



**MANUALE DI GESTIONE DOCUMENTALE DELLA CITTA'
METROPOLITANA DI TORINO**

V01

Area Organizzativa Omogenea CMTO

VERIFICHE E APPROVAZIONI

v.	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
1						

STATO DELLE VARIAZIONI

v.	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
1	Tutto il documento	Versione iniziale

INDICE

1. PRINCIPI GENERALI	8
1.1 Premessa	8
1.2 Ambito di applicazione del manuale	9
1.3 Valore giuridico della registrazione di protocollo	9
1.4 Aree Organizzative Omogenee	9
1.5 Servizio per la gestione informatica del protocollo	10
1.6 Registro giornaliero di protocollo	10
1.7 Caselle di Posta Elettronica	11
1.8 Sistema di classificazione dei documenti	11
1.9 Accredimento dell'AOO all'IPA	11
1.10 Dematerializzazione dei procedimenti amministrativi della AOO	12
2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO	13
3. PIANO PER LA SICUREZZA INFORMATICA	14
3.1- Generalità e obiettivi	14
3.2 Formazione dei documenti - Aspetti di sicurezza	14
3.3 Gestione dei documenti informatici - Aspetti di sicurezza	14
3.4 Componente logica	15
3.5 Componente fisica e infrastrutturale	19
3.6 Gestione delle registrazioni di protocollo e sicurezza	19
3.7 Trasmissione e interscambio dei documenti informatici	21
3.8 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)	22
3.9 All'interno della AOO	22
3.10 Politiche di sicurezza dei sistemi informativi	23

3.11 Tutela dei dati personali	23
4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DEI DOCUMENTI INFORMATICI	27
4.1 Ricezione dei documenti	28
4.2 Spedizione dei documenti	29
4.3 Documento interno formale	29
4.4 Documento interno informale	30
4.5 Formazione dei documenti - Aspetti operativi	30
4.6 Produzione dei documenti informatici - Aspetti operativi	31
4.7 Sottoscrizione di documenti informatici	34
4.8 Firma digitale	34
4.10 Identificazione elettronica	35
4.11 Copie per immagine su supporto informatico di documenti analogici	35
4.12 Copie informatiche di documenti informatici	36
4.13 Estratti informatici di documenti informatici	36
4.14 Copie analogiche di documenti informatici	37
4.15 Copie informatiche e copie analogiche degli Atti amministrativi informatici	37
4.16 Uso della posta elettronica certificata e comunicazioni tra AOO di Documenti Amministrativi Protocollati	38
5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI	40
5.1 Flusso dei documenti in arrivo alla AOO	40
5.1.1 Ricezione dei documenti CARTACEI dall'esterno	40
5.1.2 Ricezione dei documenti trasmessi alla Città Metropolitana tramite fax	42
5.1.3 Ricezione dei documenti DIGITALI trasmessi alla Città Metropolitana	43
5.2 Flusso dei documenti in uscita dalla AOO	49
5.2.1 Registrazione di protocollo e segnatura	49

5.2.2	Trasmissione di documenti informatici	49
5.2.3	Trasmissione di documenti cartacei a mezzo posta	49
5.2.4	Conservazione delle ricevute di trasmissione	50
6.	REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI	52
6.1	Assegnazione dei documenti ricevuti in formato digitale	53
6.2	Assegnazione dei documenti ricevuti in formato cartaceo	53
6.3	Modifica delle assegnazioni	54
7.	ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE	55
8.	SERVIZIO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI	56
8.1	Servizio Archivistico	56
9.	SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI	57
9.1	Protezione e conservazione degli archivi pubblici	57
9.1.1	Caratteristiche generali	57
9.1.2	Misure di protezione e conservazione degli archivi pubblici	57
9.1.3	Conservazione dei documenti digitali	58
9.2	Titolario o Piano di classificazione	58
9.2.1	Titolario	58
9.2.2	Classificazione dei documenti	59
9.3	Strutture aggregative dei documenti	59
9.3.1	Apertura del fascicolo	64
9.3.2	Modifica dell'assegnazione dei fascicoli	64
9.3.3	Apertura del dossier	64
9.3.4	Chiusura delle strutture archivistiche	65
9.4	Consultazione e movimentazione dell'archivio corrente e di deposito	65

9.4.1	Principi generali	65
9.4.2	Consultazione ai fini giuridico-amministrativi	65
9.4.3	Consultazione per scopi storici	65
9.4.5	Gestione e organizzazione dei documenti e dei fascicoli nell'archivio corrente	67
9.4.6	Archivio di deposito	67
10.	MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO	68
10.1	Unicità del protocollo informatico	68
10.2	Registro giornaliero di protocollo	69
10.3	Registrazione di protocollo	69
10.3.1	Documenti informatici	70
10.3.2	Documenti analogici (cartacei e supporti rimovibili)	70
10.3.3	Elementi facoltativi delle registrazioni di protocollo	71
10.4	Segnatura di protocollo dei documenti	71
10.4.1	Documenti informatici	72
10.4.2	Documenti cartacei ricevuti	72
10.5	Annullamento delle registrazioni di protocollo	73
10.6	Livelli di visibilità sulle registrazioni di protocollo	73
10.6.1	Livello di riservatezza dei documenti associati alle registrazioni di protocollo	73
10.7	Documenti non firmati	74
10.8	Protocollazione dei messaggi di posta elettronica ordinaria	74
10.9	Protocollazione di documenti digitali pervenuti erroneamente	75
10.10	Ricezione di documenti cartacei pervenuti erroneamente	75
10.11	Documenti ricevuti per conoscenza	76
10.12	Documenti cartacei in entrata con più destinatari	76
10.13	Differimento delle registrazioni	76

10.14	Registrazioni di protocollo	77
10.14.1	Attribuzione del protocollo	77
10.14.2	Modalità di produzione e archiviazione del registro giornaliero di protocollo informatico	77
11.	MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA	79
11.1	Il registro di emergenza	79
11.2	Modalità di apertura del registro di emergenza	79
11.3	Modalità di utilizzo del registro di emergenza	80
11.4	Modalità di chiusura e di recupero del registro di emergenza	80
12.	REGISTRI PARTICOLARI	81
12.1	Registri delle fatture attive e dei corrispettivi	81
12.2	Registri degli Atti Amministrativi	81
12.3	Registro dei Documenti pubblicati all'Albo Pretorio	82
12.4	Registro dei Contratti	82
12.5	Repertorio del Segretario Generale	82
12.6	Registri delle Convenzioni	82
12.7	Registro dei Contratti di Assunzione	83
13.	APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI	84
13.1	Modalità di approvazione e aggiornamento del manuale	84
13.2	Pubblicità del presente Manuale	84
13.3	Operatività del presente manuale	84
14	ALLEGATI	85
14.1	Elenco caselle di posta elettronica certificata	85
14.2	Titolario di Classificazione	85
14.3	Elenco dei formati ammessi	85

1. PRINCIPI GENERALI

1.1 Premessa

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale (D. Lgs. 82/2005 e ss.mm.ii) prevedono l'adozione del "Manuale di gestione documentale" per tutte le amministrazioni di cui all'articolo 2, comma 2 del CAD.

