

# MANUALE DI GESTIONE DOCUMENTALE

---

*Questo documento è di proprietà AMTAB S.p.A. che se ne riserva tutti i diritti.*

## Sommario

|       |                                                                        |    |
|-------|------------------------------------------------------------------------|----|
| 1     | Premessa .....                                                         | 4  |
| 2     | I Profili Organizzativi .....                                          | 4  |
| 2.1   | Area Organizzativa Omogenea ed Unità Organizzativa Responsabile .....  | 4  |
| 2.2   | Ruoli e responsabilità.....                                            | 4  |
| 2.2.1 | Responsabile della Gestione Documentale .....                          | 4  |
| 2.2.2 | Servizio per la tenuta del protocollo informatico .....                | 4  |
| 2.2.3 | Responsabile per la Transizione al Digitale .....                      | 5  |
| 2.2.4 | Responsabile della Conservazione .....                                 | 5  |
| 3     | I Documenti .....                                                      | 6  |
| 3.1   | Tipologie di documenti .....                                           | 6  |
| 3.1.1 | Documento analogico .....                                              | 6  |
| 3.1.2 | Documento informatico .....                                            | 6  |
| 3.2   | Formazione dei documenti .....                                         | 7  |
| 3.2.1 | Formazione del documento analogico .....                               | 7  |
| 3.2.2 | Formazione del documento informatico .....                             | 8  |
| 3.3   | Tipologie di sottoscrizione .....                                      | 8  |
| 3.3.1 | Firma elettronica qualificata .....                                    | 9  |
| 3.4   | Copie di documenti .....                                               | 9  |
| 3.4.1 | Copia di un documento informatico.....                                 | 9  |
| 3.4.2 | Copia di un documento analogico .....                                  | 9  |
| 3.4.3 | Copia per immagine su supporto informatico di documenti analogici..... | 9  |
| 3.4.4 | Duplicato di un documento informatico.....                             | 10 |
| 4     | Flusso di Lavorazione dei Documenti.....                               | 10 |
| 4.1   | Protocollo informatico .....                                           | 10 |
| 5     | Uso della Posta Elettronica Certificata .....                          | 10 |
| 6     | Gestione Dei Documenti.....                                            | 11 |
| 6.1   | La classificazione ai sensi del "Titolario di Classificazione" .....   | 11 |
| 6.2   | Il Titolario di Classificazione.....                                   | 11 |
| 6.3   | I fascicoli .....                                                      | 12 |
| 6.3.1 | Il fascicolo informatico.....                                          | 12 |
| 6.3.2 | Il fascicolo analogico .....                                           | 13 |
| 6.3.3 | Il fascicolo ibrido .....                                              | 13 |

|       |                                                            |    |
|-------|------------------------------------------------------------|----|
| 7     | Archiviazione e Conservazione dei documenti.....           | 14 |
| 7.1   | Conservazione dei documenti nell'archivio corrente .....   | 14 |
| 7.2   | Conservazione del registro giornaliero di protocollo ..... | 14 |
| 8     | Piano di Sicurezza di Gestione Documentale .....           | 15 |
| 8.1   | Obiettivi.....                                             | 15 |
| 8.1.1 | Componente fisica della sicurezza.....                     | 15 |
| 8.2   | Trasmissione e interscambio dei documenti informatici..... | 15 |
| 8.3   | Accesso ai documenti Informatici.....                      | 16 |
| 8.4   | Utenti interni .....                                       | 16 |
| 8.5   | Utenti esterni.....                                        | 16 |

---

## 1 Premessa

AMTAB S.p.A. (di seguito AMTAB) ha adottato il presente Manuale di Gestione Documentale (di seguito Manuale), nel pieno rispetto e quanto stabilito nelle “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici” emanate dall’AGID (Agenzia per l’Italia Digitale).

È parte integrante di questo documento il Manuale del Protocollo Informatico, nel quale è specificato che l’Azienda si è dotata di due Registri di Protocollo: Un protocollo generale gestito dalla segreteria e un protocollo di pertinenza dell’area risorse umane e affari legali ed essa gestito.

