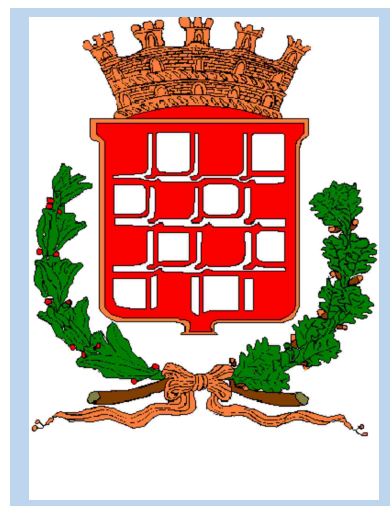


COMUNE DI FERRERE



MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Aggiornato alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022

Registro delle Versioni

N° Versione	Data Emissione	Modifiche apportate	Osservazioni
Versione base	19/01/2026		

INDICE

1 PRINCIPI GENERALI

- 1.1 Premessa
- 1.2 Ambito di applicazione del manuale
- 1.3 Definizioni
- 1.4 Norme di riferimento

2 DOCUMENTI E MODALITA' DI GESTIONE

- 2.1 Il documento informatico
 - 2.1.1 Immodificabilità e integrità del documento informatico
- 2.2 Il documento amministrativo informatico
- 2.3 Il documento analogico – cartaceo amministrativo
- 2.4 Copie per immagine su supporto informatico di documenti analogici
- 2.5 Duplicati, copie ed estratti informatici di documenti informatici
- 2.6 Copia/ estratto analogica di documento informatico
- 2.7 Autenticazione di firma
- 2.8 Timbro digitale
- 2.9 Tipologie di firme elettroniche
 - 2.9.1 La firma elettronica semplice
 - 2.9.2 La firma elettronica avanzata (FEA)
 - 2.9.3 La firma elettronica qualificata (FEQ) e la firma digitale
 - 2.9.4 Il Sigillo elettronico qualificato
- 2.10 Documento in entrata
- 2.11 Documento in uscita
- 2.12 Documento interno formale
- 2.13 Documento interno informale
- 2.14 Trasmissione informatica dei documenti
- 2.15 Uso della Posta Elettronica Certificata
- 2.16 Uso della cooperazione applicativa tra P.A.
- 2.17 Interoperabilità dei sistemi di protocollo informatico

3 ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

3.1 Il protocollo informatico

3.2 Aree Organizzative Omogenee e modelli organizzativi

3.3 Accreditamento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA)

3.4 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico

3.5 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico

3.6 Tutela dei dati personali

3.7 Formazione del personale

4 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

4.1 Generalità

4.2 Flusso dei documenti ricevuti dalla AOO

4.2.1 Ricezione di documenti informatici sulle caselle di posta elettronica certificata

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica tradizionale

4.2.3 Ricezione di documenti informatici tra PA tramite cooperazione applicata

4.2.4 Ricezione di documenti informatici su supporti rimovibili

4.2.5 Ricezione di documenti informatici da portale web dell'Ente

4.2.6 Ricezione di documenti cartacei a mezzo servizio postale, corriere o consegnati a mano

4.2.7 Corrispondenza di particolare rilevanza e documenti esclusi

4.2.8 Errata ricezione di documenti digitali

4.2.9 Errata ricezione di documenti cartacei

4.2.10 Rilascio di ricevute attestanti la ricezione di documenti informatici

4.2.11 Rilascio di ricevute attestanti la ricezione di documenti cartacei

4.2.12 Classificazione, assegnazione e presa in carico dei documenti

4.3 Flusso dei documenti creati e trasmessi dall'Aoo

4.3.1 Sorgente interna dei documenti

4.3.2 Verifica formale dei documenti

4.3.3 Registrazione di protocollo e segnature

4.3.4 Trasmissione di documenti informatici

4.3.5 Trasmissione di documenti cartacei a mezzo posta

4.3.6 Conteggi e spedizione corrispondenza cartacea

4.4 Documenti informali

5 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE DIGITALE E ARCHIVIAZIONE

5.1 Classificazione dei documenti

5.2 La fascicolazione dei documenti

5.3 Processo di assegnazione dei documenti ai fascicoli digitali

5.4 Modifica delle assegnazioni dei fascicoli digitali

5.5 Chiusura dei fascicoli digitali

5.6 Serie archivistiche, repertori e fascicoli

5.7 Archiviazione dei documenti - Tempi, criteri e regole di selezione del sistema di classificazione

5.8 Procedure di scarto

6 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO

6.1 Unicità del protocollo informatico

6.2 Registrazione di protocollo

6.3 Elementi facoltativi delle registrazioni di protocollo

6.4 Segnatura di protocollo dei documenti

6.5 Annullamento delle registrazioni di protocollo

6.6 Protocollazione documenti interni formali

6.7 Oggetti ricorrenti

6.8 Registrazione differita di protocollo

6.9 Documenti riservati (Protocollo riservato)

6.10 Documenti soggetti a registrazione particolare

7 IL SISTEMA DI GESTIONE DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

7.1 Descrizione funzionale ed operativa

8 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

8.1 Principi sulla conservazione dei documenti informatici

8.2 La conservazione dei documenti informatici dell'Ente

9 REGISTRO DI EMERGENZA

9.1 Utilizzo del registro di emergenza

10 SICUREZZA

10.1 Obiettivi

10.2 Credenziali di accesso al sistema documentale

10.3 Sicurezza nella formazione dei documenti

10.4 Trasmissione ed interscambio dei documenti informatici

10.5 Accesso ai documenti informatici

11 NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione e aggiornamento del manuale

11.2 Pubblicità del manuale

11.3 Entrata in vigore

ALLEGATI

Allegato 1 - Norme di riferimento

Allegato 2 - Nomina del Responsabile della gestione documentale e del Servizio di Protocollo informatico

Allegato 3 - Titolario di classificazione e piano di conservazione dei documenti

Allegato 4 - I formati dei documenti

Allegato 5 - I metadati dei documenti informatici

Allegato 6 - I metadati dei fascicoli digitali

Allegato 7 - Il sistema documentale e di protocollazione adottato dall'Ente

1 PRINCIPI GENERALI

1.1 Premessa

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

Nel manuale di gestione documentale sono riportati, in particolare, relativamente agli aspetti organizzativi:

- a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati";
- b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
- c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
- d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

Il Manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

1.2 Ambito di applicazione del manuale

Il presente Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi è aggiornato alle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti, oltre che la gestione dei flussi documentali dell'Ente.

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa. Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e spedizione di un documento.

1.3 Definizioni

Ai fini del presente Manuale si intende:

- per "CAD", il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale, nel testo vigente.
- per TUDA, il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 testo unico documentazione amministrativa
- per "Linee Guida", le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 01/01/2022
- Documento amministrativo informatico, ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa;

- Documento elettronico, qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
- Documento informatico, documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
- Duplicato informatico Vedi art. 1, comma 1, lett) i quinquies del CAD.

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

- AOO - Area Organizzativa Omogenea;
- PdP - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- UO – Unità Organizzativa – unità organizzativa interna (settore, servizio, ufficio)
- UCP - Unità Organizzativa Centrale di registrazione di Protocollo – rappresenta l'ufficio centrale di protocollo
- UOP – Unità Organizzativa di registrazione di Protocollo – unità organizzativa abilitata alla protocollazione, diversa dall'ufficio centrale di protocollo.
- UOR - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- RPA Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- RSP - Responsabile della gestione documentale e del Servizio di Protocollo informatico;
- MdG - Manuale di Gestione del protocollo informatico, dei flussi documentali e degli archivi;

1.4 Norme di riferimento

Le principali norme di riferimento sono elencate nell'allegato 1 - Norme di riferimento"

2 DOCUMENTI E MODALITA' DI GESTIONE

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatica dei documenti è presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio.

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

- informatico ("rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti");
- analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").

In termini operativi, il documento amministrativo è invece classificabile in:

- ricevuto;
- inviato;
- interno formale
- interno informale

2.1 Il documento informatico

Il Codice dell'Amministrazione Digitale definisce il documento informatico come “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”.

Il documento informatico è formato mediante una delle seguenti modalità:

- a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti inter-operanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente

- L'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento.
- L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti.
- In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di hash che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

2.1.1 Immodificabilità e integrità del documento informatico

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;

- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico reso immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati del documento informatico".

2.2 Il documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo. Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA, nonché i metadati relativi alla classificazione, ai sensi dell'articolo 56 del TUDA, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza. Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5.

In applicazione dell'art.23-ter comma 5-bis del CAD, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

2.3 Il documento analogico – cartaceo amministrativo

Per documento analogico si intende " la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" cioè un documento "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale".

Di seguito faremo riferimento ad un documento amministrativo cartaceo predisposto con strumenti informatici (ad esempio, una lettera prodotta tramite un software di office automation) e poi stampato.

In quest'ultimo caso si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di firma autografa.

2.4 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia. I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo" delle Linee Guida.

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici avviene solo a seguito di provvedimento di autorizzazione richiesto alla competente Soprintendenza.

2.5 Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione “.docx” in un documento “.pdf”.

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 “Certificazione di Processo” delle Linee Guida. Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto.

L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del pubblico ufficiale a ciò autorizzato.

2.6 Copia/ estratto analogica di documento informatico

Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le regole tecniche, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica.

2.7 Autenticazione di firma

L'autenticazione delle firme è prevista per la firma elettronica o qualsiasi altro tipo di firma avanzata (FEA, qualificata e digitale) e viene effettuata da un pubblico ufficiale (Segretario Comunale o funzionario delegato) che attesta, firmando con firma digitale, che

- a) la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale,
- b) l'eventuale certificato elettronico utilizzato è valido

c) il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

L'autenticazione avviene anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata

Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata.

2.8 Timbro digitale

Il timbro digitale garantisce la verificabilità e l'autenticità di un documento informatico anche dopo la sua eventuale stampa.

Il timbro digitale può essere indicato, a seconda del contesto, con termini quali 'contrassegno elettronico', 'codice bidimensionale' o 'glifo'.

Il Comune può utilizzare strumenti di timbratura digitale (ad esempio QR code) per garantire autenticità, integrità e verificabilità dei documenti informatici.

Tali strumenti non costituiscono firma elettronica, salvo che siano realizzati come sigillo elettronico qualificato ai sensi del Regolamento eIDAS e delle Linee guida AgID.”

2.9 Tipologie di firme elettroniche

La normativa vigente in materia, individua e disciplina diverse tipologie di sottoscrizione elettronica (persone fisiche) attraverso le seguenti definizioni:

- a) firma elettronica semplice – dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

- b) firma elettronica avanzata FEA – insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
- c) firma elettronica qualificata FEQ – Firma elettronica che soddisfa i requisiti del Regolamento (UE) eIDAS: è creata mediante un dispositivo qualificato per la creazione di firme elettroniche (QSCD) ed è basata su un certificato qualificato per firme elettroniche. Ha valore legale equivalente alla firma autografa.
- d) firma digitale – Particolare tipo di firma elettronica qualificata, prevista dall'ordinamento italiano, basata su un sistema di chiavi crittografiche asimmetriche (una pubblica e una privata). La firma digitale garantisce autenticità, integrità e non ripudio del documento informatico e permette a chiunque di verificarne la validità tramite la chiave pubblica.

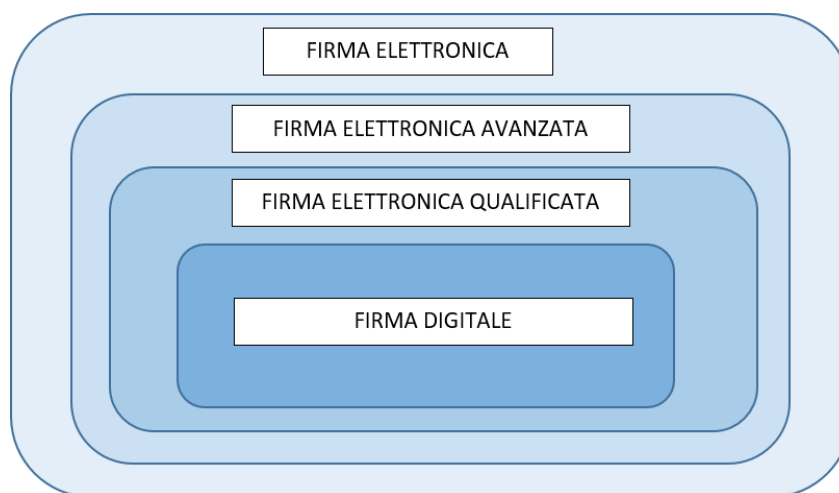


Figura 1 Le diverse firme elettroniche.

Come si evince dalla Figura 1, la firma digitale è del genere “firma elettronica qualificata.” Ai fini del presente documento, le locuzioni “firma elettronica qualificata” (o FEQ) e “firma digitale” sono pertanto utilizzati come sinonimi.