Il manuale di gestione documentale, redatto secondo quanto previsto dal successivo paragrafo 3.5 delle suddette Linee Guida, "descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi". In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile della gestione documentale preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, di cui agli articoli 50 e 61 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000).

Obiettivo del manuale di gestione è descrivere sia il sistema di gestione dei documenti, anche ai fini della conservazione, a partire dalla fase di formazione e successivamente di registrazione, archiviazione, trasmissione, interscambio e accesso sia le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il manuale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni necessarie per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione dei documenti e descrive i flussi di lavorazione interni all'Amministrazione dei documenti ricevuti, inviati o per uso interno.

Il presente documento, pertanto, si rivolge a tutti i dipendenti dell'ente e ai soggetti esterni che si relazionano con l'amministrazione.

1.2 Ambito di applicazione del manuale

Il presente manuale di gestione è redatto e approvato ai sensi delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, adottate ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale (D. Lgs. 82/2005 e ss.mm.ii.).

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi della Città Metropolitana di Torino.

1.3 Valore giuridico della registrazione di protocollo

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

La data da cui iniziano a decorrere i termini di cui all'art. 1 del «Regolamento per la determinazione dei termini per la conclusione dei procedimenti amministrativi preordinati all'adozione di un provvedimento espresso e per l'individuazione delle unità organizzative responsabili del procedimento», adottato con DCP n.286/6470/1992 del 14 maggio 1992, risulta essere individuata e certificata tramite la segnatura di Protocollo.

1.4 Aree Organizzative Omogenee

Per la gestione unica e coordinata dei documenti l'amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO), denominata "CMTO", nell'ambito della quale è istituito un unico servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

All'interno dell'AOO il sistema archivistico è unico.

All'interno della AOO il sistema di protocollazione è decentrato sia per la posta in arrivo che per la posta in partenza.

1.5 Servizio per la gestione informatica del protocollo

Nella AOO è istituito il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il Responsabile della Gestione Documentale. In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del servizio:

- predisporre lo schema del manuale di gestione documentale con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;
- abilitare gli utenti dell'AOO all'utilizzo del sistema di Gestione Informatica dei documenti e definire per ciascuno di essi il tipo di funzioni più appropriate tra quelle disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta conservazione del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento degli strumenti interni all'AOO e 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 eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollo di emergenza.

1.6 Registro giornaliero di protocollo

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, al termine della giornata lavorativa, il registro

giornaliero di protocollo viene automaticamente archiviato nell'applicativo di gestione documentale in uso nell'Ente.

1.7 Caselle di Posta Elettronica

L'AOO si è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita. Tale casella costituisce il domicilio digitale della AOO e di tutti gli uffici che ad essa fanno riferimento.

Nell'AOO sono altresì presenti caselle di posta elettronica certificata settoriali (allegato 1).

In attuazione di quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18 novembre 2005 sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione ha assegnato ai propri dipendenti, compresi quelli per i quali non sia prevista la dotazione di un personal computer, una casella di posta elettronica ordinaria.

1.8 Sistema di classificazione dei documenti

Considerata l'unicità dell'AOO viene adottato il Titolario di Classificazione dei documenti della Provincia di Torino cui sono state apportate le modifiche necessarie per adeguarlo alle funzioni nella maggior parte ereditate dalla Città Metropolitana di Torino (allegato 2). Il Titolario di Classificazione è uno schema generale di voci logiche, articolate in modo gerarchico che identificano le funzioni e le competenze dell'AOO al quale deve ricondursi la molteplicità dei documenti prodotti e ricevuti dall'AOO con la finalità principale di individuare per ciascun documento la voce finale di appartenenza all'interno di un fascicolo o di una struttura aggregativa definita.

1.9 Accredитamento dell'AOO all'IPA

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA), fornendo le informazioni che individuano l'amministrazione e l'articolazione delle sue AOO.

L'IPA è accessibile, tramite il relativo sito internet, a tutti i soggetti pubblici o privati. L'amministrazione comunica tempestivamente all'IPA ogni modifica delle proprie credenziali di riferimento nonché la data a partire dalla quale la modifica stessa sarà operativa: sarà così garantita l'affidabilità del domicilio digitale indicato.

1.10 Dematerializzazione dei procedimenti amministrativi della AOO

L'amministrazione realizza procedure tali da consentire, in coerenza con le disposizioni normative e regolamentari in materia, che nella AOO siano prodotti, gestiti, inviati e conservati solo documenti informatici.

È prevista la riproduzione su carta dei documenti originali informatici firmati e/o protocollati solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti informatici.

I documenti cartacei ricevuti, dopo registrazione e segnatura di protocollo, vengono conservati in formato cartaceo e non è fatto obbligo che vengano sottoposti a processi di scansione.

2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI PROTOCOLLO INFORMATICO

L'amministrazione ha eliminato i registri di protocollo diversi dal registro ufficiale sin dal 1992.

3. PIANO PER LA SICUREZZA INFORMATICA

3.1- Generalità e obiettivi

La Città Metropolitana di Torino, ai sensi delle Linee Guida – AgID e in conformità alla legislazione vigente in materia di cybersicurezza nazionale, adotta le misure di sicurezza ICT opportune a garantire un livello di sicurezza adeguato al rischio di violazioni in materia di protezione dei dati personali e per il rischio di violazione dei sistemi informatici. L'Ente garantisce che i dati e i documenti trattati dall'Ente siano disponibili, integri e riservati e che i dati sensibili e giudiziari siano conservati con misure adatte a ridurre rischi di distruzione o perdita, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità di raccolta. I principi e le misure indicate nel seguito si applicano anche in caso di affidamento a soggetti esterni delle attività di sviluppo e gestione dei sistemi informatici.

3.2 Formazione dei documenti - Aspetti di sicurezza

I documenti informatici prodotti dalla Città Metropolitana di Torino sono identificati in modo univoco nel sistema di gestione informatica garantendo inalterabilità, riservatezza e fruibilità basata su livelli di riservatezza.

I formati utilizzati per la formazione dei documenti sono elencati nell'allegato 3 *Formati* e rispondono alle esigenze di interoperabilità tra sistemi informatici, accessibilità e leggibilità nel tempo, come disciplinato dalle Linee Guida - AgId.

Le modalità di formazione dei documenti sono descritte nei paragrafi 4.5 e 4.6 del presente manuale.