Il Manuale descrive il sistema di produzione e gestione informatica dei documenti, la trasmissione, l’interscambio e l’accesso ai documenti informatici nel rispetto della normativa in materia di trattamento e protezione dei dati personali ed in coerenza con quanto previsto aziendali in materia di conservazione; fornisce le indicazioni per la corretta gestione dei flussi documentali e degli archivi informatici.

Il Manuale è destinato alla più ampia diffusione interna ed esterna; si rivolge a tutti i dipendenti ed ai soggetti esterni che si relazionano con l’Azienda ed è reso pubblico mediante la pubblicazione sul sito istituzionale di AMTAB nella sezione “Società Trasparente” e nell’apposita sezione della intranet, in ottemperanza agli obblighi di pubblicità previsti dalle Linee Guida AgiD.

## 2 I Profili Organizzativi

### 2.1 Area Organizzativa Omogenea ed Unità Organizzativa Responsabile

L’Area Organizzativa Omogenea (di seguito AOO) è un insieme di unità organizzative che usufruiscono, in modo omogeneo e coordinato, di comuni servizi informatici per la gestione dei flussi documentali, come descritto nell’art.50, comma 4 e nell’art.61 del d.P.R. n. 445/2000. Essa rappresenta il canale ufficiale per l’invio di istanze e l’avvio di procedimenti amministrativi.

AMTAB ha scelto di configurarsi, ai fini della gestione documentale, con una sola AOO.

Al fine di adempiere alla normativa vigente, AMTAB si è accreditata presso l’indice delle Pubbliche Amministrazioni (iPA), fornendo le informazioni che identificano l’Azienda.

### 2.2 Ruoli e responsabilità

#### 2.2.1 Responsabile della Gestione Documentale

Il Responsabile della Gestione Documentale (RGD), in conformità alle Linee Guida AgiD, garantisce la corretta gestione del protocollo informatico aziendale, dei flussi documentali e la gestione degli archivi (cfr. par.1.2.2) ai sensi dell’art. 61 del Testo Unico sulla Documentazione Amministrativa (di seguito TUDA) e s.m.i.. Egli predispone il Manuale di Gestione Documentale, d’intesa con il Responsabile della Conservazione, con il Responsabile per la Transizione Digitale.

AMTAB, in adempimento a quanto previsto dalla normativa, ha provveduto alla nomina del Responsabile della Gestione Documentale (cfr. par. "Documenti di riferimento per i Ruoli e le Responsabilità").

#### 2.2.2 Servizio per la tenuta del protocollo informatico

In ottemperanza a quanto previsto dall'art. 61 del TUDA e s.m.i., AMTAB, ha istituito una specifica struttura per la tenuta del protocollo informatico consistente nei seguenti: Ufficio Protocollo HR RUL-P (area Risorse Umane e Legale – RUL) e Segreteria (SA).

In particolare, tale struttura è chiamata a gestire i servizi documentali, ivi incluso il protocollo informatico. Per i dettagli si veda l'organigramma aziendale secondo la vigente versione.

### 2.2.3 Responsabile per la Transizione al Digitale

Il Responsabile per la Transizione al Digitale, ai sensi dell'art.17, comma 1, del Codice dell'Amministrazione Digitale (di seguito CAD) e s.m.i., cura la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione dell'amministrazione di riferimento.

Il Responsabile per la Transizione al Digitale, in considerazione della trasversalità del ruolo, svolge funzioni di impulso e coordinamento all'interno dell'azienda, garantendo i compiti espressamente previsti dall'art.17 comma 1 del CAD e s.m.i., ed individuati nella Circolare del Ministro PA n. 3 del 1° ottobre 2018.

In considerazione della trasversalità del ruolo egli è chiamato ad operare in stretta collaborazione con tutte le funzioni apicali aziendali e con le figure espressamente previste dalle normative vigenti, in particolare il Responsabile per la Protezione dei dati personali (cfr. Regolamento UE 2016/679), il Responsabile della prevenzione della corruzione e della trasparenza (cfr. L.190/12 e D. Lgs. n. 337/2013) ed il Responsabile della Gestione Documentale (cfr. d.P.R. n. 445/2000).

AMTAB, in conformità al Codice dell'Amministrazione Digitale, ha nominato il Responsabile per la Transizione al Digitale.