I documenti informatici sottoscritti elettronicamente possono essere distinti in tre categorie:

- documenti sottoscritti con firma elettronica ("semplice"),
- documenti sottoscritti con firma elettronica avanzata,
- documenti sottoscritti con firma elettronica qualificata (o firma digitale).

L'ente utilizza principalmente la firma elettronica qualificata (firma digitale) per garantire l'autenticità, l'integrità e la validità legale dei documenti che sottoscrive.

In particolare per quanto riguarda gli atti amministrativi (Delibere, determine, ordinanze decreti, contratti e convenzioni, documenti contabili e finanziari, atti di stato civile, autorizzazioni, provvedimenti, comunicazioni ufficiali via PEC, documenti destinati alla pubblicazione su albi e registri pubblici ecc

2.9.1 La firma elettronica semplice

La firma elettronica cosiddetta semplice può essere costituita da molteplici elementi che consentono di ricondurre degli atti o fatti giuridicamente rilevanti a una persona fisica. Un esempio è l'invio di un messaggio di posta elettronica utilizzando l'account personale istituzionale o la firma a stampa (il nome e cognome in calce a un documento).

Questo tipo di firma può essere utilizzata per documenti interni e/o informali.

2.9.2 La firma elettronica avanzata (FEA)

La firma elettronica avanzata (FEA) possiede i requisiti di cui all'art. 26 del Regolamento eIDAS e all'art. 56 del DPCM 22 febbraio 2013 e s.m.i.

Tra i principali requisiti vi sono: la riconducibilità della firma al sottoscrittore, il controllo esclusivo da parte di quest'ultimo degli strumenti di generazione della firma, il legame univoco tra firma e documento e la possibilità di verificare eventuali modifiche del documento dopo la sottoscrizione.

Un esempio diffuso di FEA è la firma grafometrica, realizzata mediante dispositivi di acquisizione evoluti che rilevano caratteristiche dinamiche della firma autografa e le associano in modo sicuro al documento informatico, contribuendo al rispetto dei requisiti previsti dalla normativa.

Ai sensi dell'art. 61 del DPCM 22 febbraio 2013, tali soluzioni possono essere utilizzate esclusivamente nell'ambito dei rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che rende disponibile il sistema di firma.

L'Ente, in base alla propria valutazione del rischio e alla natura degli atti da sottoscrivere, può utilizzare la FEA per specifiche tipologie di documenti, quali ad esempio documenti interni, atti non soggetti a registrazione o pubblicazione ufficiale o dichiarazioni e consensi informati.

2.9.3 La firma elettronica qualificata (FEQ) e la firma digitale

La firma elettronica qualificata è disciplinata dal Regolamento (UE) n. 910/2014 – eIDAS e dalla Decisione di esecuzione (UE) 2015/1506 della Commissione. Essa rappresenta il livello più elevato di firma elettronica e ha valore legale equivalente alla firma autografa.

La firma elettronica qualificata può essere generata esclusivamente mediante dispositivi qualificati per la creazione di firme elettroniche (QSCD) e utilizzando certificati qualificati rilasciati da Prestatori di Servizi Fiduciari Qualificati (QTSP).

In Italia, la “firma digitale” rappresenta l'implementazione nazionale della firma elettronica qualificata, basata su tecnologia crittografica a chiave pubblica/privata (PKI).

L'elenco dei prestatori di servizi fiduciari qualificati stabiliti in Italia è disponibile sul sito dell'Agenzia per l'Italia Digitale (AgID). La Commissione Europea mette inoltre a disposizione il Trusted List Browser, che consente di consultare tutti i QTSP qualificati operanti nell'Unione Europea.

2.9.4 Il Sigillo Elettronico Qualificato

Il sigillo elettronico qualificato è stato introdotto nel nostro ordinamento con l'emanazione del già citato Regolamento eIDAS. Sostanzialmente è equivalente a una firma elettronica qualificata, con la differenza che non afferisce a una persona fisica, bensì a una persona giuridica. In altri termini, mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice fiscale ecc., da un sigillo possiamo risalire con certezza ad una persona giuridica attraverso la sua denominazione, partita IVA o codice fiscale, ma non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.

Al momento, il comune adotta il sigillo elettronico qualificato per la firma della segnatrice delle PEC in uscita. Ogni messaggio PEC inviato dal Comune tramite il sistema di protocollo informatico include un file XML chiamato "segnatura di protocollo", che serve a identificare in modo univoco il documento e i suoi metadati (numero di protocollo, data, mittente, destinatario, ecc.).

Tale segnatrice deve essere garantita nella sua autenticità e integrità, ed è in questo contesto che assume rilievo l'utilizzo del sigillo elettronico qualificato.

2.10 Documenti in entrata

La corrispondenza in ingresso potrà essere recapitata con diverse modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico potrà essere recapitato, a titolo esemplificativo:

- a mezzo posta elettronica convenzionale o certificata;
- su supporto rimovibile quale, ad esempio, CD ROM, DVD, floppy disk, pen drive, hard disk esterni, etc, consegnato direttamente o inviato per posta convenzionale o corriere;

- tramite portali/servizi web dedicati;
- tramite cooperazione applicativa con le altre Pubbliche Amministrazioni (come previsto dall'Allegato 6 delle Linee Guida)

Un documento analogico potrà essere tipicamente recapitato:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telefax o telegramma;
- con consegna diretta a una delle unità organizzative aperte al pubblico da parte dell'interessato o di persona delegata.

L'Ente dà piena attuazione a quanto disposto dall'art. 45, comma 1, del CAD, in base al quale "I documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale".

Allo stato attuale, Il Comune, non sta ancora utilizzando la cooperazione applicativa per la ricezione e trasmissione della documentazione alle altre Pa.

2.11 Documento in uscita

I documenti informatici, con gli eventuali allegati, anch'essi informatici, devono essere formati con tecnologie informatiche avvalendosi del sistema di scrivania e gestione documentale.

Le modalità operative con cui vengono prodotti i documenti dal sistema documentale adottato sono specificate all'interno dell'allegato 7 del presente manuale.

I documenti così formati potranno essere inviati per mezzo della posta elettronica convenzionale, certificata oppure in cooperazione applicativa se la trasmissione è verso un'altra Pubblica Amministrazione (Allegato 6 delle Linee Guida)

Allo stato attuale, l'Ente non ha ancora attivato le modalità di cooperazione applicativa per la trasmissione della documentazione verso le altre Pubbliche Amministrazioni, proseguendo con l'utilizzo della posta elettronica certificata (PEC) quale canale ufficiale di comunicazione, sebbene l'applicativo di protocollo e gestione documentale in uso risulti già predisposto per l'attivazione di tali funzionalità.

Le modalità operative con cui vengono prodotti i documenti dal sistema documentale dell'ente sono specificate all'interno dell'allegato 7 del manuale.

Il documento informatico potrà inoltre essere riversato su supporto digitale rimovibile in formato non modificabile, per la trasmissione al destinatario con altri mezzi di trasporto.

2.12 Documento interno formale

I documenti interni potranno essere formati con tecnologie informatiche avvalendosi del sistema di scrivania e gestione documentale.

Il documento informatico di rilevanza amministrativa giuridico-probatoria scambiato tra unità organizzative mediante il sistema di gestione documentale verrà preventivamente redatto e sottoscritto con firma digitale o altra firma elettronica, protocollato come documento interno ed archiviato secondo le procedure interne, garantendo condivisione e tracciabilità. Il sistema in uso è in grado di tracciare in modo immodificabile tutte le operazioni relative alla registrazione e condivisione.

Le modalità operative con cui vengono gestiti i documenti interni dal sistema documentale dell'ente sono specificate all'interno dell'allegato 7 del manuale.

2.13 Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente, ad eccezione della obbligatorietà dell'operazioni di protocollazione e sottoscrizione elettronica.

Le modalità operative con cui vengono gestiti i documenti interni dal sistema documentale dell'ente sono specificate all'interno dell'allegato 7 del manuale.

2.14 Trasmissione informatica dei documenti

I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2.15 Uso della Posta Elettronica e della Posta Elettronica Certificata

Le comunicazioni di documenti tra le pubbliche amministrazioni e i privati cittadini e professionisti avvengono di norma mediante l'utilizzo della posta elettronica o della posta elettronica certificata; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Ai fini della verifica della provenienza le comunicazioni sono valide se:

- a) Sono sottoscritte con firma autografa, corredata, se necessario, da copia del documento di identità del sottoscrittore (ad esempio in caso di copia per immagine di un documento analogico);
- b) Sono sottoscritte con firma elettronica qualificata, inclusa la firma digitale ai sensi del CAD e del Regolamento eIDAS;
- c) Sono dotate di segnatura di protocollo informatizzato, secondo quanto previsto dagli articoli 55 e seguenti del CAD;
- d) È comunque possibile accertarne la provenienza con modalità alternative, conformi alla normativa vigente o alle regole tecniche di cui all'articolo 71 del CAD;

- e) Sono trasmesse tramite posta elettronica certificata (PEC), ai sensi del DPR 11 febbraio 2005, n. 68, garantendo la certezza della provenienza e della data di trasmissione.

Il documento informatico trasmesso per via telematica si considera inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato, nei limiti dei canali ammessi dall'Ente (ad esempio PEC o sistemi di posta elettronica autorizzati).

La dichiarazione da parte dell'utente del proprio indirizzo di posta elettronica costituisce accettazione dell'invio tramite tale canale degli atti e dei provvedimenti amministrativi relativi ai procedimenti specifici avviati con l'Ente, secondo quanto previsto dalla normativa vigente.

La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

L'utilizzo della Posta Elettronica Certificata (PEC) o di altro sistema analogo consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica certificata dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO.

L'AOO dispone almeno di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici che ad essa fanno riferimento.

All'interno dell'Indice delle Pubbliche Amministrazioni (IPA) sono resi disponibili i riferimenti (PEC) per comunicare con le Pubbliche Amministrazioni e i Gestori di Pubblici Servizi, inclusi i riferimenti necessari per la fatturazione elettronica e per gli ordini elettronici.

Gli indirizzi di posta elettronica certificata (PEC) dei cittadini, professionisti e altri soggetti privati che abbiano registrato il proprio domicilio digitale sono reperibili tramite l'Indice Nazionale degli Indirizzi Digitali (INAD), un registro pubblico gestito da AgID. La registrazione del domicilio digitale consente di ricevere comunicazioni ufficiali e documenti a valore legale dalla Pubblica Amministrazione. In tal modo, tramite il domicilio digitale, la PA può inviare comunicazioni telematiche valide a tutti gli effetti di legge, analogamente a quanto avviene con l'INI-PEC per imprese e professionisti.

Per quanto riguarda utilizzo della posta elettronica per le comunicazioni tra Pubbliche Amministrazioni è da intendersi quale modalità transitoria nelle more dell'applicazione delle comunicazioni tra AOO tramite cooperazione applicativa" come previsto dall'allegato 6 delle Linee Guida.

2.16 Uso della cooperazione applicativa (solo tra P.A.)

L'applicativo di protocollo in uso è predisposto per la cooperazione applicativa tra Pubbliche Amministrazioni, in linea con le Linee Guida e le specifiche tecniche dell'Allegato 6.

Il sistema consente lo scambio sicuro di messaggi protocollati tra AOO, garantendo: integrità e autenticità dei documenti tramite firme o sigilli elettronici qualificati, non ripudio delle comunicazioni, tracciamento dei documenti principali e degli allegati, e protocollazione sia in invio che in ricezione. In caso di anomalie (file illeggibili, firme o sigilli non validi, marcature temporali non verificate), il destinatario segnala la problematica al mittente, che può annullare o ripetere la trasmissione.

Il sistema è già predisposto per la cooperazione applicativa, ma al momento l'Ente utilizza prevalentemente la posta elettronica certificata (PEC) per le comunicazioni ufficiali con altre amministrazioni, in considerazione della diffusione ancora limitata del sistema nella PA. L'adozione della cooperazione applicativa avverrà in linea con l'evoluzione normativa e la disponibilità delle controparti.

2.17 Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico e di gestione documentale si intende la possibilità di trattamento automatico, da parte di un sistema ricevente, delle informazioni trasmesse da un sistema mittente, allo scopo di automatizzare le attività e i processi amministrativi conseguenti (art. 55, comma 4, DPR 28 dicembre 2000, n. 445).

Per realizzare tale interoperabilità tra sistemi gestiti dalle pubbliche amministrazioni è necessario utilizzare modalità di comunicazione standardizzate, come descritto nella sezione precedente, garantendo un'efficace interazione tra i sistemi di gestione documentale. In particolare, ogni messaggio protocollato deve riportare informazioni archivistiche fondamentali, incluse nella segnatura informatica, per consentire al sistema ricevente un trattamento automatico e corretto dei documenti.

L'Allegato 6 delle Linee Guida indica le modalità di trasmissione dei documenti informatici, il tipo e il formato delle informazioni archivistiche di protocollo minime e accessorie da scambiare tra le pubbliche amministrazioni e associate ai messaggi protocollati. Le modalità tecniche e i formati definiti verranno adeguati nel tempo in relazione all'evoluzione tecnologica e alle future esigenze delle amministrazioni, includendo l'introduzione di interfacce REST/JSON a complemento della modalità SOAP tradizionale.