3.3 Gestione dei documenti informatici - Aspetti di sicurezza

Il sistema di gestione informatica dei documenti adottato dalla Città Metropolitana di Torino è conforme alle specifiche previste dalla normativa vigente. Ai sensi dell'art. 45 del DPR 445/2000:

- a) è garantita la sicurezza e l'integrità del sistema;

- b) è garantita la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
- c) sono fornite informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- d) è consentito il reperimento delle informazioni riguardanti i documenti registrati;
- e) è consentito, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- f) è garantita la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

I paragrafi seguenti esplicitano gli aspetti di sicurezza nelle componenti logiche, fisiche e infrastrutturali.

3.4 Componente logica

Per componente logica si intende il complesso di misure adottate ad impedire l'accesso ai “luoghi digitali” (come server, database, computer, sistema di gestione documentale) da parte di persone non autorizzate. Tali misure prevedono:

- l'identificazione, autenticazione e autorizzazione degli utenti, secondo il principio del privilegio minimo;
- la profilazione degli accessi tramite liste controllate;
- processi per la gestione (creazione, modifica e cancellazione) dei privilegi di accesso per gli utenti e per gli amministratori di sistema;
- l'integrità dei dati e dei flussi;
- il monitoraggio della disponibilità dei sistemi;
- l'adozione di soluzioni di sicurezza perimetrale (es: *firewall applicativi*, strumenti di *intrusion detection e prevention systems*, *protezione anti DDoS*, ecc.)
- strumenti di protezione degli endpoint utilizzati dagli utenti;
- l'impiego di figure professionali specializzate interne o esterne, per il monitoraggio degli eventi (SOC) e per la gestione degli incidenti (CSIRT);

- l'utilizzo di servizi di *Threat Intelligence*;
- l'adozione di politiche di backup dei dati e dei sistemi;
- l'adozione di linee guida per i principi di *Security by design* e *Security by default*.

Le specifiche di sicurezza logiche del sistema di gestione documentale adottato dalla Città Metropolitana di Torino possono essere delegate al soggetto erogatore del servizio, nell'ambito di nomina a Responsabile del Trattamento.

Per quanto riguarda il sistema di gestione informatica dei documenti, dal punto di vista logico, la sicurezza applicativa è definita attraverso delle regole di accesso agli oggetti del sistema che determinano:

- le abilitazioni alle funzionalità di cui possono disporre gli utenti all'interno del sistema;
- le restrizioni agli accessi sugli oggetti condivisi gestiti (serie, fascicoli, ...), in maniera indipendente dalle abilitazioni alle funzionalità.

Gli aspetti che concorrono nella gestione della sicurezza sono:

- *tipologia di dati contenuti* nel documento;
- *profilazione*;
- *controllo degli accessi* (ACL – Access Control List – Lista di Controllo degli Accessi).

La *tipologia di dati contenuti* è applicata alle aggregazioni documentali e ai documenti in modo da renderli visibili ed accessibili all'utente opportunamente profilato. Per *tipologia di dati contenuti* si intendono i seguenti dati:

- *dati personali*: visibili a qualunque tipo di utente;
- *dati particolari e dati relativi a condanne penali e reati*: visibili solo ad opportuni utenti profilati;
- *dati riservati*: visibili solo ad opportuni utenti profilati.

La *tipologia dei dati contenuti* è gestita tramite assegnazione specifica a:

- *aggregazioni documentali*: limita la visibilità dell'aggregazione documentale stessa, dei suoi metadati e di tutti i suoi contenuti;

- *documento*: limita la visibilità del singolo documento, consentendo all'utente l'accesso e la consultazione all'aggregazione documentale che lo contiene.

Per quanto riguarda i dati personali, particolari e riservati, la limitazione della visibilità è indipendente dalla classificazione: un documento con più classificazioni ha sempre la stessa tipologia di dati contenuti.

La tipologia dei dati contenuti è applicata oltre che alla consultazione anche alla ricerca, per cui il risultato di una ricerca rispetta il grado di visibilità dell'utente che l'ha eseguita e quindi presenta le sole aggregazioni documentali e i soli documenti che rispettano tale grado di visibilità.

La *profilazione* è il processo di attribuzione delle funzionalità ad un profilo. Ad ogni utente sono associati uno o più profili in base alle attività che deve svolgere, queste associazioni definiscono le *identità* (associazione utente-profilo).

L'associazione tra utente (CHI), collocazione (DOVE) e profili (COSA) è detta *identità collocata* e rappresenta il ruolo che l'utente riveste nei suoi ambiti lavorativi.

Ogni identità è collocata in una struttura organizzativa dell'Ente (nodo organizzativo) definendo il ruolo che l'utente riveste nel suo ambito lavorativo.

Gli utenti possono essere contemporaneamente collocati in più nodi dell'albero organizzativo andando a definire più identità collocate. Le collocazioni, oltre a descrivere la struttura di appartenenza dell'utente, sono fortemente connesse alla profilazione: l'utente può rivestire ruoli differenti nell'Ente a seconda di dove è collocato in organigramma.

Il *controllo degli accessi* indica se l'utente può applicare una funzionalità ad un certo oggetto del sistema di gestione informatica dei documenti. La gestione delle abilitazioni degli utenti all'accesso ai contenuti avviene attraverso le liste di controllo degli accessi (ACL), associate ad ogni singola aggregazione documentale. Le ACL specificano quali operazioni fondamentali (lettura, modifica, inserimento.) sono possibili e quale gruppo di utenti può compierle. Le ACL sono definite sull'archivio ed in particolare sulle aggregazioni documentali, secondo le regole di seguito descritte.

- *abilitazioni per l'accesso al titolare*: solo chi ha una ben determinata profilazione può accedere alla modifica del Titolare. Su ogni voce di titolare possono essere indicati i *diritti di lavoro* che indicano quali strutture organizzative possono creare aggregazioni documentali in quella voce;
- *abilitazioni per l'accesso ai fascicoli temporanei*: i fascicoli temporanei sono particolari aggregazioni documentali presenti o meno sulle voci di titolare e permettono di effettuare una classificazione temporanea della documentazione in una voce di titolare. Pertanto, è possibile indicare come classificazione temporanea solo le voci a cui è stato attribuito un fascicolo temporaneo. Sono utilizzate dal protocollista in fase di registrazione di un protocollo in arrivo quando non è nota l'aggregazione documentale in cui effettuare la classificazione definitiva. Il protocollista effettuerà poi lo smistamento per competenza alla struttura organizzativa preposta che provvederà alla classificazione definitiva in un'aggregazione documentale;
- *abilitazioni per l'accesso alle strutture aggregative*: le operazioni possibili sulle aggregazioni documentali (serie, dossier, fascicoli, ...) collegate alle ACL sono:
 - *Read* (accesso e lettura dell'aggregazione documentale);
 - *Insert* (creazione dell'aggregazione documentale e sua alimentazione);
 - *Modify* (modifica dell'aggregazione documentale, azioni di riclassificazione, invito, smistamento, ...).