### 2.2.4 Responsabile della Conservazione

Il Responsabile della Conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD<sup>1</sup> e s.m.i.. definisce le politiche complessive del sistema di conservazione (informatico e fisico) e ne governa la gestione direttamente e/o attraverso i soggetti aziendali chiamati a gestire il sistema di conservazione.

In particolare, il Responsabile della Conservazione:

- a) Definisce le politiche di conservazione ed i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che AMTAB svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) Gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) Effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) Effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- g) Al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare

---

<sup>1</sup> L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis".

tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

- h) Predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- i) Assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

AMTAB ha affidato il servizio di conservazione del registro giornaliero di protocollo ad un conservatore esterno, delegandogli le attività suddette o alcune di esse, ad esclusione della predisposizione ed aggiornamento del Manuale di Conservazione.

In ogni caso la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al Responsabile della Conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing da AMTAB.

Oggetto di conservazione è il Registro Giornaliero di Protocollo.

---

## 3 I Documenti

### 3.1 Tipologie di documenti

La seguente classificazione è da applicarsi limitatamente a quei documenti emessi, gestiti e classificati da AMTAB quali "documenti amministrativi", ossia la rappresentazione (analogica o digitale) di atti con cui AMTAB esprime una propria prerogativa prevista per legge o regolamento. In tal senso vengono individuate le seguenti tipologie:

#### 3.1.1 Documento analogico

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

#### 3.1.2 Documento informatico

È un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati anche giuridicamente rilevanti. Il documento informatico è quindi un file digitale indifferente al supporto fisico su cui è memorizzato. Deve essere identificato in modo univoco e persistente:

- 1) nel caso di documenti oggetto di registrazione di protocollo, l'identificazione è rappresentata dalla segnatura di protocollo univocamente associata al documento;
- 2) nel caso di documenti non oggetto di registrazione di protocollo l'identificazione è garantita dalla apposizione della firma digitale.

Le caratteristiche del documento informatico sono:

- a) **Riconducibilità all'autore:** la certezza dell'autore è la capacità di poter associare in maniera certa e permanente il soggetto che lo ha sottoscritto al documento stesso. L'utilizzo del dispositivo, nel caso di firma digitale, si presume riconducibile al titolare, salvo che questi ne dia prova contraria.
- b) **Efficacia giuridico-probatoria:** ai sensi dell'art.20 del CAD il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati

dall'AgID ai sensi dell'articolo 71 del CAD.

In tutti gli altri casi l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.

La data e l'ora di formazione del documento informatico sono opponibili ai terzi, se apposte in conformità alle Linee Guida AgID. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria.

Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa, anche regolamentare, in materia di processo telematico.

- c) **Requisito della forma scritta:** il documento informatico, sottoscritto con firma elettronica qualificata o con **firma digitale**, soddisfa il requisito legale della forma scritta, se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 del CAD e s.m.i., che garantiscano l'identificabilità dell'autore e l'integrità del documento.
- d) **Immodificabilità ed all'integrità:** il documento informatico assume la caratteristica di immodificabilità se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione. La sicurezza di un formato dipende dal grado di modificabilità del contenuto del file e dalla capacità di essere immune dall'inserimento di un codice maligno. L'integrità è l'insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.

## 3.2 Formazione dei documenti

### 3.2.1 Formazione del documento analogico

Nell'attività aziendale, di norma il documento analogico è un documento formato con strumenti analogici o con strumenti informatici (es. documento prodotto con un sistema di videoscrittura e stampato su carta). L'originale analogico è il documento nella sua redazione definitiva, perfetta ed autentica negli elementi formali e sostanziali, comprendente tutti gli elementi di garanzia e di informazione, del mittente e del destinatario e dotato di firma autografa.

I documenti analogici dotati di firma autografa, aventi per destinatario una struttura interna aziendale, un ente o soggetto terzo, vengono protocollati ed inviati/consegnati con le seguenti modalità: in caso di invio tramite pec, il documento in originale rimane agli atti, la copia scannerizzata viene inviata al destinatario; in caso di invio tramite posta o consegna brevi manu, il documento originale viene inviato, la copia rimane agli atti; in caso di notifica attraverso protocollo informatico (protocolli interni) il documento originale rimane agli atti e viene consegnato in copia alla struttura.