3 ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

3.1 Il protocollo informatico

L'Ente gestisce un unico protocollo informatico per tutti i documenti in arrivo, in partenza nell'ambito di un sistema di gestione documentale aggiornato alle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Maggio 2021)

Il registro è generato automaticamente dal sistema di protocollo che assegna a ciascun documento registrato il numero e la data di protocollazione.

All'unico sistema di protocollazione corrisponde un unico titolario di classificazione.

L'Ente produce un unico archivio, l'articolazione in archivio corrente, archivio di deposito ed archivio storico risponde esclusivamente a criteri di funzionalità.

I responsabili dei procedimenti amministrativi dei singoli uffici provvedono alla implementazione della fascicolazione della corrispondenza in arrivo ed alla protocollazione e fascicolazione della corrispondenza in partenza. Gestiscono e custodiscono i documenti dell'archivio corrente (e, in alcuni casi, dell'archivio di deposito).

Nell'ambito della gestione documentale il sistema di protocollo si compone di:

- risorse archivistiche: piano di classificazione o titolario (Allegato 3) e presente manuale di gestione documentale
- risorse informatiche: software applicativo dedicato (Allegato 7), piattaforma documentale, PEC e posta elettronica ordinaria, cooperazione applicativa tra Pubbliche Amministrazioni, piattaforme di interscambio;
- risorse umane: operatori del servizio, responsabile della gestione documentale, coordinatore della gestione documentale (Allegato 2)

- risorse normative: D.Lsg 82/2005 e sm.i., Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (Maggio 2021), il presente manuale.

3.2 Aree Organizzative Omogenee e modelli organizzativi

L'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) che è composta dall'insieme di tutte le unità organizzative (settori, servizi, uffici). All'interno della AOO il sistema di protocollazione è unico.

Il sistema di protocollazione all'interno della AOO è parzialmente centralizzato per la corrispondenza in entrata mentre è decentralizzato per la corrispondenza in uscita, attraverso tutte le unità organizzative che svolgono anche i compiti di UOP.

Gli operatori incaricati dell'attività di protocollazione sono abilitati dal Responsabile della gestione documentale e del Servizio di Protocollo informatico che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

3.3 Accredитamento dell'amministrazione/AOO all'Indice delle Pubbliche Amministrazioni (IPA)

Nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;
- l'indirizzo della sede principale della amministrazione;
- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:
 - della denominazione;
 - del codice identificativo;
 - della casella di posta elettronica;

- del nominativo del RSP;
- della data di istituzione;
- dell'eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'AOO.
- i dati relativi alla fatturazione elettronica
- i dati relativi al Responsabile della Transizione digitale
- ecc

L'Indice delle Pubbliche Amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa in modo da garantire l'affidabilità di tutti i dati.

Per assicurare la comunicazione tra AOO le Amministrazioni devono registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

3.4 Individuazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico

Nell'AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Alla guida del suddetto servizio è posto il Responsabile della gestione documentale e del Servizio di Protocollo informatico (RSP). La nomina è riportata nell'allegato 2 del presente manuale.

Il Responsabile è funzionalmente individuato nella figura del Responsabile dell'Area amministrativa. In caso di assenza del Responsabile, le sue funzioni sono demandate al vicario formalmente delegato.

E' compito del Responsabile:

- provvedere all'aggiornamento e all'eventuale revisione del Manuale della gestione documentale e del Servizio di Protocollo informatico;
- provvedere alla pubblicazione e divulgazione del Manuale, anche attraverso il sito Internet dell'Amministrazione;
- abilitare gli addetti dell'amministrazione all'utilizzo del sistema software di gestione documentale e definire per ciascuno di essi il tipo di funzioni disponibili (ad esempio consultazione, modifica ecc.) e l'ambito di azione consentito;
- verificare il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- supervisionare la corretta produzione del registro giornaliero di protocollo curata dall'ufficio protocollo;
- supervisionare la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard ammessi dalla normativa vigente;
- la supervisione dell'invio del pacchetto di versamento che sarà formato dai delegati di ogni unità organizzativa dell'AOO e quindi del transito del pacchetto al sistema di conservazione. Il documento, il fascicolo o l'aggregazione per poter essere correttamente versati in conservazione devono essere stati formati e gestiti in ottemperanza alle regole tecniche sulla formazione, protocollazione e firma secondo le regole tecniche e secondo quanto esplicitato nel presente manuale.
- proporre eventuali modifiche al Titolare di classificazione;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e comunque in conformità a quanto stabilito nel Piano di continuità operativa/DR e relativi allegati;
- conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
- supervisionare il buon funzionamento degli strumenti e curare il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le operazioni di annullamento della registrazione di protocollo;

- aprire e chiudere il registro di protocollazione di emergenza.
- ...ecc.

3.5 Requisiti minimi di sicurezza dei sistemi di gestione documentale e protocollo informatico

Il sistema di gestione documentale e protocollo informatico assicura:

- a) l'univoca identificazione ed autenticazione degli utenti;
- b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.
- e) l'univoca identificazione dei documenti;

Le registrazioni sono protette da modifiche non autorizzate ed inoltre, il sistema di gestione documentale e protocollo informatico consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti e consente il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è prodotto automaticamente dal software gestionale del protocollo e viene trasmesso entro la giornata lavorativa successiva al sistema di conservazione, a garanzia dell'immodificabilità del contenuto.

3.6 Tutela dei dati personali

L'Ente garantisce che la gestione documentale avvenga nel pieno rispetto delle disposizioni del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.

Il trattamento dei dati personali contenuti nei documenti amministrativi è improntato ai principi di liceità, correttezza, trasparenza, minimizzazione, esattezza, integrità e riservatezza.

Gli addetti autorizzati ad accedere al sistema di protocollo informatico e di gestione documentale sono formalmente incaricati e istruiti in merito alle procedure e alle misure di sicurezza da adottare, in conformità a quanto previsto dall'art. 29 del GDPR e dalle indicazioni del Responsabile della Protezione dei Dati (RPD).

L'accesso ai dati e ai documenti è consentito esclusivamente nei limiti delle funzioni e delle mansioni attribuite, in base al principio di autorizzazione granulare e alla profilazione degli utenti prevista dal sistema informatico, che assicura che ciascun operatore possa visualizzare, modificare o trattare solo le informazioni necessarie allo svolgimento del proprio ruolo.

I Responsabili delle unità organizzative comunicano al Responsabile del Servizio protocollo le funzioni da abilitare agli operatori delle rispettive Aree/Uffici.

Per quanto riguarda i rapporti con soggetti esterni, l'Amministrazione garantisce che i documenti trasmessi ad altre Pubbliche Amministrazioni contengano esclusivamente le informazioni strettamente necessarie e pertinenti alle finalità del procedimento, nel rispetto delle disposizioni di legge.

L'Ente adotta misure tecniche e organizzative adeguate per proteggere i dati personali da accessi non autorizzati, perdita o divulgazione indebita.

Tra le principali misure di sicurezza rientrano:

- autenticazione forte e gestione profilata degli accessi al sistema documentale;
- accesso da rete esterna alla rete comunale, o comunque da reti non preventivamente autorizzate, consentito esclusivamente tramite identità digitale;
- tracciabilità e registrazione delle operazioni di consultazione e modifica;
- crittografia dei file e delle comunicazioni digitali;
- sistemi di backup;

- procedure di verifica periodica e aggiornamento delle misure di sicurezza.

La consultazione di atti e documenti da parte di cittadini e imprese avviene nel rispetto delle disposizioni della Legge 241/1990, del D.Lgs. 33/2013 e del D.Lgs. 97/2016, nonché dei limiti imposti dalla normativa in materia di protezione dei dati personali.

In sede di pubblicazione o diffusione, l'Ente provvede all'oscuramento o anonimizzazione dei dati non pertinenti o eccedenti rispetto alle finalità della pubblicazione.

È garantito, in ogni fase del trattamento documentale, il diritto dei cittadini e delle imprese a che l'uso delle tecnologie informatiche e telematiche avvenga nel rispetto dei diritti e delle libertà fondamentali, della dignità della persona e della protezione dei dati personali, secondo quanto previsto dalla normativa vigente.

3.7 Formazione del personale

Nell'ambito delle attività di attivazione ed applicazione del sistema di gestione documentale e di workflow, l'Ente organizza percorsi formativi specifici e generali che coinvolgono il personale.

In particolare, considerato che il personale assegnato al servizio di protocollo deve conoscere sia l'organizzazione e i compiti svolti da ciascuna unità organizzativa all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, vengono effettuati percorsi formativi e di aggiornamento volti ad assicurare l'operatività del personale stesso.

4 DESCRIZIONE DEL FLUSSO DI ELABORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

4.1 Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi riportati nelle pagine seguenti.

Essi si riferiscono, in particolare, ai documenti:

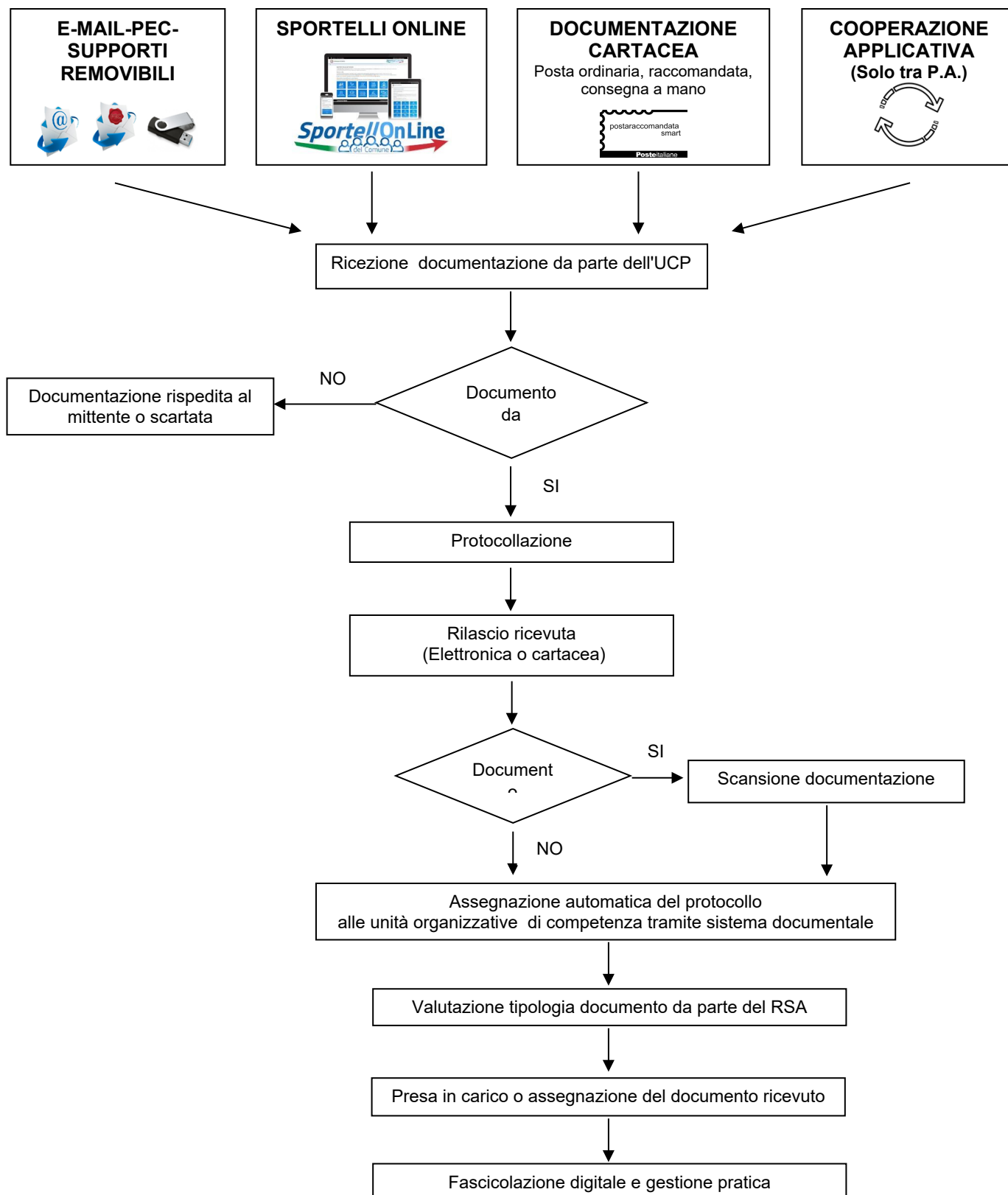
- ricevuti dalla AOO, dall'esterno
- inviati dalla AOO, all'esterno

La schematizzazione relativa ai documenti ricevuti si riferisce ad un flusso di lavoro ove la maggior parte delle operazioni sono gestite dall'ufficio protocollo.