Le aggregazioni documentali hanno tutte un responsabile della materia a cui è associata una ACL con le operazioni di *Read*, *Insert* e *Modify*. Se si deve dare, all'aggregazione documentale, l'accesso ad un'altra struttura organizzativa allora il responsabile della materia può effettuare un invito alla struttura organizzativa indicandone il tipo:

- *Lettura* abilita solo l'operazione *Read*;
- *Alimentazione* abilita le operazioni *Read* e *Insert*;
- *Collaborazione* abilita le operazioni *Read*, *Insert* e *Modify*.

L'invito effettuato creerà la corrispondente ACL;

- *abilitazioni per l'accesso ai documenti*: non è gestito il controllo degli accessi tramite ACL a livello di singolo documento. Quindi la visibilità di un documento dipende dall'identità

collocata associata all'utente e dalla ACL presente sull'aggregazione documentale che lo contiene.

3.5 Componente fisica e infrastrutturale

Per componente fisica si intende il complesso di misure adottate ad impedire l'accesso agli ambienti fisici dove sono custoditi i sistemi hardware che contengono i dati da parte di persone non autorizzate.

Città Metropolitana di Torino attraverso il Consorzio per il Sistema Informativo (CSI-Piemonte), garantisce la sicurezza degli ambienti in cui sono custodite le risorse del sistema informativo attraverso misure quali:

- accesso controllato dei luoghi consentito solo da personale autorizzato;
- registrazione degli accessi;
- utilizzo di strumenti e figure professionali specializzate per la sorveglianza dei locali;
- adeguate misure per la protezione contro gli eventi esterni (incendi, allagamenti, crolli, ecc.);
- sistemi di controllo della temperatura ambientale.

3.6 Gestione delle registrazioni di protocollo e sicurezza

Per quanto riguarda il sistema di gestione informatica dei documenti, dal punto di vista logico, la sicurezza applicativa è definita attraverso delle regole di accesso alle registrazioni di protocollo che determinano:

- le abilitazioni alle funzionalità di cui possono disporre gli utenti all'interno del sistema;
- le restrizioni agli accessi sulle registrazioni di protocollo in maniera indipendente dalle abilitazioni alle funzionalità.

Gli aspetti che concorrono nella gestione della sicurezza sono:

- *riservatezza delle registrazioni di protocollo;*
- *profilazione;*
- *controllo degli accessi (ACL – Access Control List – Lista di Controllo degli Accessi).*

La *riservatezza delle registrazioni di protocollo* è applicata alle singole registrazioni di protocollo in modo da renderle visibili ed accessibili all'utente opportunamente profilato. La riservatezza delle registrazioni di protocollo è applicata oltre che alla consultazione anche alla ricerca.

La *profilazione* è il processo di attribuzione delle funzionalità ad un profilo. Ad ogni utente sono associati uno o più profili in base alle attività che deve svolgere, queste associazioni definiscono le *identità* (associazione utente-profilo).

L'associazione tra utente (CHI), collocazione (DOVE) e profili (COSA) è detta *identità collocata* e rappresenta il ruolo che l'utente riveste nei suoi ambiti lavorativi.

Ogni identità è collocata in una struttura organizzativa dell'Ente (nodo organizzativo) definendo il ruolo che l'utente riveste nel suo ambito lavorativo.

Pertanto, la visibilità delle registrazioni di protocollo e le azioni che si possono fare su di essa possono differire sulla base del profilo dato all'utente: un utente può, ad esempio, consultare solo le registrazioni di protocollo e non crearle, un altro utente può creare le registrazioni e smistarle ma solo per il proprio Settore, un altro utente ancora può creare, ricercare e smistare le registrazioni per tutta l'AOO.

Il *controllo degli accessi* indica se l'utente può applicare una funzionalità ad una registrazione di protocollo. La gestione delle abilitazioni degli utenti all'accesso alle registrazioni di protocollo avviene attraverso le liste di controllo degli accessi (ACL), associate ad ogni singola registrazione. Le ACL specificano quali operazioni fondamentali (lettura, modifica, inserimento...) sono possibili e quale gruppo di utenti può compierle. Le ACL sono definite sul registro di protocollo ed in particolare sulle registrazioni di protocollo, secondo le regole di seguito descritte.

- *abilitazioni per l'accesso al registro di protocollo*: solo chi ha una ben determinata profilazione può accedere alla modifica di alcuni metadati del registro di protocollo;
- *abilitazioni per l'accesso alle registrazioni di protocollo*: le operazioni possibili sulle registrazioni di protocollo collegate alle ACL sono:
 - *Read* (accesso e lettura della registrazione di protocollo);
 - *Insert* (creazione della registrazione di protocollo);

- *Modify* (modifica dei soli metadati modificabili della registrazione di protocollo, azioni di smistamento, invio segnatrice, ...).

Le registrazioni di protocollo hanno tutte un responsabile a cui è associata una ACL con le operazioni di *Read*, *Insert* e *Modify*, altresì è presente il protocollante che indica la struttura che effettua la protocollazione. Responsabile e protocollante sono uguali all'atto della registrazione di protocollo ma possono differire a seguito di modifiche organizzative dell'Ente: il protocollante non cambia mai, cambia invece il responsabile. Se si deve dare, al registro di protocollo o ad una singola registrazione di protocollo, l'accesso ad un'altra struttura organizzativa allora il responsabile può effettuare un invito alla struttura organizzativa indicandone il tipo:

- *Lettura* abilita solo l'operazione *Read*.

L'invito effettuato creerà la corrispondente ACL

3.7 Trasmissione e interscambio dei documenti informatici

Gli addetti della AOO 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.

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.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO, 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 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.

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

3.8 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente (articolo 55, comma 4, del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato .MIME per la codifica dei messaggi. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

3.9 All'interno della AOO

Tutte le informazioni trasmesse internamente alla Città Metropolitana di Torino contengono solamente i dati di cui è consentita la diffusione e strettamente necessari per il perseguimento delle finalità per le quali vengono interscambiati.

Come sicurezza sulla trasmissione sono presi in considerazione i sistemi di sicurezza che partono da cifratura di canale (TSL 1.2), autenticazione applicativa, riconoscimento e profilazione utenti.

3.10 Politiche di sicurezza dei sistemi informativi

Il Responsabile della sicurezza insieme al Responsabile della tutela dei dati personali si occupano di verificare, perfezionare e divulgare le politiche di sicurezza dell'Ente volte a stabilire le misure per la tutela e l'accesso al patrimonio informativo e per la gestione di incidenti informatici.

Con Determinazione Dirigenziale n. 4861/2022 del 23/09/2022, è stato approvato il "Disciplinare per l'utilizzo degli strumenti informatici", attraverso il quale la Città Metropolitana di Torino fornisce a Dipendenti e Collaboratori le modalità d'utilizzo degli strumenti aziendali e le istruzioni da seguire durante lo svolgimento delle attività lavorative che comportano un trattamento di dati personali, al fine di evitare che, anche inconsapevolmente, possano minacciare o compromettere la sicurezza del sistema informatico aziendale o la protezione dei dati ivi contenuti o arrecare un qualunque danno all'azienda (economico o di immagine).

