insieme di autorizzazioni ad operare su un determinato applicativo o parte di esso e relative funzionalità disponibili) all'utilizzo degli applicativi informatici ricompresi nel sistema di gestione documentale si basa su un sistema di Identity Governance & Intelligence (IGI), nell'ambito del quale, per ciascun applicativo,

L'Ente definisce il Catalogo dei profili, con previsione delle strutture organizzative per le quali è prevista l'attribuzione "standard", la cui assegnazione agli utenti è sottoposta ad un iter approvativo ordinario (mentre per quelle "fuori standard" è necessario un iter approvativo rafforzato). L'assegnazione/revoca dei profili nell'ambito del sistema IGI è gestita per taluni applicativi (incluso il sistema Docway), sempre previo iter autorizzativo, attraverso un processo semi-automatizzato. L'impostazione tiene conto delle attività e dei processi di competenza funzionale di ciascuna struttura organizzativa all'interno dell'Ente, secondo quanto previsto dai documenti organizzativi dello stesso. In particolare, per quanto attiene al Catalogo dei profili del sistema di protocollazione Docway si rinvia a quanto evidenziato in precedenza.

L'**accesso agli applicativi**, per i profili abilitati, prevede l'utilizzo di credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo mobile in uso esclusivo all'utente), definite secondo specifiche policy e regole di sicurezza.

L'**accesso fisico** agli applicativi del sistema di gestione documentale gestiti nel Data Center dell'Ente, ove specificamente motivato e in presenza di personale autorizzato, è ammesso solo a seguito di preventiva autorizzazione e con identificazione (con specifico badge).

Le previsioni di sicurezza per le attività di gestione operativa dei sistemi sono regolamentate nella normativa interna dell'Ente, che disciplina anche il processo di gestione degli incidenti per tutti i sistemi dell'Ente, identificando ruoli e responsabilità degli attori coinvolti e definendo le casistiche, le modalità e le tempistiche di segnalazione degli eventi agli enti interni ed esterni previsti.

Il sistema operativo del Protocollo Informatico utilizzato dall'Ente è conforme alle specifiche previste dalle Linee Guida ai sensi degli articoli 40 bis, 41, 47, 57 bis e 71 del CAD. Il sistema operativo del server che funge da deposito dei documenti è configurato in modo tale da inibire l'accesso agli utenti non autorizzati.

I servizi sono erogati dalle infrastrutture presenti nel Data Center di Roma e sono garantiti da un sito di **Disaster Recovery** (di livello Tier 3) situato presso la sede di Torino.

Le attività di **manutenzione** del sistema di gestione documentale, che prevedono l'intervento del fornitore o le attività di collaudo che interessano utenti esterni all'Ente (qualificati per le verifiche ai fini della certificazione di qualità del sistema), sono gestite dalla Direzione Tecnologie e Innovazione secondo quanto previsto dai contratti in essere e nel rispetto della normativa interna dell'Ente.

Le **registrazioni di sicurezza** (LOG) sono costituite da informazioni (dati o transazioni) presenti o transitate sui componenti del sistema documentale che è opportuno mantenere poiché

possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza. Le registrazioni di sicurezza sono costituite:

- dai log di sistema generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall);
- dalle registrazioni dei singoli componenti.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- I log dei firewall vengono mantenute in linea sul sistema per poi essere copiate e mantenute su nastro;
- I log generati dal sistema operativo e quelli generati dagli applicativi sono soggetti a backup.

Specifiche misure di sicurezza sono adottate per le **operazioni trasmissione** di atti, dati e documenti, volte a garantirne l'integrità, la riservatezza, la protezione dei dati personali (ai sensi del Regolamento Europeo n. 679/2016) e la tutela della proprietà, per tutte le modalità di trasmissione, gli operatori coinvolti (interni e esterni) e i destinatari dei documenti (siano essi quindi privati, altre pubbliche amministrazioni o altre strutture dell'Ente). Al riguardo, in particolare in caso di trasmissione telematica, non è consentito agli operatori non autorizzati di 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, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

### 6.4 Normativa interna

Sul tema della gestione documentale e del presidio della relativa sicurezza, si richiamano, in aggiunta agli elementi di portata generale del sistema di controllo interno dell'Ente (statuto, regolamento di amministrazione, funzionigramma, codice etico, codice disciplinare, Piano triennale prevenzione corruzione e trasparenza ai sensi della L. n. 190/2012, modello di organizzazione, gestione e controllo ai sensi della L. n. 231/2001, ecc.), i principali documenti della normativa interna già vigenti:

- DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI E PER L'ACCESSO ALLE RISORSE E AI DATI DI ADER;

- DOCUMENTI DEL SISTEMA DI GESTIONE DELLA SICUREZZA INFORMATICA (SGSI);
- DOCUMENTI DEL SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI, che include la PROCEDURA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH);
- Circolare ADER n. 12 – INVIO CORRISPONDENZA ESTERNA;
- Circolare ADER n. 24 – POSTA INTERNA E CORRIERE ESPRESSO;
- Circolare ADER n. 39 – MISURE DI SICUREZZA ICT;
- Circolare ADER n. 41 – ASSET MANAGEMENT IGI;
- Circolare ADER n. 44 – ARCHIVIAZIONE DOCUMENTAZIONE CARTACEA PRESSO IL CGD;
- Circolare ADER n. 50 – IMPLEMENTAZIONI SERVIZI ICT;
- Circolare ADER n. 60 – GESTIONE DELLA FIRMA DIGITALE;
- Manuale Unico ADER n. 4 – LA SICUREZZA;
- Documento Tecnico Operativo n. 44 – ISTRUZIONI PER LA VERIFICA DELLA FIRMA DIGITALE;
- Circolare n. 191 – INDICAZIONI AVVIO AGENZIA DELLE ENTRATE-RISCOSSIONE;
- Circolare n. 30 – SERVIZIO DI HELP DESK PER LA GESTIONE UNITARIA DELLE RICHIESTE DI INTERVENTO SUI SERVIZI EROGATI DALLA DIVISIONE SERVIZI ICT E INDICAZIONE DEI RELATIVI CANALI DI CONTATTO;
- Circolare n. 78 – GESTIONE DELLA POSTA ELETTRONICA (PEL), POSTA ELETTRONICA CERTIFICATA (PEC) E RICHIESTA FIRMA DIGITALE;
- Circolare n. 90 – HELP DESK MAAC;
- Procedura n. 30 – MANUTENZIONE CORRETTIVA (MAC).

Inoltre, con specifici Documenti Tecnico Operativi (DTO) o Manuali Operativi sono dettagliate le modalità di utilizzo degli applicativi che compongono il sistema di gestione documentale.

## 7. STORICIZZAZIONE DEL DOCUMENTO

Data pubblicazione	Note	Versione
01/07/2017	Approvato con determinazione del Commissario Straordinario n. 15 del 30 giugno 2017	v.1.0
01/01/2022	Modificato con determinazione del Presidente n. 27 del 21 dicembre 2021, per adeguamento alle Linee guida AGID del 9/9/2020 (modificate il 17/5/2021) in vigore dal 1/1/2022	v.2.0