L'avvio effettivo del procedimento collegato alla documentazione protocollata viene gestita dalle singole unità organizzative competenti

La schematizzazione relativa ai documenti inviati si riferisce ad un flusso di lavoro svolto prevalentemente dall'unità organizzativa competente.

4.2 Flusso dei documenti ricevuti dalla AOO



4.2.1 Ricezione di documenti informatici sulle caselle di posta elettronica certificata

Di norma la ricezione dei documenti informatici è assicurata tramite le caselle di posta elettronica certificata.

Le caselle PEC sono controllate quotidianamente dalla UCP o dai singoli servizi.

Tale modalità rappresenta la norma anche per la ricezione dei documenti per i quali è richiesta la pubblicazione all'Albo Pretorio on line dell'Ente.

Ogni messaggio deve riferirsi a una sola questione. Anche nel caso in cui vengano inviati contestualmente più documenti, deve essere possibile attribuire all'invio una unica protocollazione, e una unica classificazione.

Quando i documenti informatici pervengono all' ufficio protocollo (o ad altro servizio tramite la propria casella di posta elettronica certificata) la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo.

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi. L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

I documenti ricevuti per via telematica sono resi disponibili agli uffici attraverso il sistema di gestione documentale adottato dall'Ente subito dopo l'operazione di classificazione e smistamento.

Qualora si riceva un messaggio/documento con oggetti plurimi, cioè riferito a più procedimenti amministrativi, lo stesso viene registrato e assegnato ai diversi uffici responsabili dei procedimenti citati, che provvedono così ciascuno per la propria

competenza all'apertura dei relativi iter procedimentali di competenza ed alla fascicolazione (eventualmente multipla se non si utilizza un fascicolo comune)

Nel sistema di gestione documentale si può **collegare lo stesso documento a più fascicoli** digitali.

4.2.2 Ricezione di documenti informatici sulla casella di posta elettronica tradizionale

Nel caso in cui un messaggio venga ricevuto su una casella di posta elettronica non destinata specificamente al servizio di protocollazione e non PEC o similare, spettano al titolare della casella le valutazioni e le incombenze relative alla ricevibilità, alla protocollazione e alla classificazione del documento, con conseguente inserimento nel sistema comunale di gestione documentale.

Le caselle di posta elettronica collegate al sistema di gestione documentale sono intestate esclusivamente agli uffici, e ne è formalmente responsabile il titolare, che vigila sul corretto uso, sulla sicurezza e sulla riservatezza delle comunicazioni.

Ogni messaggio di posta elettronica costituisce una singola operazione di registrazione di protocollo, che comprende il contenuto del messaggio e gli eventuali documenti allegati.

Qualora si riceva un messaggio/documento con oggetti plurimi, cioè riferito a più procedimenti amministrativi, lo stesso viene registrato e assegnato ai diversi uffici responsabili dei procedimenti citati, che provvedono così ciascuno per la propria competenza all'apertura dei relativi iter procedimentali di competenza ed alla fascicolazione (eventualmente multipla se non si utilizza un fascicolo comune).

Nel sistema di gestione documentale si può collegare lo stesso documento a più fascicoli digitali.

Le comunicazioni pervenute da altre pubbliche amministrazioni attraverso i medesimi canali sono considerate valide ai fini del procedimento amministrativo solo se è possibile accertarne la provenienza, in conformità a quanto previsto dall'art. 47 del CAD. L'attività di accertamento della provenienza e autenticità del documento ricevuto è effettuata dall'ufficio titolare della casella.

Gli uffici titolari di caselle di posta elettronica ordinaria possono procedere autonomamente alla registrazione di protocollo, archiviazione, assegnazione e fascicolazione se autorizzati dal Responsabile della Gestione Documentale e Protocollo.

In caso l'Ufficio ricevente non fosse autorizzato alla protocollazione in entrata, il messaggio email ricevuto può essere inoltrato all'ufficio protocollo direttamente tramite il sistema documentale. In tal caso l'ufficio titolare della casella assicura le attività preliminari di classificazione, assegnazione e fascicolazione dei documenti mentre successivamente l'Ufficio Protocollo procede alla conferma e registrazione.

È vietato l'uso di caselle personali per l'invio o la ricezione di documenti destinati alla protocollazione.

I messaggi oggetto di registrazione al protocollo possono essere ricevuti sulle caselle di posta ufficiali dell'Ente. L'elenco aggiornato di tutte le caselle istituzionali abilitate è disponibile sul sito dell'ente e sul portale dell'Indice delle Pubbliche Amministrazioni (IPA).

L'accesso alle caselle avviene nel rispetto delle misure di sicurezza interne e delle norme sulla protezione dei dati personali ed è consentito esclusivamente al personale formalmente autorizzato. L'accesso ai documenti è profilato in base a ruoli e mansioni, garantendo che ciascun operatore possa consultare o trattare esclusivamente le informazioni pertinenti alle proprie competenze.

4.2.3 Ricezione di documenti informatici tra PA tramite cooperazione applicata

Come previsto dall'Allegato 6 delle Linee Guida, per la comunicazione tra AOO mittente e AOO destinataria è possibile utilizzare la modalità di trasmissione dei protocolli in cooperazione applicativa.

Per garantire la comunicazione tra AOO, le Amministrazioni DEVONO registrare e mantenere aggiornato, per ciascuna AOO della propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA), con il prefisso condiviso dagli endpoint di esposizione dei servizi indicati nell'Appendice B dell'Allegato 6.

Le AOO mittente e destinataria assicurano il non ripudio della comunicazione attraverso la firma dei messaggi scambiati e il loro trasporto sicuro su canale TLS, secondo le specifiche WS-Security.

Il sistema è già predisposto per la cooperazione applicativa, ma al momento l'Ente utilizza prevalentemente la posta elettronica certificata (PEC) per le comunicazioni ufficiali con altre amministrazioni, in considerazione della diffusione ancora limitata del sistema nella PA. L'adozione della cooperazione applicativa avverrà in linea con l'evoluzione normativa e la disponibilità delle controparti.

4.2.4 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati su supporti rimovibili. L' AOO si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a verificare, decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase, il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

4.2.5 Ricezione di documenti informatici da portale web dell'Ente

L'Ente consente la ricezione di documenti digitali attraverso il sito internet istituzionale, mediante appositi servizi web accessibili agli utenti autenticati con identità digitale.

I cittadini e le imprese possono avviare online le procedure relative ai servizi erogati dall'Ente. Tra i servizi attivi si segnalano, a titolo esemplificativo:

- Sportello Unico dell'Edilizia (SUE): per la presentazione di pratiche edilizie, comunicazioni e permessi.
- Sportello del Cittadino: per la presentazione di istanze e segnalazioni, nonché per la gestione di prenotazioni di appuntamenti.

Attraverso questi sportelli online, l'utente può:

- Compilare moduli digitali guidati;
- Allegare documenti informatici;
- Effettuare pagamenti online tramite il circuito PagoPA, ove previsto;
- Inviare la pratica direttamente al Comune.

Al termine dell'operazione, l'utente riceve una ricevuta elettronica attestante l'avvenuta presa in carico della richiesta.

Le pratiche trasmesse tramite i portali online vengono acquisite automaticamente dal sistema documentale. La protocollazione automatica è resa possibile perché le impostazioni del sistema sono preventivamente configurate per garantire la corretta registrazione, classificazione e fascicolazione di queste movimentazioni. Il flusso documentale prevede la registrazione a protocollo come segue:

- Classificazione secondo il titolario dei procedimenti;
- Fascicolazione e associazione al procedimento amministrativo e all'ufficio competente;

- Tracciabilità completa delle operazioni, garantendo integrità, autenticità e sicurezza dei documenti.

In questo modo, l'Ente assicura che la gestione delle pratiche online sia conforme alle disposizioni normative in materia di protocollo informatico, digitalizzazione dei procedimenti e protezione dei dati personali.

4.2.6 Ricezione di documenti cartacei a mezzo servizio postale, corriere o consegnati a mano

I documenti pervenuti a mezzo posta convenzionale o tramite corriere sono consegnati all'ufficio protocollo.

I documenti consegnati a mano agli uffici comunali sono verificati ed eventualmente protocollati e scansati dall'ufficio ricevente appositamente autorizzato, oppure possono essere consegnati all'ufficio protocollo che provvede alla scansione dei documenti ed alla corretta protocollazione/registrazione nel sistema di gestione documentale.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.

La corrispondenza cartacea relativa a bandi di gara è registrata (con scansione della busta, e annotazione dell'orario preciso di ricezione ove richiesto) e successivamente consegnata chiusa all'ufficio responsabile della gara.

La corrispondenza personale non deve essere aperta, né protocollata: deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, consegnata all'ufficio protocollo per la registrazione e le operazioni complementari alla stessa. Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta, e contestualmente protocollata.

Le ricevute di ritorno della posta raccomandata potranno essere scansionate ed inserite nel sistema di gestione documentale collegate al relativo fascicolo/procedimento.

L'originale cartaceo viene conservato fino ad eventuale scarto autorizzato dalla competente Soprintendenza.

4.2.7 Corrispondenza di particolare rilevanza e documenti esclusi

La corrispondenza di particolare rilevanza comprende tutti i documenti e le comunicazioni che, per contenuto, natura o impatto sull'attività istituzionale, richiedono una gestione e un'archiviazione prioritaria e specifica.

In particolare, si considerano di rilevanza speciale, a titolo esemplificativo:

- Comunicazioni istituzionali ufficiali: note, decreti, circolari e provvedimenti emanati da autorità superiori o organi di governo, aventi effetti normativi o organizzativi.
- Corrispondenza legale e contenziosa: atti giudiziari, diffide, citazioni, memorie difensive e ogni documento correlato a procedimenti legali in corso o potenziali.
- Corrispondenza strategica o sensibile: lettere, email o comunicazioni riguardanti progetti strategici, pianificazioni urbanistiche, sicurezza, emergenze o dati sensibili ai sensi della normativa vigente sulla privacy

Tali documenti devono essere identificati chiaramente, protocollati tempestivamente e archiviati secondo le modalità previste dal presente manuale, con particolare attenzione alla tracciabilità, alla sicurezza e alla protezione dei dati.

Altre categorie documentali possono essere escluse invece dalla protocollazione, su disposizione del Responsabile della gestione documentale e del Servizio di Protocollo informatico debitamente comunicata a tutti gli interessati.

Al di fuori di queste categorie, non sono ammesse eccezioni all'obbligo di protocollazione, segnatura e corretta gestione dei documenti.

Sono esclusi dal protocollo ordinario e dalla gestione documentale formalizzata i seguenti documenti:

- Materiale pubblicitario o promozionale privo di rilevanza istituzionale (es. volantini, brochure, proposte di corsi di formazione).
- Giornali, riviste, pubblicazioni
- Comunicazioni personali di dipendenti o di terzi non relative ad attività istituzionali (inviti ad eventi, cartoline di auguri, ..).
- Documentazione di mero interesse informativo senza effetti giuridici, amministrativi o contabili (es. newsletter esterne, comunicazioni generiche non aventi seguito).
- Duplicati non necessari di documenti già protocollati, salvo casi in cui siano previsti obblighi normativi o gestionali di conservazione separata.
- documenti già soggetti ad altro tipo di registrazione particolare presso l'Amministrazione (atti amministrativi, mandati, reversali, verbali...)

Altre categorie documentali potranno essere escluse dalla protocollazione, su disposizione del Responsabile della gestione documentale e del Servizio di Protocollo informatico debitamente comunicata a tutti gli interessati.

4.2.8 Errata ricezione di documenti digitali

Nel caso in cui pervengano messaggi istituzionali erroneamente ricevuti, l'addetto provvede a rispedire il messaggio al mittente con la dicitura: *"Messaggio pervenuto per errore - non di competenza di questa Amministrazione"*.

Se il messaggio è pervenuto tramite cooperazione applicativa da un'altra pubblica amministrazione, l'addetto inoltra la richiesta di annullamento del messaggio di protocollo precedentemente ricevuto, secondo le modalità previste dalle regole tecniche di cooperazione applicativa.

4.2.9 Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente all'Ente documenti indirizzati ad altre Amministrazioni o soggetti, possono verificarsi le seguenti eventualità:

- si restituiscono al servizio postale;
- se si tratta di documento cartaceo e la busta viene aperta per errore, il documento è protocollato in entrata e successivamente in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore", provvedendo quindi al rinvio al mittente.

4.2.10 Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti attraverso la casella di posta certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.

Nel caso di invio documentazione tramite servizi on line sul portale dell'Ente viene automaticamente rilasciata dal sistema una ricevuta attestante l'invio della documentazione.

Nel caso di documenti inviati via posta elettronica certificata per la pubblicazione all'Albo pretorio Comunale, la conferma di pubblicazione (se richiesta) potrà essere trasmessa al mittente attraverso lo stesso canale, immediatamente dopo la scadenza della pubblicazione richiesta.