Il documento analogico in uscita deve essere redatto su carta intestata, o su altri formati standardizzati secondo quanto definito dalla Corporate Identity aziendale, e deve di norma contenere:

1. data,
2. classificazione,
3. numero di allegati se presenti,
4. oggetto,
5. destinatario,

6. testo,
7. sottoscrizione.

### 3.2.2 Formazione del documento informatico

I documenti informatici redatti/generati da AMTAB sono convertiti nel formato standard PDF e poi formalizzati con firma digitale e/o mediante l'apposizione di sigillo elettronico, garantendo la leggibilità, la non alterabilità durante le fasi di accesso e conservazione, l'immutabilità nel tempo del contenuto e della struttura del documento.

Il documento informatico in uscita deve essere redatto su carta intestata, o su altri formati standardizzati secondo quanto definito dalla Corporate Identity aziendale, e deve di norma contenere:

1. data,
2. classificazione,
3. numero di allegati se presenti,
4. oggetto,
5. destinatario,
6. testo,

Il documento informatico è formato mediante una delle modalità di seguito descritte:

a) **creazione tramite l'utilizzo di strumenti software** (documento nativo digitale), che assicurino la produzione di documenti nei formati suindicati

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**.

In tal caso l'immodificabilità, l'integrità e la conservazione nel tempo sono garantite, oltre che da apposizione di firma digitale e/o apposizione di sigillo elettronico, da una o più delle seguenti operazioni:

- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza (es. protocollo informatico);
- versamento ad un sistema di conservazione digitale a norma.

c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni e/o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

d) generazione a raggruppamento anche in via automatica di un insieme di dati a **registrazioni**, provenienti da una o più banche dati, secondo una struttura logica predeterminata e memorizzata in forma statica.

### 3.3 Tipologie di sottoscrizione

Come già evidenziato AMTAB, quale gestore di pubblici servizi, è tenuta ad allinearsi alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" adottate con determinazione dell'AgID n°.40712020 e successive modifiche ed integrazioni.

Al fine di assicurare la compliance aziendale ai dettami normativi, AMTAB ha regolato l'utilizzo della firma digitale ribadendo "la necessità a tutti i soggetti aziendali coinvolti di approvare i documenti, che hanno efficacia probatoria, di proprio interesse esclusivamente attraverso la firma digitale" ed ha emesso le "Linee Guida per l'utilizzo

della firma elettronica", che fanno parte integrante del presente Manuale.

Di seguito si riportano le principali definizioni relative alle diverse tipologie di firma elettronica utilizzate in azienda.

### 3.3.1 Firma elettronica qualificata

La firma elettronica qualificata è un particolare tipo di firma basata su un sistema di chiavi crittografiche (comunemente chiamate "certificati"), una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica e ad un soggetto terzo (il gestore del servizio) di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti. La firma elettronica qualificata, in base alla definizione contenuta nell'articolo 24 del CAD, si riferisce «in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata», inoltre «integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente». In altre parole, ha lo stesso valore di una firma autografa e comporta le medesime conseguenze, in termini di assunzione di responsabilità, per il sottoscrittore.

In AMTAB l'utilizzo di tale tipologia di firma viene attribuito in funzione del ruolo rivestito nel processo di riferimento ed in particolare è stata conferita a tutti i capi area.

Mediante la firma elettronica qualificata possono essere sottoscritti documenti che abbiano la capacità di vincolare AMTAB con effetti anche patrimoniali, sia interni che esterni, come — ad esempio — contratti, bandi di gara, provvedimenti disciplinari nei confronti di dipendenti, ecc.

## 3.4 Copie di documenti

### 3.4.1 Copia di un documento informatico

La copia di 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 (Esempio: salvare un file da un formato ad un altro da ".doc" a ".pdf", oppure da ".doc" a ".odt" e, più in generale, tutti i formati di documento informatico, licenziati ed in uso in azienda).

### 3.4.2 Copia di un documento analogico

La copia del documento analogico è la trascrizione o riproduzione dell'originale. Si distingue in copia semplice, imitativa e conforme. La copia semplice è la pura trascrizione dell'originale senza riguardo agli elementi formali. La copia imitativa riproduce sia il contenuto che la forma (es. fotocopia). La copia conforme è la copia certificata come conforme all'originale da un pubblico ufficiale autorizzato ad eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autenticata").