3.11 Tutela dei dati personali

I soggetti esterni a cui è delegata la tenuta del sistema di conservazione sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del *General Data Protection Regulation* (GDPR, Regolamento UE 2016/679) e garantisca la tutela dei diritti dell'interessato in conformità all'art. 28 del GDPR.

Detto ciò, la Città Metropolitana di Torino nomina, attraverso una convenzione, un soggetto esterno quale Responsabile Esterno del trattamento dei dati personali. Il soggetto nominato è tenuto a:

- a) adottare le misure organizzative, tecniche, procedurali e logistiche sulla sicurezza nei trattamenti concordate con il Titolare, indicate in dettaglio per ciascuna attività nelle CTE/PTE tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, nonché assicurarsi che le misure di sicurezza predisposte e adottate siano adeguate a garantire un livello di sicurezza adeguato al rischio, in particolare contro:

- a. distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- b. trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento;
- b) individuare, verificare e, in caso, aggiornare in funzione delle istruzioni fornite dal Titolare le persone fisiche incaricate a trattare i dati in relazione a ciascuna area di trattamento;
- c) garantire - anche in accordo con il delegato del Titolare - che gli incaricati al trattamento dei dati personali si attengano alle istruzioni e alle procedure di volta in volta indicate specificatamente, sia oralmente che per iscritto nonché rispettino gli obblighi di segretezza e riservatezza e abbiano ricevuto la formazione necessaria in materia di protezione dei dati personali;
- d) assistere il delegato del Titolare nel garantire il rispetto degli obblighi relativi alla valutazione d'impatto sulla protezione dei dati nonché alla eventuale consultazione preventiva all'Autorità di Controllo;
- e) se richiesto, assistere il delegato del Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare le eventuali richieste per l'esercizio dei diritti dell'interessato;
- f) se richiesto, assistere il delegato del Titolare del trattamento nel garantire il rispetto degli obblighi in materia di violazione dei dati (*data breach*) tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- g) comunicare ogni eventuale trasferimento di dati e informazioni verso paesi terzi extra UE o organizzazioni internazionali, anche per fini tecnici connessi ai servizi di *Providing* e *backup* utilizzati in azienda.

In caso di danni derivanti dal trattamento, il Responsabile del trattamento dei dati ne risponderà qualora non abbia adempiuto agli obblighi della normativa pro tempore vigente in materia o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del delegato del Titolare.

Ogni trattamento dei dati succitati, da effettuarsi solamente in conformità alle finalità come sopra definite, dovrà essere limitato al tempo necessario a dare esecuzione alla convenzione stipulata tra le parti. Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte del Responsabile del trattamento dei dati, quest'ultimo sarà

tenuto a restituire al delegato del Titolare i dati personali oggetti del trattamento oppure a provvedere alla loro integrale distruzione salvo i casi in cui la conservazione dei dati sia richiesta da norme di legge o altri fini (contabili, fiscali, ecc.). In entrambi i casi il Responsabile provvederà a rilasciare al delegato del Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni del Titolare. Il delegato Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

Per tutte le specifiche si rimanda alle convenzioni attualmente in uso.

Per garantire il rispetto delle norme in materia di protezione dei dati personali la Città Metropolitana di Torino ha definito l'organizzazione in materia di privacy che prevede i seguenti ruoli:

- *Responsabile della protezione dei dati - RPD (detto anche DPO – Data Protection Officer).*
È il ruolo che sorveglia l'osservanza delle norme in materia di protezione dei dati, informa e fornisce consulenza sugli obblighi che derivano dalle norme, è il punto di contatto sia per l'Autorità Garante sia per i dipendenti ed il cittadino;
- *Delegato del trattamento.* I Dirigenti sono i soggetti delegati nel rispettivo ambito di competenza, in conformità all'assetto organizzativo della Città Metropolitana di Torino e alle disposizioni del Regolamento della Città Metropolitana di Torino per l'attuazione del regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- *Referenti privacy.* Sono i dipendenti dell'Ente Città Metropolitana di Torino che hanno i seguenti compiti:
 - a) supportare il Dirigente nello svolgimento dei diversi compiti assegnati in materia di tutela dei dati personali;
 - b) costituire il primo punto di riferimento delle strutture assegnate per le questioni relative alla tutela dei dati personali;
 - c) partecipare alle iniziative informative, formative e di sensibilizzazione in materia di protezione dei dati personali organizzate dall'Ufficio DPO al fine di accrescere la "cultura della privacy" nell'Ente.

- *Autorizzati.* Tutti i dipendenti dell'Ente Città Metropolitana di Torino sono autorizzati in via generale a effettuare trattamento di dati personali in relazione al profilo professionale, alla funzione organizzativa di appartenenza e all'attività svolta.

Si elenca, di seguito, la documentazione predisposta dalla Città Metropolitana di Torino inerente alle modalità e all'organizzazione attuata per la gestione della privacy e la protezione dei dati:

- Regolamento della Città Metropolitana di Torino per l'attuazione del regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- Vademecum privacy;
- Politica di Data Breach della Città Metropolitana di Torino;
- Determinazione Dirigenziale n. 4861/2022 del 23/09/2022, "Disciplinare per l'utilizzo degli strumenti informatici".

4. MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DEI DOCUMENTI INFORMATICI

La presente sezione fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per la formazione e lo scambio di documenti all'interno ed all'esterno dell'AOO.

Ai sensi dell'art. 40, comma 1 del D.Lgs. n. 82/2005 (CAD) “le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le Linee guida”.

La Città Metropolitana forma documenti amministrativi informatici ai sensi delle Linee Guida. Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici.

Si definisce documento amministrativo informatico ogni rappresentazione del contenuto di atti, anche interni, formati dalla pubblica amministrazione, o, comunque, da questa ultima utilizzati ai fini dell'attività amministrativa.

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

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

Il documento amministrativo oggetto di scambio, in termini tecnologici, è così classificabile:

- informatico;
- analogico.

4.1 Ricezione dei documenti

La fase di ricezione è riferita ai documenti che l'AOO riceve dall'esterno, per i quali è tenuta a registrare l'ingresso tramite l'associazione di un numero progressivo di protocollo, completo di data, ora, oggetto, mittente (= segnatura di protocollo).

Le modalità di ricezione sono:

- posta elettronica certificata (PEC), di norma la ricezione dei documenti informatici è assicurata tramite caselle di posta elettronica certificata (istituzionale e settoriali), accessibili alle Direzioni responsabili delle caselle. Le caselle sono associate al Registro di protocollo garantendo così l'acquisizione automatica dei documenti;
- posta elettronica ordinaria (PEO), la ricezione dei documenti informatici è assicurata tramite caselle di posta elettronica ordinaria. Le caselle che sono associate al Registro di protocollo garantiscono l'acquisizione automatica dei documenti;
- piattaforma telematica, in seguito a presentazione di istanze on-line, i documenti seguono il flusso di workflow di business, comprensivo di protocollazione e archiviazione;
- cooperazione applicativa, in seguito a integrazione tra sistemi informativi il documento viene automaticamente acquisito e protocollato;
- presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- consegna a mano, a mezzo posta o fax (non tra P.A.) di documenti analogici o informatici su supporto magnetico/ottico.