Nel caso di documenti inviati tra PA tramite cooperazione applicativa, l'AOO destinataria rilascia la conferma di protocollazione del messaggio di protocollo ricevuto.

Nessuna ricevuta viene di norma rilasciata o trasmessa in caso di ricezione di documenti tramite posta elettronica tradizionale, salvo specifica richiesta.

4.2.11 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alla protocollazione in arrivo non rilasciano, di regola, ricevute per i documenti che non sono soggetti a regolare protocollazione. Sono di regola esclusi dalla protocollazione i documenti non indirizzati all'Ente, per i quali lo stesso funge unicamente da tramite tra il mittente e il destinatario finale.

Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata all'ufficio protocollo ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'ufficio rilascia una ricevuta generata automaticamente dal sistema di protocollo oppure può essere rilasciata copia della prima pagina del documento (o fotocopia della busta chiusa) riportante il timbro o l'etichetta con gli estremi della segnatura.

Nel caso di istanze che diano avvio a un procedimento, in luogo del suddetto documento viene rilasciata una "ricevuta di presentazione/comunicazione di avvio del procedimento", riportante tutte le indicazioni richieste dalla normativa vigente.

4.2.12 Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla protocollazione, per i documenti da loro trattati, eseguono di norma la classificazione sulla base del Titolario di classificazione adottato presso l'AOO e provvedono ad inviarli tramite il sistema documentale all'unità organizzativa di destinazione

Il sistema documentale consente di assegnare il documento a uno o più responsabili o uffici, in base alla competenza.

L'assegnazione può essere automatica (tramite regole predefinite) o manuale da parte degli addetti alla protocollazione.

L'unità organizzativa di destinazione esegue una verifica di congruità in base alle proprie competenze;

- in caso di errore, ritrasmette il documento all'ufficio protocollo;
- in caso di verifica positiva, esegue l'operazione di presa in carico e fascicolazione digitale;
- assegna le eventuali visibilità ulteriori rispetto a quelle attribuite automaticamente in base alla classificazione;
- gestisce il documento

Terminata la fase di protocollazione, i documenti sono portati automaticamente nella disponibilità dei soggetti competenti alla loro trattazione grazie al sistema documentale. Il sistema consente comunque di assegnare la visibilità dei documenti ad altri soggetti singoli, uffici o gruppi trasversali di addetti configurati sul sistema. Questa modalità operativa consente di portare il documento all'attenzione di tutti i soggetti interessati, attraverso la condivisione interna del sistema documentale. Si tratta di una modalità particolarmente utile per favorire la conoscenza, e la disponibilità diffusa, di tipologie documentali quali circolari, manualistica, disposizioni operative, documenti di interesse generale ecc.

Viceversa, i documenti risultano inesistenti per i soggetti ai quali non è stata assegnata, automaticamente o meno, la visibilità specifica. Si tratta di un meccanismo semplice ed affidabile per garantire la corretta gestione dei documenti riservati, contenenti dati sensibili o giudiziari, o comunque particolarmente delicati.

Nel caso di assegnazione errata, l'unità organizzativa che riceve il documento comunica l'errore all'ufficio protocollo che ha assegnato il documento, affinché proceda ad una nuova assegnazione

Tutti i documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'unità organizzativa competente attraverso il sistema di gestione documentale al termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione.

I documenti ricevuti dall'amministrazione in formato cartaceo, di regola acquisiti in formato immagine o altro formato standard non modificabile con l'ausilio di scanner, una volta concluse le operazioni di registrazione segnatura e assegnazione sono fatti pervenire al Servizio di competenza per via informatica attraverso il sistema di gestione documentale.

L'unità organizzativa competente ha notizia dell'arrivo del documento tramite apposita "notifica" generata automaticamente dal sistema documentale.

L'originale cartaceo, successivamente alla scansione, è anche trasmesso al servizio o all'ufficio competente, dove rimane disponibile per eventuale consultazione o lavorazione fino alla conclusione del procedimento. Al termine del procedimento, il documento cartaceo può essere trasferito nell'archivio di deposito, dove resta per il periodo previsto dal piano di conservazione dell'Ente. Qualora il documento presenti valore storico, giuridico o amministrativo permanente, esso potrà essere versato all'archivio storico del Comune. In caso contrario, potrà poi essere scartato, previa autorizzazione della competente Soprintendenza.

4.3 Flusso dei documenti creati e trasmessi dall'AOO

L'Area Organizzativa Omogenea (AOO) forma, gestisce e trasmette la documentazione prevalentemente in formato digitale, nel rispetto delle disposizioni del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.) e delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

I documenti prodotti dagli uffici dell'AOO vengono redatti nel sistema informatico di gestione documentale, che costituisce l'ambiente unico di riferimento per la gestione dei flussi documentali interni ed esterni, e sottoscritti mediante firma digitale o firma elettronica qualificata dove vengono anche protocollati, classificati e fascicolati.

La trasmissione dei documenti digitali avviene preferibilmente tramite Posta Elettronica Certificata (PEC) o altri canali telematici sicuri, nel rispetto delle modalità previste dal presente Manuale e dalle normative vigenti in materia di interoperabilità e conservazione dei documenti informatici.

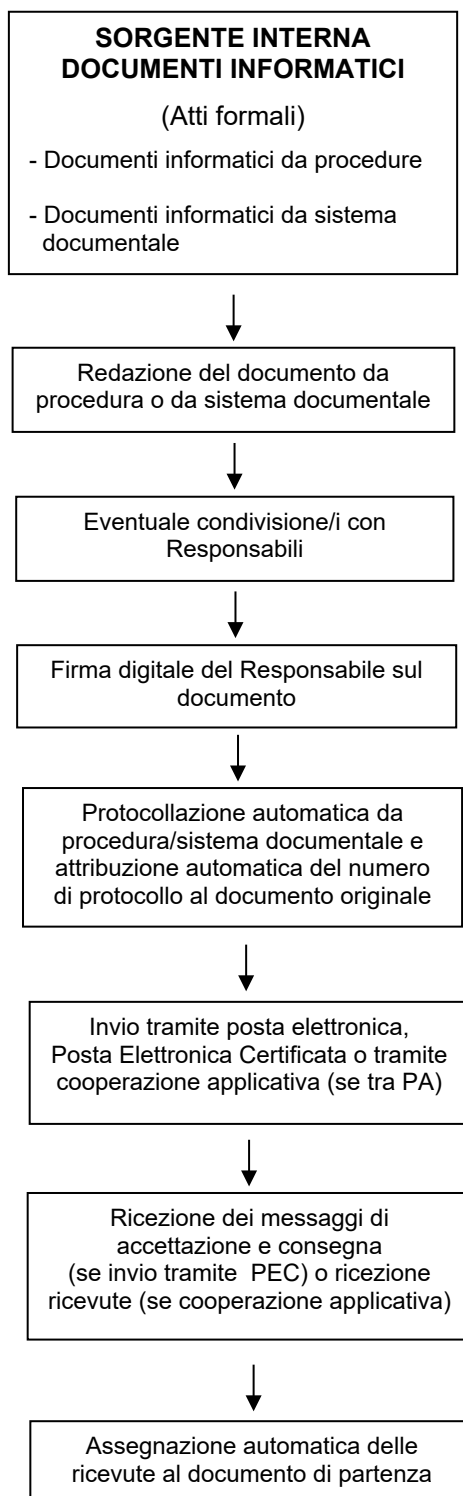
Esistono ancora alcune tipologie documentarie che richiedono la firma autografa originale, per motivi normativi, probatori o di prassi amministrativa o legati all'interoperabilità con soggetti esterni non digitali.

A titolo esemplificativo, rientrano in questa tipologia i contratti e le convenzioni sottoscritti con soggetti privi di firma digitale, le procure speciali e le scritture private autenticate, nonché i verbali e gli atti della Polizia Locale redatti in situazioni operative che non consentono l'utilizzo di strumenti digitali, i verbali di commissioni, concorsi o selezioni e i registri o moduli operativi utilizzati nei servizi esterni o in attività sul territorio.

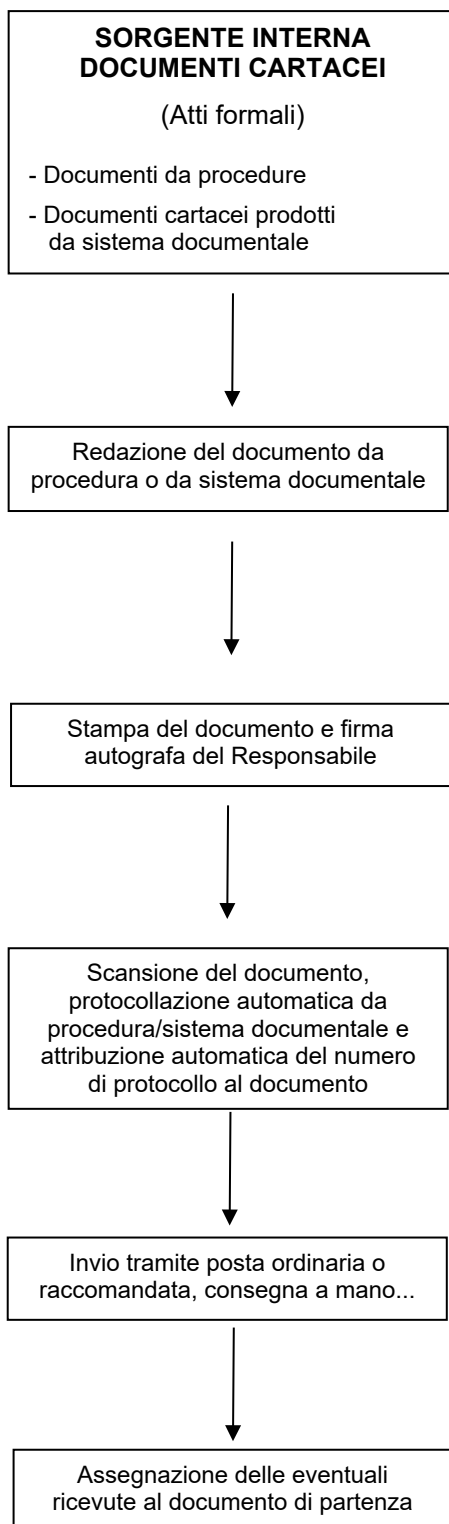
L'Ente sta progressivamente riducendo la produzione di documentazione analogica, favorendo la formazione nativa digitale e la sottoscrizione elettronica qualificata.

Di seguito sono riportati gli esempi di diagrammi di flusso relativi alla produzione dei documenti

SORGENTE INTERNA - DOCUMENTI INFORMATICI



**SORGENTE INTERNA - DOCUMENTI CON FIRMA AUTOGRAFA E TRASMISSIONE
“NON DIGITALE”**



4.3.1 Sorgente interna dei documenti

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridico-probatoria e destinati ad essere trasmessi a soggetti esterni all'Amministrazione.

Il documento viene predisposto in formato digitale, secondo gli standard illustrati nei precedenti capitoli, e recapito prioritariamente tramite posta elettronica certificata.

I documenti vengono prodotti con il sistema documentale in dotazione all'Ente con le modalità descritte nell'allegato 7

Nei casi in cui il destinatario non abbia dichiarato un domicilio digitale, oppure quando la normativa o la natura del documento richiedano la firma autografa o la trasmissione in formato analogico, l'Ente invia i documenti in formato cartaceo.

Il recapito avviene generalmente tramite servizio postale, nelle sue diverse modalità, o mediante consegna diretta allo sportello.

Tali documenti comprendono, a titolo esemplificativo, avvisi di pagamento, convocazioni e notifiche elettorali, comunicazioni relative a pratiche edilizie, contratti e convenzioni con soggetti privi di firma digitale, procure speciali, scritture private autenticate e verbali operativi.

4.3.2 Verifica formale dei documenti

Ogni unità organizzativa è autorizzata dal Responsabile della gestione documentale e del Servizio di Protocollo informatico; a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita. Le unità organizzative provvedono quindi ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa.

4.3.3 Registrazione di protocollo e segnatura

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dalle singole unità organizzative abilitate, in quanto collegate al sistema di protocollo informatico della AOO a cui appartengono.

La segnatura di protocollo viene generata dal software di gestione del Protocollo Informatico secondo le specifiche tecniche indicate nell'allegato 6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

4.3.4 Trasmissione di documenti informatici

Per la spedizione dei documenti informatici, l'AOO si avvale di:

- Posta elettronica certificata
- Cooperazione Applicativa (tra Pubbliche Amministrazioni)
- Posta elettronica
- Supporti rimovibili
- Adeguati canali telematici alternativi

Nota: il sistema è già predisposto per la cooperazione applicativa, ma al momento l'Ente utilizza prevalentemente la posta elettronica certificata (PEC) per le comunicazioni ufficiali con altre amministrazioni, in considerazione della diffusione ancora limitata del sistema nella PA. L'adozione della cooperazione applicativa avverrà in linea con l'evoluzione normativa e la disponibilità delle controparti.