### 3.4.3 Copia 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.

Fermo restando quanto previsto dalla legge nel caso in cui non vi sia 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 altro tipo di firma prevista dalla legge, 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 del notaio o del pubblico ufficiale a ciò autorizzato. La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di legge.

### 3.4.4 Duplicato di un documento informatico

Il duplicato del documento informatico è un documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. L'uguale numero e sequenza di bit del duplicato è il risultato di un'operazione di copia incolla o di download del documento originario - ad esempio - su un supporto diverso (come una chiavetta). Pertanto, a differenza delle copie di documenti analogici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

AMTAB nei propri processi si attiene a quanto sopra evidenziato in termini di copia dei documenti.

## 4 Flusso di Lavorazione dei Documenti

Per flusso documentale si intende l'insieme dei documenti che entrano, che escono e/o che vengono prodotti da un ente/amministrazione/azienda.

Alla registrazione dei documenti si provvede con la protocollazione informatica.

### 4.1 Protocollo informatico

Il protocollo informatico è lo strumento, che consente di attribuire un numero univoco, una data ed un'identificazione specifica ad un documento. Tale strumento viene acquisito e gestito dal punto di vista informatico dalla Struttura ICT a supporto del Responsabile della Gestione Documentale.

Obiettivo fondamentale è quello di individuare in maniera inequivocabile ciascun documento attraverso la segnatura di protocollo, cioè l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. L'operazione di segnatura di protocollo è effettuata:

- per i documenti analogici, previa stampa dell'etichetta prodotta dall'applicativo informatico ed apposizione sull'originale del documento/i;
- per i documenti digitali, sottoscritti con firma elettronica qualificata, attraverso l'apposizione della segnatura via sigillo elettronico sul documento/i contestualmente all'allegato dello stesso/i nella scheda di protocollo.

## 5 Uso della Posta Elettronica Certificata

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato:

- mediante messaggi di Posta Elettronica Certificata (PEC), codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche e loro

successive modificazioni o integrazioni;

- mediante messaggi e-mail non PEC, provenienti da cittadini/utenti non dotati di account PEC.

In linea generale AMTAB riceve e invia PEC attraverso il seguente indirizzo istituzionale [info@pec.amtabservizio.it](mailto:info@pec.amtabservizio.it) connesso al sistema di protocollo informatico. Per la gestione della corrispondenza tramite PEC si rimanda al Manuale del Protocollo Informatico.

In alcuni casi specifici, laddove le esigenze di processo lo richiedano, vengono attivati indirizzi di posta elettronica certificata specifici per le Unità Organizzative Responsabili (UOR).

AMTAB ha fornito a ciascun dipendente un indirizzo PEC da utilizzare per comunicazioni ufficiali da e verso l'azienda.

Gli automatismi della posta elettronica certificata consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione del ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno, che sono classificati in:

- Accettazione del messaggio da parte del sistema di posta elettronica certificata
- conferma di ricezione;
- notifica di eccezione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da AMTAB e sono codificati secondo lo stesso standard MIME.

Il servizio di posta elettronica certificata è strettamente correlato all'indice della Pubblica Amministrazione (iPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato sull'iPA, salvo diverse specifiche intese tra le parti. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa, vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale, nei casi consentiti dalla legge, alla notifica per mezzo della posta.

## 6 Gestione Dei Documenti

### 6.1 La classificazione ai sensi del "Titolario di Classificazione"

La classificazione dei documenti<sup>1</sup> consiste in un sistema logico astratto, che ordina i documenti. In base alle funzioni ed alle materie di competenza dell'azienda. Ciò consenta di organizzare in maniera omogenea e coerente i documenti, che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi. Per assolvere a tale obbligo AMTAB ha elaborato e formalizzato un "Titolario di Classificazione" (di seguito Titolario), che costituisce parte integrante del presente Manuale.

### 6.2 Il Titolario di Classificazione

Il Titolario si suddivide in titoli, classi, sottoclassi.

Il titolo individua per lo più funzioni primarie e di organizzazione di AMTAB; le successive partizioni, classi e

sottoclassi, corrispondono a specifiche competenze, che rientrano concettualmente nella macrofunzione descritta dal titolo.