La ricezione dei documenti avviene inoltre tramite acquisizione automatica dei documenti in archivio attraverso le seguenti modalità:

- *alimentazione puntuale sincrona*: prevede che gli applicativi gestionali di ciascuna filiera documentale richi amino i servizi di archiviazione esposti dall'applicativo di gestione documentale;
- *alimentazione massiva asincrona*: gestita in automatico dal sistema, passa attraverso la definizione a priori delle porzioni di archivio da alimentare, congiuntamente al popolamento di un xml che contiene i metadati obbligatori definiti dall'archivista a corredo dei documenti.

4.2 Spedizione dei documenti

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma tramite caselle di posta elettronica ordinaria o caselle di posta elettronica certificata qualora necessitino di una ricevuta di invio e di una ricevuta di consegna.

I documenti informatici, compresi di eventuali allegati possono inoltre essere messi a disposizione degli utenti esterni sulle piattaforme telematiche utilizzate per la ricezione e gestione di istanze on – line.

La spedizione a privati cittadini può avvenire anche utilizzando la posta ordinaria, la posta raccomandata, il fax.

4.3 Documento interno formale

I documenti interni formali sono formati con tecnologie informatiche e prodotti in formato non modificabile.

Quando il documento risulta ben formato e atto ad assolvere le funzioni per cui è stato prodotto viene inserito nel sistema di gestione documentale all'interno dell'appropriata struttura aggregativa nella porzione di titolare che riguarda la materia trattata, su cui è definita una responsabilità specifica da Organigramma.

La trasmissione all'interno dell'AOO avviene tramite la funzione di smistamento.

Solo nei casi in cui la trasmissione dovesse avvenire nei confronti di una pluralità di soggetti non censiti nell'Organigramma del sistema di gestione documentale (ad esempio: tutti i Direttori, tutti i Dirigenti, tutti o parte dei dipendenti, ecc.) viene utilizzata la posta elettronica. Il documento viene comunque archiviato nel sistema di gestione documentale.

I documenti formali interni sono sottratti all'obbligo di protocollazione ad eccezione di quelli che si inseriscono nel procedimento amministrativo e sono tra loro coordinati e preordinati all'adozione del provvedimento quale atto finale del procedimento (quali ad esempio pareri, accordi preliminari, designazioni, esiti di istruttorie tecniche o amministrative)¹.

¹ Cfr. Regolamento di protocollazione e archiviazione dei documenti approvato con DCP 340512/2003.

4.4 Documento interno informale

I documenti interni informali sono formati con tecnologie informatiche e prodotti in formato anche modificabile.

Possono essere inseriti nel sistema di gestione documentale all'interno dell'appropriata struttura aggregativa nella porzione di titolario che riguarda la materia trattata, su cui è definita una responsabilità specifica da Organigramma.

La trasmissione all'interno dell'AOO avviene tramite la posta elettronica.

La funzione di smistamento presente nel sistema di gestione documentale viene utilizzata per i documenti informali per i quali si necessita di data certa di invio da parte dell'ufficio mittente e di data certa di presa in carico o di rifiuto da parte dell'ufficio ricevente.

I documenti informali interni sono sottratti all'obbligo di protocollazione.

4.5 Formazione dei documenti - Aspetti operativi

I documenti dell'amministrazione sono prodotti con sistemi informatici, come previsto dalla vigente normativa. Ogni documento è formato per essere inoltrato formalmente all'esterno o all'interno dell'Amministrazione.

Il documento deve consentire l'identificazione dell'amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della Direzione che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero civico, CAP, città, provincia);
- il numero di telefono della Direzione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- la data (giorno, mese, anno);
- il numero degli allegati, se presenti;
- l'oggetto;

- sottoscrizione digitale del responsabile procedimento amministrativo.

4.6 Produzione dei documenti informatici - Aspetti operativi

La fase di produzione di un documento è generalmente gestita esternamente al sistema di gestione documentale, da opportune procedure gestionali (ad esempio: Atti amministrativi, Bilancio, Applicazioni di workflow, ecc) o direttamente da strumenti di word processing o da 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 o tramite generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Al termine della sua formazione, il documento informatico possiede le seguenti cinque caratteristiche fondamentali:

- 1. staticità:** assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni (es: link) o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione;
- 2. integrità:** dotato di caratteristiche che ne dichiarano la qualità di essere completo ed inalterato. L'integrità del documento è garantita attraverso l'impronta, ovvero la sequenza di simboli binari di lunghezza fissa ottenuta attraverso l'applicazione di una specifica funzione di calcolo (SHA 256) alla rappresentazione digitale del documento che garantisce una associazione biunivoca tra l'impronta stessa ed il documento su cui è stata calcolata;
- 3. immutabilità:** non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e di successiva conservazione;
- 4. leggibilità:** le informazioni in esso contenute sono fruibili durante l'intero ciclo di gestione;
- 5. autenticità:** il documento informatico è riconducibile con certezza alla volontà del suo autore senza aver subito alterazioni o modifiche.

L'imputabilità di un documento al suo autore è garantita dalla sottoscrizione; per il documento informatico si è reso necessario concepire una **sottoscrizione elettronica** in grado di assicurare il legame tra il firmatario e il documento informatico.

Una volta conclusa la redazione del documento, il sistema di gestione documentale può gestire il giro di visto/i e firma/e, se non è già stato compiuto all'interno della procedura gestionale oppure se il documento non è stato ancora sottoscritto. Il processo parte dall'inserimento del documento all'interno dell'appropriata struttura aggregativa (ad es. serie tipologica, fascicolo, dossier) nella porzione di titolare che riguarda la materia trattata, su cui è definita una responsabilità specifica da Organigramma. Al termine del flusso di visto e firma, il documento risulta ben formato e atto ad assolvere le funzioni per cui è stato prodotto (perfetto ed efficace). Nel caso in cui la procedura gestionale fornisca un documento già perfezionato (completo di visti e firma), il sistema di gestione documentale può acquisirlo via servizi applicativi o tramite procedure massive.

Per attribuire una data certa a un documento informatico firmato digitalmente prodotto all'interno della AOO, si applicano le regole per la validazione temporale di cui al DPCM 22 febbraio 2013, pertanto le firme necessarie al perfezionamento, sotto il profilo giuridico, del documento in partenza devono essere apposte prima della sua protocollazione.

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'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.