Per la spedizione a soggetti privati (cittadini e imprese) dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, e di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno

elettroniche. In particolare, la PEC è strumento ordinario di trasmissione verso i cittadini che hanno dichiarato il loro domicilio digitale, nonché verso i soggetti inseriti nell'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti, o in altri indici analoghi che si rendessero disponibili in futuro.

È consentito il recapito dei documenti tramite posta elettronica tradizionale solo se sono disponibili i riferimenti del destinatario e il cittadino o l'ente, ha volontariamente fornito il proprio indirizzo email e ha accettato di ricevere comunicazioni tramite tale canale.

Questa modalità è altresì utilizzabile per le comunicazioni non formali o prive di effetti giuridici rilevanti, quali promemoria, aggiornamenti, inviti o risposte a richieste generiche.

Ai sensi del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, artt. 3-bis e 65), la posta elettronica ordinaria non sostituisce la PEC per documenti aventi rilevanza legale.

Se il documento è firmato digitalmente, conserva comunque pieno valore legale anche se trasmesso via email ordinaria, poiché la firma digitale garantisce autenticità, integrità e non ripudio del documento.

Nel caso in cui gli allegati al documento superino la capacità della casella di posta elettronica, è possibile utilizzare supporti rimovibili oppure ricorrere a canali telematici alternativi adeguati come l'upload di file su area cloud certificata dedicata dell'Ente, dalla quale è poi possibile scaricare la documentazione, oppure, in base alle specifiche esigenze, il caricamento dei documenti sullo sportello online del cittadino e/o sullo sportello unico dell'edilizia.

La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene sempre, ove tecnicamente possibile, mediante posta elettronica certificata, con effetto equivalente alla notificazione per mezzo della posta raccomandata.

4.3.5 Trasmissione di documenti cartacei a mezzo posta

L'ufficio protocollo gestisce le operazioni di spedizione della corrispondenza predisposta dagli uffici comunali. Gli uffici comunali recapitano al protocollo i plichi da spedire, in tempo utile per consentire di organizzare al meglio la gestione.

4.3.6 Conteggi e spedizione corrispondenza cartacea

L'ufficio protocollo effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza cartacea e cura il costante monitoraggio della spesa e verifica la disponibilità delle necessarie risorse economiche, informando con congruo anticipo il RSP dell'imminente esaurimento dei fondi a disposizione.

Il Responsabile della gestione documentale e del Servizio di Protocollo informatico promuove l'utilizzo di strumenti alternativi al servizio postale (e-mail, e-mail certificata ecc.) presso gli uffici comunali.

4.4 Documenti informali

Si considerano documenti informali i documenti che non assumono rilievo all'interno di procedimenti (informazioni etc).

Gli scambi di documenti informali, all'interno dell'AOO o verso l'esterno, non danno luogo a protocollazione.

5 SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE DIGITALE E ARCHIVIAZIONE

Il presente capitolo illustra il sistema di classificazione dei documenti, di formazione del fascicolo digitale e di corretta gestione e formazione dell'archivio corrente e di deposito.

5.1 La classificazione dei documenti informatici

La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi prodotti o ricevuti da un ente nell'esercizio delle sue funzioni.

Il sistema complessivo di organizzazione dei documenti è definito nel titolario di classificazione, cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti gestiti".

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo, ai sensi degli articoli 5628 e 64, comma 429, del TUDA. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

La classificazione dei documenti protocollati è di competenza dell'ufficio protocollo, che attribuisce a ciascun documento il titolo e la classe secondo il titolario adottato dal Comune. I fascicoli, destinati a raggruppare documenti relativi a uno stesso procedimento o oggetto, possono essere aperti e gestiti sia dall'ufficio protocollo sia dagli uffici responsabili delle pratiche, garantendo così una corretta organizzazione e reperibilità della documentazione.

Il Responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere.

Esso è strutturato a livelli che si articolano gerarchicamente tra loro.

Le voci di primo e secondo livello del titolario (titoli e classi) individuano le funzioni primarie e di organizzazione dell'Ente.

L'elenco dei titoli e delle classi associate è disponibile nell'allegato 3.

Le modifiche al Titolario sono apportate con provvedimento esplicito della funzione di governo dell'Amministrazione.

La revisione anche parziale del Titolario viene proposta dal RSP quando necessaria ed opportuna.

Dopo ogni modifica del Titolario, il RSP provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a fornire loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Viene garantita la storicizzazione delle variazioni di Titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

Per ogni modifica di una voce, viene riportata la data di introduzione e la data di variazione. Le variazioni sono di norma introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolario, e valgono almeno per l'intero anno.

Nel sistema di gestione informatica dei documenti dell'AOO l'attività di classificazione guida la formazione dell'archivio mediante il piano di organizzazione delle aggregazioni documentali.

5.2 La fascicolazione dei documenti

L'ente gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.

Le Linee Guida di AgID stabiliscono che ogni documento prodotto o ricevuto da una Pubblica Amministrazione deve essere correttamente classificato e fascicolato.

Le operazioni di classificazione vengono generalmente svolte in momenti diversi e da personale differente.

I primi due livelli di classificazione (*titolo-classe*) vengono generalmente attribuiti nella fase di protocollazione; l'individuazione dei successivi livelli (*macro-fascicolo*, fascicolo, sotto-fascicolo digitale...) è invece generalmente demandata al Responsabile del servizio e/o procedimento o suo incaricato.

Tutti i documenti ricevuti e prodotti dall'Ente sono classificati in base al sopra citato titolario.

I documenti ricevuti e prodotti dall'Ente sono raccolti in fascicoli costituiti in modo che ciascuno rappresenti l'insieme ordinato dei documenti riferiti ad uno stesso procedimento amministrativo o, comunque, ad una stessa pratica.

I fascicoli possono essere:

- **Fascicoli cartacei**: laddove tutta la documentazione originale della pratica è prodotta in formato cartaceo;
- **Fascicoli informatici**: laddove tutta la documentazione originale della pratica è prodotta in formato elettronico;

- **Fascicoli ibridi:** nel caso in cui la documentazione riguardante la pratica sia stata formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico. In questi casi vengono prodotti due fascicoli distinti:
 - un fascicolo cartaceo nel quale viene raccolta la documentazione cartacea
 - un fascicolo informatico, archiviato nel sistema di gestione documentale, nel quale sono raccolti tutti i documenti prodotti in formato elettronico ed i documenti analogici protocollati/archiviati scansionati.

I due fascicoli sono collegati tra loro e i riferimenti al fascicolo collegato sono riportati sia nella copertina del fascicolo cartaceo che nei dati di identificazione del fascicolo informatico.

All'interno del sistema di gestione informatica dei documenti l'Ente forma, gestisce e utilizza tipologie di aggregazioni documentali informatiche diverse dai fascicoli:

- serie che aggregano documenti
- serie che aggregano fascicoli.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

I fascicoli appartenenti a serie diverse possono essere collegati tra loro.

I Responsabili dei singoli uffici interni dell'AOO forniscono le indicazioni operative per la gestione dei fascicoli e assicurano che la costituzione dei fascicoli avvenga secondo modalità uniformi, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco che di quelli adottati per la descrizione del fascicolo.

I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.

Il fascicolo digitale corrisponde generalmente ad una "Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento.

La formazione di un nuovo fascicolo/sotto-fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali (metadati) così come previsto nell'allegato 5 delle Linee Guida.

Le informazioni (metadati) che devono essere valorizzate sul fascicolo sono:

Nome metadato	Descrizione sintetica	Obbligatorietà	Note
IdAggregazione	Identificativo univoco del fascicolo o serie	Obbligatorio	Deve essere un identificatore persistente e univoco nel sistema di gestione documentale
TipoAggregazione	Indica la tipologia dell'aggregazione (es. "fascicolo", "serie")	Obbligatorio	Serve a distinguere la natura dell'aggregazione
DataApertura	Data di apertura del fascicolo	Obbligatorio	Rappresenta il momento di creazione del fascicolo
Classificazione	Riferimento al piano di classificazione	Obbligatorio	Codice di classificazione assegnato al fascicolo
Progressivo	Numero progressivo del fascicolo all'interno della classificazione	Obbligatorio	Sequenziale per garantire un'identificazione univoca
ChiaveDescrittiva (Oggetto)	Oggetto o titolo del fascicolo	Obbligatorio	Descrive sinteticamente il contenuto o l'argomento

Nome metadato	Descrizione sintetica	Obbligatorietà	Note
Soggetti	Soggetti coinvolti nel fascicolo	Obbligatorio	Include i ruoli e gli identificativi dei soggetti
Assegnazione	Ufficio o AOO titolare o assegnatario del fascicolo	Obbligatorio	Permette la tracciabilità gestionale
Indice Documenti	Elenco strutturato dei documenti contenuti nel fascicolo	Obbligatorio	Deve consentire il collegamento ai singoli documenti

Oltre a questi metadati previsti per il fascicolo informatico, possono essere valorizzati anche ulteriori metadati quali la data di chiusura, lo stato del fascicolo e il livello di accesso.

Inoltre, qualora i tempi di conservazione siano determinati per l'intera aggregazione documentale (fascicolo o serie), deve essere valorizzato anche il metadato relativo al tempo di conservazione a tale livello, come avviene, ad esempio, per le serie delle Deliberazioni di Consiglio e di Giunta, delle Determinazioni o delle Fatture.

Ogni unità organizzativa è responsabile per la creazione e la gestione dei fascicoli nell'ambito dei servizi di competenza e delle prestazioni effettuate. I documenti contenuti in un fascicolo sono facilmente ricercabili attraverso metadati.

I criteri di visibilità dei fascicoli digitali e dei loro relativi sottofascicoli all'interno dell'AOO sono definiti dai vari Responsabili dei Procedimenti Amministrativi in accordo con il Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

I fascicoli possono anche essere distinti in annuali e non annuali, con riferimento alla durata e alla tipologia delle pratiche.

Si riporta di seguito la struttura di base del sistema di fascicolazione.

STRUTTURA DI BASE DEL SISTEMA DI FASCICOLAZIONE

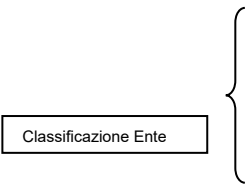
1° LIVELLO: Titoli (Attribuiti in fase di protocollatura)

2° LIVELLO: Classi (Attribuiti in fase di protocollatura)

3° LIVELLO: Macro-fascicoli (macro-aggregati) (Attribuiti dai servizi o automaticamente dalle procedure)

4° LIVELLO: Sotto-fascicoli (Inseriti dai servizi o automaticamente dalle procedure)

5° LIVELLO:

Classificazione Ente

Per quanto riguarda la classificazione ed i relativi tempi di conservazione dei documenti, si rinvia al Piano di fascicolazione e conservazione di cui all'Allegato 3 del presente manuale.

5.3 Processo di assegnazione dei documenti ai fascicoli digitali

Quando un nuovo documento viene recapitato al servizio competente o creato dall'Ente, il Responsabile del servizio o suo incaricato stabilisce se il documento si riferisce a un nuovo affare o procedimento; in caso affermativo è necessario aprire un nuovo fascicolo, altrimenti, se il documento stesso può essere ricollegato ad un affare o procedimento in corso, viene inserito in un fascicolo digitale già esistente.

A seconda delle ipotesi, si procede come segue:

- Se il documento dà avvio ad un *NUOVO PROCEDIMENTO*, il soggetto preposto:
 - esegue l'operazione di apertura del fascicolo/sottofascicolo collegato al macro-fascicolo;
 - collega il documento al nuovo fascicolo aperto;
 - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà istruire la pratica.
- Se il documento si ricollega ad un *affare o procedimento in corso*, l'addetto:
 - seleziona il relativo fascicolo utente collegato al macro-fascicolo;
 - collega il documento al fascicolo selezionato;
 - si occupa della gestione del documento o assegna il documento al collaboratore che dovrà gestire la pratica.

5.4 Modifica delle assegnazioni dei fascicoli digitali

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico.

Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora dell'operazione.

5.5 Chiusura dei fascicoli digitali

Il fascicolo digitale viene chiuso generalmente al termine del procedimento amministrativo o all'esaurimento dell'affare.

5.6 Serie archivistiche, repertori e fascicoli

I documenti soggetti a registrazione particolare, come i verbali e le deliberazioni degli organi di governo dell'amministrazione, le determinazioni dirigenziali o i contratti, costituiscono serie archivistiche.

Tali documenti sono organizzati e numerati all'interno del repertorio informatico (registro delle registrazioni particolari), che ne garantisce la tracciabilità e l'univoca identificazione.

Per quanto concerne la gestione dei documenti informatici, ciascun verbale, deliberazione, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al repertorio, con l'assegnazione di un numero progressivo di repertorio;
- al fascicolo informatico, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Le principali tipologie documentarie soggette a registrazione particolare comprendono:

- Deliberazioni e verbali di Giunta e Consiglio;

- Determinazioni dirigenziali;
- Contratti e convenzioni;
- Ordinanze;
- Provvedimenti in economia;
- Bilanci di previsione e consuntivi;
- Fascicoli del personale;
- Convenzioni e accordi di collaborazione;
- Verbali di commissioni e conferenze di servizi;
- Registro di protocollo generale

...