Titoli, classi, sottoclassi sono nel numero prestabilito dal Titolare e non sono modificabili né nel numero né nell'oggetto. Le modifiche e gli aggiornamenti sono attuabili solo se approvate dal Responsabile della Gestione Documentale.

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

Il sistema di protocollazione garantisce la storicizzazione delle variazioni di Titolare e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del Titolare vigente al momento della produzione degli stessi.

Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.

Di norma, le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo Titolare e hanno durata almeno per l'intero anno.

## 6.3 I fascicoli

All'interno di AMTAB si procederà alla gestione dei flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione vigente e relativo piano di organizzazione delle aggregazioni documentali.

Tutti i documenti registrati nel sistema di protocollo informatico e classificati ai sensi del Titolare indipendentemente dal supporto sul quale sono formati, saranno riuniti in fascicoli.

Ogni documento, dopo la classificazione, verranno inserito nel fascicolo di riferimento.

### 6.3.1 Il fascicolo informatico

Il fascicolo informatico è l'aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività.

Il fascicolo informatico reca le seguenti Indicazioni:

- oggetto;
- elenco dei documenti contenuti;
- indice di classificazione (titolo, classe, etc.);
- data di apertura e di chiusura del fascicolo.
- numero del fascicolo, Identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell'anno di creazione;

---

<sup>^</sup> Tele classificazione è formulata ai sensi delle "Linee Guida sulla formazione, gestione e conservazione del documento informatico" emanate dall'AgID.

Il fascicolo informatico è creato da un utente incaricato ed è visualizzabile con possibilità di intervento da parte degli utenti abilitati a operare sui documenti della Unità Organizzativa Responsabile.

Se necessario, i fascicoli possono essere rinominati. Il fascicolo informatico in un sistema totalmente digitale garantisce la possibilità di essere direttamente consultato ed alimentato dalle amministrazioni coinvolte nel procedimento.

Il fascicolo viene chiuso al termine del procedimento o con l'esaurimento dell'attività e la data di chiusura si riferisce alla data dell'ultimo documento prodotto.

Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.

### 6.3.2 Il fascicolo analogico

Si conservano in un fascicolo cartaceo gli atti, i documenti e i dati da chiunque formati su supporto cartaceo. Va mantenuto il formato nativo: possono però essere conservati nei fascicoli, oltre ai documenti nativi analogici, copie analogiche di documenti nativi informatici per non compromettere il vincolo archivistico e garantire la completezza del fascicolo.

### 6.3.3 Il fascicolo ibrido

Nelle more della realizzazione dell'integrale processo di digitalizzazione dei documenti aziendali, in talune fattispecie esiste il "fascicolo ibrido".

Tale fascicolo, inteso come unità logica, può conservare documenti diversi quanto al supporto (documenti analogici e documenti informatici, siano essi originali o derivati da stampa, scansione, web, on line, etc.). Un fascicolo di tale natura occuperà due luoghi distinti (un faldone e un *file system*). Tale peculiarità rende, ovviamente, più complessa la gestione del fascicolo e dei documenti che vi afferiscono: entrambi vanno gestiti correttamente rispettando le caratteristiche proprie del supporto su cui il documento è stato prodotto e deve essere conservato.

Qualora si ravvisi l'utilità di avere tutti i documenti presenti in un fascicolo in un determinato formato, la forma necessaria è quella del fascicolo informatico, in cui inserire le opportune copie per immagine dei documenti nativi analogici.

Se tali copie di documenti analogici devono avere valenza giuridica, per garantire l'opponibilità a terzi, essi devono essere soggetti alla "Certificazione notarile di processo e attestazione di conformità delle copie informatiche di documenti analogici" (cfr. art. 2715 Codice Civile).

Si parla di certificazione di processo solo qualora l'attestazione di conformità venga rilasciata da Notaio o Pubblico Ufficiale a ciò autorizzato e sottoscritta per mezzo della firma digitale o di altra firma elettronica qualificata (ex artt. 22 comma 2 e 23-ter comma 3 del CAD e s.m.i.).