Nel momento in cui il documento informatico viene inserito nel sistema di gestione documentale ad esso vengono associati i metadati. Il set di metadati per i documenti amministrativi

informatici, è definito nell'allegato 5 alle Linee Guida in base al quale la Città Metropolitana ha individuato i seguenti metadati minimi:

per i documenti non protocollati

- Impronta;
- Algoritmo;
- Identificativo (UUID);
- Data registrazione (se registrato su registri ufficiali dell'AOO diversi dal registro di protocollo);
- Numero di registrazione del documento (se registrato su registri ufficiali dell'AOO diversi dal registro di protocollo);
- Oggetto;
- Numero degli allegati;
- Identificativo del documento relativo all'allegato (impronta, algoritmo UUID);
- Oggetto dell'allegato (descrizione);
- Indice di classificazione esteso;
- Presenza firma digitale;
- Presenza sigillo elettronico;
- Presenza marca temporale;
- Tracciamento della modifica;
- Codice fiscale autore della modifica;
- Data della modifica.

per i documenti protocollati

- Impronta;
- Algoritmo;
- Identificativo (UUID);
- Segnatura di protocollo;
- Tipologia di flusso (arrivo/partenza/interno);
- Data registrazione di protocollo;
- Numero di protocollo;
- Oggetto;

- Mittente;
- Destinatario;
- Numero degli allegati;
- Identificativo del documento relativo all'allegato (impronta, algoritmo UUID);
- Oggetto dell'allegato (descrizione);
- Indice di classificazione esteso;
- Presenza firma digitale;
- Presenza sigillo elettronico;
- Presenza marca temporale;
- Tracciamento della modifica;
- Codice fiscale autore della modifica;
- Data della modifica.

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

4.7 Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, al fine di garantirne l'immodificabilità, sono convertiti in uno dei formati standard previsti dalla normativa vigente che possono maggiormente garantire il principio dell'interoperabilità tra i sistemi di gestione documentale e conservazione (Allegato 5 alle Linee Guida) ed elencati nelle linee guida in materia di dematerializzazione dei documenti e utilizzo della posta elettronica certificata deliberate dall'Ente.

4.8 Firma digitale

La firma digitale è utilizzata per inviare e ricevere documenti per l'AOO con valenza giuridico-probatoria.

L'acquisizione del documento all'interno del sistema di gestione documentale prevede la verifica della firma digitale e la produzione di un rapporto di verifica che viene archiviato sotto forma di metadati del documento.

I passi di verifica previsti sono:

- 1 Verifica conformità e integrità della busta crittografica;
- 2 Sbustamento della busta crittografica;
- 3 Verifica della consistenza della firma;
- 4 Verifica della validità del certificato di firma;
- 5 Verifica dell'Ente certificatore (CA - Certification Authority);
- 6 Verifica della lista di revoca del certificato (CRL – Certificate Revocation List);
- 7 Verifica lista di revoca – certificato non presente nella CRL.

Il rapporto di verifica con esito positivo garantisce il valore giuridico del documento dal suo ingresso nel sistema di gestione documentale. Una volta acquisito, il sistema di gestione documentale archivia il documento congiuntamente ai metadati relativi al rapporto di verifica e ai dati del certificato del firmatario.

4.10 Identificazione elettronica

Per i documenti provenienti dall'esterno e formati tramite compilazione di moduli on line, la Città Metropolitana consente l'autenticazione tramite sistemi di identificazione elettronica ai sensi dell'art. 20 comma 1bis del D.Lgs. 7 marzo 2005 n. 82 – Codice dell'Amministrazione Digitale.

4.11 Copie per immagine su supporto informatico di documenti analogici

Le copie per immagine su supporto informatico di documenti analogici sono prodotte con sistemi esterni al sistema di gestione documentale. Esse si ottengono tramite scansione del documento cartaceo e raffronto del documento originale e della copia per immagine.

L'attestazione di conformità della copia per immagine su supporto informatico di un documento analogico viene prodotta su un documento informatico separato, in formato immutabile che viene unito alla copia per immagine tramite funzionalità di unione file. I due documenti devono essere prodotti nello stesso formato. Il documento così ottenuto (copia per immagine e attestazione di conformità) viene sottoscritto con firma digitale dal pubblico ufficiale a ciò autorizzato.

4.12 Copie informatiche di documenti informatici

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 oppure è un documento privo delle firme digitali e/o marche temporali che sono apposte sul documento originale.

Le copie informatiche di documenti informatici si producono con sistemi esterni al sistema di gestione documentale cui segue il raffronto fra i documenti al fine di assicurare la conformità del contenuto della copia alle informazioni del documento informatico di origine.

L'attestazione di conformità della copia informatica di un documento informatico viene prodotta su un documento informatico separato, in formato immutabile che viene unito alla copia tramite funzionalità di unione file. I due documenti devono essere prodotti nello stesso formato. Il documento così ottenuto (copia e attestazione di conformità) viene sottoscritto con firma digitale dal pubblico ufficiale a ciò autorizzato.

4.13 Estratti informatici di documenti informatici

L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto.

Gli estratti si producono con sistemi esterni al sistema di gestione documentale cui segue il raffronto fra i documenti al fine di assicurare la conformità del contenuto dell'estratto informatico alle informazioni del documento informatico di origine

Per *estratto di un documento* si intende quindi un nuovo documento che, a partire da un documento di origine, contiene una porzione del patrimonio informativo originario. Gli estratti dei documenti possono essere generati per poter fornire copia del documento originale al quale sono applicati degli omissis.

L'attestazione di conformità dell'estratto informatico di un documento informatico viene prodotta su un documento informatico separato, in formato imm modificabile che viene unito all'estratto tramite funzionalità di unione file. I due documenti devono essere prodotti nello stesso formato. Il documento così ottenuto (estratto e attestazione di conformità) viene sottoscritto con firma digitale dal pubblico ufficiale a ciò autorizzato.

4.14 Copie analogiche di documenti informatici

Le copie analogiche di documenti informatici si ottengono attraverso la stampa del documento informatico. È prevista la riproduzione su carta dei documenti originali informatici firmati e/o protocollati solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti informatici.

L'attestazione di conformità della copia analogica all'originale informatico viene prodotta dal sistema di gestione documentale mediante la funzionalità di rendition.

4.15 Copie informatiche e copie analogiche degli Atti amministrativi informatici

Le copie informatiche e le copie analogiche degli Atti amministrativi informatici vengono prodotte dal sistema gestionale di produzione degli Atti stessi.

Le attestazioni di conformità di tali copie vengono parimenti prodotte dal sistema gestionale di produzione degli Atti stessi.

L'attestazione di conformità della copia analogica all'originale informatico dell'Atto amministrativo informatico viene prodotta anche dal sistema di gestione documentale mediante la funzionalità di rendition.