Per quanto riguarda la classificazione ed i relativi tempi di conservazione dei documenti, si rinvia al Piano di fascicolazione e conservazione di cui all'Allegato 3 del presente manuale.

5.7 Archiviazione dei documenti - Tempi, criteri e regole di selezione del sistema di classificazione

L'Archivio è il complesso organico dei documenti prodotti o acquisiti dall'Ente nello svolgimento della propria attività istituzionale.

Gli archivi dell'Ente costituiscono, ai sensi degli artt. 30 e 41 del Codice dei beni culturali e del paesaggio (D.Lgs. 42/2004), un bene culturale pubblico tutelato dallo Stato. Tutti i soggetti che operano nel sistema di gestione documentale dell'Ente concorrono allo svolgimento dell'attività archivistica e sono tenuti a garantire la corretta formazione, gestione e conservazione dei documenti, in conformità al Codice dell'amministrazione digitale (D.Lgs. 82/2005) e alle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

Ai fini di una gestione corretta ed efficiente, la documentazione è organizzata in tre sezioni principali:

- Archivio corrente, costituito dai documenti e fascicoli relativi ad affari e procedimenti in corso di trattazione. Per i documenti e fascicoli informatici, l'archiviazione corrente coincide con la gestione all'interno del sistema di gestione documentale;
- Archivio di deposito, costituito dai documenti relativi ad affari conclusi, non più occorrenti all'attività corrente ma ancora soggetti a eventuale consultazione o ad obblighi di conservazione. L'archivio di deposito rimane all'interno del sistema di gestione documentale dell'Ente e non coincide con il sistema di conservazione gestito dal conservatore accreditato;
- Archivio storico, costituito dalla documentazione destinata alla conservazione permanente per il suo valore giuridico, amministrativo e/o storico nel sistema di conservazione gestito dal conservatore in outsourcing accreditato .

Qualora un fascicolo resti aperto per più esercizi o anni (ad esempio per procedimenti pluriennali o di lunga durata), la documentazione in esso contenuta è comunque oggetto di versamento periodico secondo le modalità e la cadenza temporale definite nel Manuale di conservazione dell'Ente.

In particolare, i documenti e i fascicoli destinati alla conservazione permanente vengono progressivamente riversati al conservatore accreditato in outsourcing, al fine di garantirne la conservazione continua, l'integrità, la tracciabilità e la disponibilità nel tempo.

La restante documentazione, soggetta a conservazione temporanea, rimane invece archiviata nel sistema documentale dell'Ente per il periodo necessario, fino al raggiungimento dei termini previsti dal piano di classificazione e conservazione.

Nel Manuale di conservazione e nell'allegato 3 Titolario di classificazione e piano di conservazione dei documenti sono riportate modalità e criteri di fascicolazione e i tempi di conservazione

La coesistenza, nell'ambito di uno stesso procedimento, di documenti analogici e digitali dà luogo al cosiddetto archivio ibrido. Nel sistema documentale informatico, la chiusura del fascicolo comporta il trasferimento logico del relativo contenuto all'archivio di deposito. I fascicoli cartacei chiusi, non più necessari alla trattazione corrente, sono trasferiti fisicamente presso l'archivio di deposito comunale.

La gestione dei processi di selezione e valutazione della documentazione conservata nell'archivio di deposito può condurre a due esiti:

- la conservazione permanente dei documenti di valore storico o giuridico-probatorio;
- lo scarto, ossia l'eliminazione dei documenti privi di valore permanente, da effettuare esclusivamente previa autorizzazione della Soprintendenza archivistica competente per territorio, ai sensi dell'art. 21 del D.Lgs. 42/2004.

I criteri e le regole di selezione e conservazione delle diverse tipologie documentarie gestite dall'Ente sono definiti nel Manuale di conservazione.

Per quanto riguarda la classificazione ed i relativi tempi di conservazione dei documenti, si rinvia al Piano di fascicolazione e conservazione di cui all'Allegato 3 del presente manuale.

5.8 Procedure di scarto

Lo scarto documentale costituisce l'insieme delle operazioni volte a eliminare, previa autorizzazione della competente Soprintendenza archivistica, la documentazione divenuta non più utile ai fini amministrativi, giuridici o probatori, e priva di rilevanza storica.

L'attività di scarto è finalizzata a garantire la corretta gestione del patrimonio documentale dell'Ente, favorendo l'efficienza degli archivi e il contenimento dei costi di conservazione.

Lo scarto è effettuato in conformità al piano di conservazione adottato dal Comune e alle disposizioni normative in materia di archivi pubblici.

La procedura prevede le seguenti fasi:

- Individuazione delle serie documentarie eventualmente scartabili sulla base dei tempi di conservazione stabiliti nel piano
- Redazione dell'elenco di scarto, contenente la descrizione delle unità documentarie o delle serie da eliminare, con l'indicazione delle rispettive estremità cronologiche e quantità.
- Approvazione dell'elenco da parte del Responsabile della gestione documentale e dell'archivio, che verifica la conformità al piano di classificazione e conservazione.
- Richiesta di autorizzazione alla Soprintendenza archivistica e bibliografica competente, ai sensi dell'art. 21 del D.Lgs. 42/2004 ("Codice dei beni culturali e del paesaggio").
- Esecuzione materiale dello scarto, da effettuarsi solo dopo il ricevimento del nulla osta della Soprintendenza, mediante distruzione controllata dei documenti, nel rispetto della normativa in materia di protezione dei dati personali (Regolamento UE 2016/679 e D.Lgs. 196/2003 e s.m.i.).
- Redazione e conservazione del verbale di avvenuto scarto, contenente il riferimento all'autorizzazione rilasciata e alle modalità di distruzione adottate.

Tutte le operazioni di scarto devono essere documentate e tracciabili, al fine di garantire la trasparenza e la tutela del patrimonio documentale dell'Ente.

6 GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Il presente capitolo illustra le modalità di produzione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione.

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

6.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche. Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza. La documentazione che non è stata registrata sul protocollo viene considerata giuridicamente inesistente presso l'amministrazione. Non è consentita la protocollazione di un documento già protocollato. Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.

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.

Il registro di protocollo è 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, garantendone l'immodificabilità del contenuto

6.2 Registrazione di protocollo

Di seguito vengono illustrate le regole di registrazione del protocollo valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- l'indicazione del mittente o del destinatario, registrata in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la data e protocollo del documento ricevuto, se disponibili;
- la classificazione;
- l'impronta del documento informatico.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono inoltre elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

6.3 Elementi facoltativi delle registrazioni di protocollo

Il Responsabile del Servizio Protocollo, con proprio provvedimento e al fine di migliorare la gestione, la ricerca e la conservazione della documentazione, può modificare e integrare gli elementi facoltativi del protocollo, anche per singole categorie o tipologie di documenti.

La registrazione degli elementi facoltativi del protocollo, previa autorizzazione del Responsabile della gestione documentale e del Servizio di Protocollo informatico, può essere modificata, integrata e cancellata in base alle effettive esigenze delle unità organizzative o del servizio protocollo. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

6.4 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo da parte del software di protocollo.

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

La struttura tecnica e i contenuti della segnatura di protocollo sono contenute nell'allegato 6 delle Linee Guida.

6.5 Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori e immutabili della registrazione di protocollo per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare la registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla

procedura, ivi comprese le visualizzazioni e le stampe, insieme a data, ora e autore dell'annullamento e agli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RSP.

In tale ipotesi la procedura riporta l'annotazione di annullamento. Il sistema inoltre registra l'avvenuta rettifica, la data e il soggetto che è intervenuto.

Solo il Responsabile della gestione documentale e del Servizio di Protocollo informatico è autorizzato ad annullare, direttamente o delegando gli addetti, una registrazione di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al Responsabile della gestione documentale e del Servizio di Protocollo informatico.

6.6 Protocollo collazione documenti interni formali

I documenti formali prodotti e scambiati internamente sono soggetti a protocollazione e indicati come protocolli interni. Vengono inseriti nel sistema di gestione documentale con opportuna classificazione, assegnazione di visibilità, collegamento ai documenti o procedimenti correlati, fascicolazione e archiviazione.

6.7 Oggetti ricorrenti

Ciascun Servizio può individuare tipologie di documenti per i quali concordare con il Protocollo generale l'indicazione esatta dell'oggetto, la titolazione, la tipologia e l'assegnazione a predeterminati soggetti o ambiti organizzativi (modelli predefiniti di protocollazione).

È compito di ciascun Servizio provvedere a verificare il permanere dell'attualità di ciascun oggetto individuato e del relativo smistamento.

6.8 Registrazione differita di protocollo

Per "protocollo differito" si intende la registrazione di documento in arrivo che indica nello specifico la data alla quale si riferisce il ricevimento del documento stesso e la causa che ne ha determinato il differimento.

E' possibile effettuare la registrazione differita di protocollo, qualora dalla mancata registrazione di un documento nell'ambito del sistema nel medesimo giorno lavorativo di ricezione, possa venire meno un diritto di terzi.

La registrazione differita di un documento in arrivo nel sistema va richiesta e deve essere autorizzata dal Responsabile della gestione documentale e del Servizio di Protocollo informatico o suo delegato.

6.9 Documenti riservati e sensibili (Protocollo riservato)

Sono previste particolari forme di riservatezza per i documenti relativi a procedimenti disciplinari nei confronti dei dipendenti, vicende o a fatti privati, politici o giudiziari (giudizi pendenti) o documenti che richiedono, comunque, una trattazione riservata. Per tali atti sul registro di protocollo generale compare solo il numero attribuito a ciascun documento e l'annotazione "Riservato".

I documenti registrati con tali forme appartengono al cosiddetto "protocollo riservato" costituito dalle registrazioni il cui accesso è autorizzato solo alle persone espressamente abilitate. Queste ultime hanno comunque la visibilità dei soli documenti riservati trattati dall'unità di appartenenza. Le procedure adottate per la gestione dei documenti ad accesso riservato, comprese le registrazioni, la segnatura, la classificazione e la fascicolazione, sono le stesse adottate per gli altri documenti.

6.10 Documenti soggetti a registrazione particolare

La presente procedura disciplina le modalità di gestione e di eventuale registrazione nel sistema di protocollo informatico dei documenti pervenuti al Comune che presentano caratteristiche particolari.

Ai sensi dell'art. 53, comma 5, del D.P.C.M. 3 dicembre 2013, sono soggetti a registrazione di protocollo i documenti ricevuti o spediti dal Comune che rilevano ai fini dell'attività amministrativa.

I documenti che non presentano tale rilevanza non devono essere protocollati, ma gestiti secondo le modalità interne previste dal presente Manuale.

a) Lettere anonime

Le lettere anonime sono valutate dal responsabile del procedimento o dall'ufficio competente al fine di accertarne la rilevanza per l'attività istituzionale dell'Ente.

Se il contenuto è attinente all'attività amministrativa, la lettera è registrata a protocollo.

- Nel campo Mittente si inserisce: ANONIMO.
- Nel campo Oggetto si specifica il contenuto, aggiungendo l'annotazione: "Lettera anonima".

Se il contenuto non è attinente o non presenta alcun rilievo amministrativo, la lettera non viene protocollata e può essere conservata in un'apposita sezione dell'archivio corrente, secondo le disposizioni interne.

b) Documenti privi di firma

I documenti privi di sottoscrizione sono esaminati per determinarne la rilevanza amministrativa.

Se il contenuto è rilevante ai fini istituzionali, il documento è registrato a protocollo con annotazione nel campo Note: "Documento privo di firma", fatti salvi i casi di irricevibilità

prescritti per specifici documenti/procedimenti (es: istanze, domande di partecipazione a norma di regolamenti, ecc..).

Se il documento ha contenuto personale o non attinente all'attività dell'Ente, è escluso dalla protocollazione e gestito internamente dall'ufficio competente, secondo le procedure di archivio corrente.

c) Documenti con firma illeggibile o non verificabile

Qualora un documento presenti una firma manoscritta illeggibile o una firma digitale non verificabile:

Se il documento è rilevante per l'attività amministrativa, è registrato a protocollo con annotazione nel campo Note: "Firma illeggibile" oppure "Firma non verificata".

In caso contrario, può essere escluso dalla registrazione e gestito secondo le modalità interne.

d) Documenti a carattere personale o non attinenti all'attività istituzionale

I documenti di natura personale o non connessi all'attività istituzionale del Comune non devono essere protocollati.

Essi sono valutati dal responsabile del servizio di protocollo o dall'ufficio ricevente per accertare l'eventuale presenza di elementi di interesse pubblico.

Se il contenuto non ha rilevanza amministrativa, il documento è archiviato separatamente e non incluso nel registro di protocollo.