## 7 Archiviazione e Conservazione dei documenti

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 informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento. La gestione va effettuata secondo i principi applicabili in materia di trattamento e protezione dei dati personali anche mediante un'adeguata analisi del rischio. Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi. Dal punto di vista archivistico, si distinguono tradizionalmente tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

In AMTAB, a seconda del processo generante la documentazione oggetto di conservazione, le strutture aziendali *owner* dei relativi documenti gestiscono i relativi archivi e sono chiamate a rispettare gli obiettivi di qualità, efficienza, razionalità, sistematicità e accessibilità, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano.

L'adozione del presente Manuale di Gestione Documentale non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo al quale fa seguito la pubblicazione sul sito istituzionale dell'ente.

### 7.1 Conservazione dei documenti nell'archivio corrente

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

- classificazione di livello superiore, sulla base del Titolario di classificazione di AMTAB;
- fascicolazione del documento, secondo le procedure previste in fase di implementazione.

### 7.2 Conservazione del registro giornaliero di protocollo

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

## 8 Piano di Sicurezza di Gestione Documentale

### 8.1 Obiettivi

In AMTAB è previsto che siano garantite la riservatezza, l'integrità e la disponibilità dei documenti, delle informazioni trattate (cfr. Linea Guida “Classificazione e protezione delle informazioni e dei dati personali” e IL 17.5-81 “Gestione delle informazioni e dei dati personali contenuti nei documenti”). In particolare, si prevede che i dati personali - siano essi dati comuni, dati particolari e/o dati cd giudiziari —vengano trattati 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.

#### 8.1.1 Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi, siti aziendali dove si svolgono le attività di gestione documentale (formazione, gestione e conservazione) è garantito e regolato dalla Direzione Aziendale, secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono essere sottoposti ad apposita procedura di registrazione. Essi possono accedere esclusivamente su invito e previa verifica da parte del personale AMTAB;
- ogni persona che accede alle sedi è identificata in modo certo;
- il personale ha l'obbligo di rispettare le procedure aziendali di accesso

In linea generale, le stesse misure di sicurezza sia informatica che fisica devono essere garantite dai soggetti terzi cui l'Azienda dovesse delegare la gestione e/o la conservazione dei documenti.

### 8.2 Trasmissione e interscambio dei documenti informatici

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

In conformità alla normativa in materia di trattamento e protezione dei dati personali, i certificati ed i documenti trasmessi all'interno di AMTAB, contengono soltanto le informazioni e i dati relativi a stati, fatti e qualità personali che sono strettamente necessari per il perseguimento delle finalità per i quali vengono trattati.

Per quanto concerne i messaggi di posta elettronica, essi vengono trattati con le seguenti modalità:

Posta elettronica certificata: Il server di posta certificata del fornitore esterno (*provider*) di cui si avvale AMTAB, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel *file* di log della posta;
- gestione automatica delle ricevute di ritorno.

- posta elettronica non certificata: il servizio di posta elettronica è gestito da un fornitore esterno di cui si avvale AMTAB.

### 8.3 Accesso ai documenti Informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso, pubblica (*UserID*) e privata (*Password*) ed un sistema di autorizzazione basato sulla profilazione preventiva degli utenti.

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

- Consultazione - per visualizzare in modo selettivo le registrazioni di protocollo eseguite da altri;
- *Protocollo* - per inserire gli estremi di protocollo, effettuare una registrazione di protocollo ed associare i documenti;
- *Modifica* - per modificare i dati opzionali di una registrazione di protocollo;
- *Annullamento* - per annullare una registrazione di protocollo, inserendo apposita motivazione.

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per l'amministratore che per gli utenti.

Le relative politiche di composizione, aggiornamento e, in generale, di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.

Il sistema di Protocollo, (di seguito sdP), fruito dagli utenti di AMTAB:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è possibile associare una *Access Control List* (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il sdP segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati alla sua Unità Organizzativa, o alle strutture ad esse subordinate.

Il sistema consente, altresì, di associare un livello di riservatezza per ogni tipo di documento trattato.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

### 8.4 Utenti interni

La visibilità completa sul registro di protocollo è consentita soltanto all'utente/i con il profilo di utenza di "Responsabile del registro", nonché all'amministratore di sistema.

L'utente assegnatario dei documenti protocollati è invece abilitato ad una visione parziale sul registro di protocollo; tale visione è definita in base alla struttura gerarchica inserita a sistema.

### 8.5 Utenti esterni

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.