Se invece il contenuto richiede un intervento o un seguito amministrativo (ad esempio segnalazioni di disagio sociale, richieste di aiuto o altre comunicazioni rilevanti), il documento è protocollato e assegnato all'ufficio competente per competenza o conoscenza.

Il responsabile della gestione documentale assicura che la presente procedura sia applicata in modo uniforme da tutti gli uffici comunali e che siano effettuati controlli periodici

sull'osservanza delle disposizioni relative alla protocollazione e alla gestione dei documenti particolari.

7 IL SISTEMA DI GESTIONE DOCUMENTALE E DI PROTOCOLLAZIONE ADOTTATO DALL'ENTE

Il sistema di gestione documentale e di protocollazione adottato dall'Ente è basato sulla piattaforma **OLIMPO – Archiviazione documentale e scrivania digitale** della **SISCOM S.p.A.**

La soluzione per la protocollazione prevede un modulo specifico denominato **EGISTO**, che gestisce tutte le fasi di protocollazione in arrivo, partenza e interne, in modo totalmente integrato con il sistema documentale.

Il sistema consente inoltre la gestione della ricezione e trasmissione delle PEC e delle e-mail, assicurando la protocollazione e l'archiviazione automatica dei documenti in modalità sicura e non modificabile. I documenti protocollati vengono condivisi con gli uffici destinatari e tracciati lungo l'intero iter procedimentale.

I documenti prodotti dall'Ente vengono gestiti all'interno del sistema documentale in tutte le loro fasi: redazione, protocollazione, trasmissione e archiviazione, in modo completamente integrato.

Durante la fase di archiviazione, il documento informatico viene considerato completo e definitivo: non è più soggetto a modifiche o integrazioni.

In questa fase, il documento viene:

- classificato secondo il piano di classificazione dell'Ente e associato al relativo fascicolo o pratica;
- registrato con l'associazione dei metadati previsti dall'allegato 5 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- reso immodificabile e conservato nel sistema documentale, garantendo autenticità, integrità e tracciabilità.

Il documento archiviato rimane disponibile per la consultazione e l'utilizzo da parte degli uffici competenti fino al suo eventuale versamento nel sistema di conservazione.

Tutti gli applicativi verticali e gli sportelli online in uso presso l'Ente risultano, ove necessario, nativamente integrati con il sistema di gestione documentale *OLIMPO*, mediante servizi di interoperabilità che garantiscono lo scambio automatico e sicuro di dati e documenti. Tale integrazione assicura la coerenza dei flussi documentali, l'unicità dell'archiviazione e l'allineamento costante tra i diversi sistemi applicativi e i canali di interazione con l'utenza.

Questa integrazione consente di:

- trasferire automaticamente nel sistema documentale i documenti e i fascicoli generati o ricevuti dagli applicativi verticali;
- garantire la protocollazione automatica tramite il modulo Egisto, assicurando coerenza e unicità dei protocolli;
- effettuare l'archiviazione automatica dei documenti nei fascicoli di riferimento, secondo le regole tecniche AgID;
- mantenere una tracciabilità completa e uniforme dei documenti e dei procedimenti.

In tal modo, il sistema documentale costituisce il punto di riferimento unico per la gestione, la conservazione e la consultazione di tutta la documentazione amministrativa dell'Ente.

7.1 Descrizione funzionale ed operativa

La descrizione funzionale ed operativa del sistema di protocollo informatico viene specificata in dettaglio all'interno dell'allegato 7.

8 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD.

La conservazione può riguardare sia documenti informatici all'origine che documenti analogici convertiti in formato digitale.

8.1 Principi sulla conservazione dei documenti informatici

La conservazione digitale è l'insieme delle attività e dei processi finalizzati a garantire, nel tempo, l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti informatici, dei fascicoli e delle aggregazioni documentali con i relativi metadati, nel medio e lungo periodo, anche in un ambiente tecnologico diverso da quello originario.

Il processo di conservazione può essere realizzato internamente all'Ente oppure mediante affidamento a un conservatore esterno accreditato, nel rispetto di quanto previsto dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.) e dalle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

In particolare, la conservazione permanente dei documenti informatici può essere svolta in modalità di outsourcing, nel rispetto dei principi di autenticità, integrità, affidabilità, leggibilità e reperibilità del patrimonio documentale dell'Ente.

Il valore giuridico e probatorio dei documenti conservati è garantito dall'osservanza delle norme vigenti, delle regole tecniche e delle procedure descritte nel Manuale della conservazione.

Le serie documentali annuali a conservazione permanente (ad esempio deliberazioni, determinazioni, ordinanze, registri di protocollo) sono versate al sistema di conservazione entro il primo trimestre dell'anno successivo alla chiusura della serie.

I fascicoli dei procedimenti a conservazione permanente sono versati entro dodici mesi dalla chiusura del fascicolo, preferibilmente con cadenza semestrale, per assicurare la continuità della conservazione e la tempestiva presa in carico da parte del conservatore.

Il ciclo di gestione della conservazione e il servizio adottato dall'Ente sono descritti in dettaglio nel Manuale della conservazione.

8.2 La conservazione dei documenti informatici dell'Ente

L'Ente, nel rispetto della disciplina vigente, decide di affidare la gestione della conservazione permanente ad outsourcer esterno che possiede i requisiti di qualità, sicurezza e organizzazione individuati nelle Linee guida.

Il conservatore esterno accreditato a cui è affidata la conservazione è indicato nel Manuale della Conservazione documentale adottato dall'Ente.

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (Information security management systems - Requirements) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (Open Archival Information System - Sistema informativo aperto per l'archiviazione), e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

Il "ciclo completo di gestione della conservazione" ed il servizio adottato dall'Ente vengono descritti in dettaglio nel Manuale della Conservazione documentale adottato dall'Ente.

9 REGISTRO DI EMERGENZA

9.1 Utilizzo del registro di emergenza

Il registro di emergenza assicura la continuità del servizio di protocollo informatico nei casi in cui non sia possibile utilizzare il sistema di protocollo nelle normali modalità operative - per cause tecniche, organizzative o emergenziali (quali guasti infrastrutturali, calamità naturali, inagibilità degli uffici, interruzioni di rete, ecc.) - garantendo comunque la tracciabilità dei documenti.

Il Responsabile del servizio di protocollo informatico autorizza formalmente l'utilizzo del registro di emergenza se l'impossibilità si prolunga oltre ventiquattro ore.

Tutti gli uffici comunali si avvalgono dell'Ufficio Protocollo per l'assegnazione del numero di protocollo in emergenza, sia in entrata che in uscita.

Il registro di emergenza è unico per l'Area Organizzativa Omogenea (AOO) e per l'anno solare, dal 1° gennaio al 31 dicembre. Anche in caso di più eventi di emergenza nel corso dell'anno, tutte le registrazioni vengono annotate sullo stesso registro, indicando chiaramente le date e le cause di ciascuna interruzione. Al termine dell'anno, il registro viene archiviato secondo le regole previste nel Manuale della gestione documentale.

Le modalità operative sono le seguenti:

Sul registro di emergenza sono annotate le cause dell'interruzione, la data e l'ora dell'inizio e del ripristino della funzionalità ordinaria del sistema;

Per ogni giornata di registrazione in emergenza è indicato il numero totale delle operazioni effettuate;

La sequenza numerica utilizzata sul registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti nell'ambito del sistema documentario dell'AOO;

Campi minimi da indicare per ciascun documento protocollato in emergenza:

- Data e ora di registrazione;
- Mittente / destinatario;
- Oggetto del documento;
- Tipologia del documento (entrata/uscita/altro);
- Numero progressivo assegnato nel registro di emergenza;
- Classe e fascicolo di riferimento, secondo il Piano di classificazione
- Note eventualmente necessarie per identificare documenti allegati o particolari condizioni;

Le informazioni relative ai documenti protocollati in emergenza vengono inserite, senza ritardo, nel sistema di protocollo informatico ordinario al momento del ripristino;

Durante la fase di ripristino, ciascun documento registrato in emergenza riceve un numero di protocollo ordinario del sistema informatico, mantenendo stabilmente la correlazione univoca con il numero attribuito in emergenza.

10 SICUREZZA

Il piano di sicurezza informatica relativo al sistema informativo dell'Amministrazione viene definito dall'organizzazione dell'Ente responsabile della gestione complessiva del sistema informatico. Tale piano stabilisce le linee guida e le misure necessarie a garantire la protezione delle informazioni e la continuità operativa, nel pieno rispetto delle normative vigenti in materia di sicurezza informatica e protezione dei dati personali, inclusi il D.Lgs. 196/2003 e il Regolamento UE 2016/679 (GDPR).

Il presente capitolo descrive le principali misure di sicurezza adottate in relazione all'infrastruttura di protocollo informatico e gestione documentale, con particolare attenzione alla tutela dei dati e alla prevenzione di rischi informatici.

Per quanto riguarda il sistema documentale adottato dall'Ente, la gestione dei documenti avviene tramite la soluzione SaaS "NuvolaComuni" di Siscom S.p.A., qualificata ACN. Questa soluzione garantisce conformità agli standard di sicurezza definiti dall'Agenzia per l'Italia Digitale, tutela dei dati personali e continuità dei servizi documentali, integrandosi con le procedure di protocollo e gestione dei flussi informativi dell'Amministrazione.

10.1 Obiettivi

La politica in merito alla sicurezza di questo Ente è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

A tale fine l'Ente definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
 - le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
 - gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, in caso di trattamento di dati personali;
 - i piani specifici di formazione degli addetti;
 - le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.
-
- la protezione dei sistemi di accesso e conservazione delle informazioni;
 - l'assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione (user) e di una credenziale di autenticazione (password) e di un profilo di autorizzazione;
 - cambio delle password con frequenza prestabilita durante la fase di esercizio;
 - piano di continuità del servizio e copie di backup come previsto dal piano di sicurezza dell'Ente;
 - impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
 - cifratura o uso di codici identificativi (o altre soluzioni) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati allo scopo di rendere i dati e i documenti accessibili esclusivamente ai soggetti autorizzati dal sistema di gestione documentale;
 - impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati;

10.2 Credenziali di accesso al sistema documentale

Il sistema documentale dell'Ente garantisce sicurezza, tracciabilità e conformità alle normative vigenti in materia di gestione documentale e protezione dei dati.

L'accesso è riservato agli utenti autorizzati, profilati secondo i ruoli e le responsabilità definiti dall'Area Organizzativa Omogenea (AOO). Le credenziali individuali consentono di:

- Identificare in modo univoco ciascun utente;
- Garantire la tracciabilità delle operazioni effettuate;
- Limitare l'accesso alle funzionalità e ai documenti secondo il principio di minimo privilegio.

L'accesso dall'interno delle reti autorizzate può avvenire mediante credenziali individuali fornite dal Responsabile del sistema documentale oppure tramite identità digitale con SPID o CIE di livello 2. Per gli accessi da reti esterne, l'autenticazione è consentita esclusivamente tramite identità digitale SPID o CIE di livello 2, secondo le modalità previste dalla normativa nazionale. Tale approccio garantisce un elevato livello di sicurezza, assicurando la conformità alle regole AgID in materia di autenticazione, protezione dei dati e gestione degli accessi..

Le responsabilità degli utenti comprendono:

- Custodire con diligenza le proprie credenziali e non condividerle con terzi;
- Modificare periodicamente le password secondo le policy di sicurezza;
- Segnalare tempestivamente eventuali accessi non autorizzati o sospetti;
- Utilizzare il sistema documentale esclusivamente per attività di servizio autorizzate.

Il sistema documentale registra automaticamente tutti gli accessi e le operazioni effettuate, consentendo al Responsabile della gestione documentale di effettuare verifiche periodiche e garantire la sicurezza, l'integrità e la riservatezza dei documenti gestiti.

10.3 Sicurezza nella formazione dei documenti

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti sono prodotti con l'ausilio dell'applicativo specificato nell'allegato 7 che possiede i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici prodotti dall'A OO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno di una A OO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici.

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'A OO, sono sottoposti

ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

10.4 Trasmissione ed interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Lo scambio per via telematica di messaggi protocollati tra AOO di amministrazioni diverse presenta, in generale, esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196, del REG. UE 679/2016 e s.m.i.

10.5 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.

E' inoltre possibile associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

11 NORME TRANSITORIE E FINALI

11.1 Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il "Manuale di gestione" su proposta del responsabile del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi (RSP).

Il Manuale sarà aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevata nello svolgimento delle attività correnti;
- introduzione di nuove procedure

Il Manuale viene approvato e modificato con deliberazione della Giunta.

Gli allegati sono modificati, di norma e fatte salve le eccezioni esplicitamente dichiarate, con provvedimenti del Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

11.2 Pubblicità del manuale

Il Manuale è reso disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

Inoltre copia del presente Manuale è:

- resa disponibile a tutto il personale dell'AOO tramite il sistema di gestione documentale;
- pubblicata sul sito internet dell'Amministrazione.

11.3 Entrata in vigore

Il presente documento diviene efficace al conseguimento dell'eseguibilità della deliberazione di approvazione.