4.16 Uso della posta elettronica certificata e comunicazioni tra AOO di Documenti Amministrativi Protocollati

Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo. Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- convertirlo in uno dei formati che ne garantisca l'immodificabilità elencati nelle linee guida in materia di dematerializzazione dei documenti e utilizzo della posta elettronica certificata deliberate dall'Ente;
- apporvi la firma digitale;
- inserirlo nel sistema di gestione documentale, all'interno della struttura aggregativa relativa al procedimento di cui tratta;
- smistarlo per protocollazione in partenza;
- inserire i dati del destinatario: denominazione, indirizzo, casella di posta elettronica (ricavati dalla funzionalità AOO – Interscambio presente nella ricerca anagrafica del protocollo informatico);
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- invio del messaggio contenente il documento firmato e protocollato in uscita alla casella di posta del destinatario.

L'utilizzo della posta elettronica certificata (PEC) consente di:

- validare temporalmente la firma digitale;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;

- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti ad altre amministrazioni.

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

I messaggi di ritorno, che sono classificati in:

- conferma di protocollazione del messaggio di protocollo da parte della AOO destinataria alla AOO mittente;
- anomalia riscontrata sul messaggio di protocollo ricevuto (000_irricevibile, 001_validazione firma, 002_ anomalia impronta) da parte della AOO destinataria alla AOO mittente;
- annullamento di protocollazione sia da parte della AOO mittente qualora annulli il messaggio di protocollo precedentemente inviato, sia da parte della AOO destinataria qualora annulli il messaggio di protocollo precedentemente ricevuto;
- sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

Per assicurare la comunicazione tra AOO la Città Metropolitana ha registrato e mantiene aggiornato l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. 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.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

I documenti vengono inviati alla Città Metropolitana per mezzo della posta elettronica ordinaria, posta elettronica certificata, portali dedicati, piattaforme telematiche, modulistica on line, del servizio postale, dei corrieri, tramite il recapito a mano, tramite fax (ma non tra P.A.).

I documenti prodotti dagli uffici della Città Metropolitana vengono spediti per mezzo di posta elettronica ordinaria, posta elettronica certificata, messa a disposizione su piattaforme telematiche, utilizzo di portali dedicati, fax (ma non tra P.A.) e in via residuale tramite servizio postale.

5.1 Flusso dei documenti in arrivo alla AOO

Per documenti in arrivo si intendono i documenti acquisiti dalla Città Metropolitana di Torino nell'esercizio delle proprie funzioni.

5.1.1 Ricezione dei documenti CARTACEI dall'esterno

La posta cartacea perviene presso la Città Metropolitana di Torino attraverso i seguenti canali:

- la posta viene ritirata al mattino presso la Sede centrale di Poste Italiane - Via Alfieri 10 – dal personale addetto dell'Ente e depositata presso l'Ufficio Protocollo Generale che provvede all'apertura delle buste e agli altri adempimenti di propria competenza;
- la posta recapitata a mano o per corriere viene consegnata all'Ufficio Protocollo Generale (anche quella ritirata in via eccezionale dall'URP o dalla Portineria);
- la posta recapitata a mano presso gli sportelli individuati dall'Ente viene ritirata dagli sportelli stessi.

5.1.1.1 Corrispondenza inoltrata all'ufficio Protocollo Generale

All'Ufficio Protocollo Generale viene consegnata la posta cartacea ritirata presso l'ufficio postale e viene consegnata la posta recapitata a mano o tramite corriere.

La posta viene consegnata all'Ufficio Protocollo dopo le 10 del mattino.

L'Ufficio Protocollo apre la posta e provvede alla protocollazione delle raccomandate A/R e della corrispondenza ordinaria soggetta a obbligo di protocollazione. Il timbro di protocollo, riportante numero e data di protocollo viene obbligatoriamente apposto sulla lettera e non sulla busta. Le buste delle lettere vengono pinzate alla lettera stessa.

Tutta la corrispondenza aperta e timbrata viene depositata nell'apposito casellario o nelle apposite cartelline affinché possa essere ritirata dagli uscieri e consegnata agli uffici di destinazione.

5.1.1.2 Apertura della corrispondenza

Al fine di garantire modalità uniformi nella gestione della corrispondenza, dal momento che la corrispondenza che giunge alla Città Metropolitana riguarda l'attività svolta dall'Ente nella realizzazione delle proprie funzioni, si è stabilito di aprire tutta la corrispondenza sulla quale non sia riportata una dicitura del tipo "Riservata", "Personale", "Confidenziale", anche quando essa sia indirizzata nominativamente.

Non vengono aperte, ma vengono timbrate esclusivamente sulla busta con timbro datario riportante la dicitura "Città Metropolitana di Torino" e la data di ricezione della posta presso l'ufficio Protocollo stesso le lettere e i plichi relativi a:

- offerte per gare di appalto e/o procedure negoziate e/o acquisto di immobili che in via residuale vengono consegnate in formato cartaceo; nel giorno di scadenza delle offerte vicino al timbro datario viene apposta anche l'ora di consegna della busta e la sigla dell'impiegato che la ha ricevuta; successivamente le buste vengono consegnate alla Direzione competente. Per motivi organizzativi, tutte le Direzioni sono tenute ad informare con congruo anticipo il Responsabile del servizio di protocollo in merito alle scadenze di gare e bandi di ogni genere;
- associazioni che hanno sede presso i locali della Città Metropolitana, ma che non sono uffici dell'Ente, quali, a titolo esemplificativo e non esaustivo, l'ANCI.

Nel caso in cui una lettera contenga dati personali e/o dati sensibili e/o dati riservati, essa viene aperta, protocollata timbrata e poi riposta nella busta che viene nuovamente chiusa tramite pinzatrice.

5.1.1.3 Atti giudiziari

Gli atti giudiziari vengono consegnati a mano all'Ufficio Protocollo dall'ufficiale Giudiziario oppure vengono inoltrati per posta.

- Se l'atto viene consegnato a mano, sul medesimo non viene apposto alcun timbro. Viene fatta una fotocopia dell'atto sulla quale viene apposta la data di ricezione dell'atto da parte dell'ufficio competente e la firma del dipendente che ritira l'atto trasmesso dall'ufficio Protocollo. L'atto viene trasmesso all'ufficio competente in busta chiusa.
- Se l'atto perviene tramite il servizio postale, oltre alla compilazione del modulo di cui sopra, viene apposta sulla busta del medesimo il timbro datario e viene fotocopiata la busta.

5.1.1.4 Rilascio di ricevuta di un documento consegnato a mano

A richiesta dell'interessato, l'Ufficio Protocollo appone il timbro datario o di protocollo su una fotocopia del documento consegnato a mano all'ufficio stesso. Tale fotocopia deve essere fornita dall'utente interessato ed ha valore di ricevuta.

5.1.1.5 Errata ricezione di documenti cartacei

Se la busta è indirizzata ad altro soggetto viene restituita al servizio postale per il recapito all'indirizzo corretto.

Se la busta è indirizzata alla Città Metropolitana, ma all'interno contiene documenti destinati ad altro soggetto, essa viene chiusa con pinzatrice e restituita al servizio postale per il recapito all'indirizzo corretto.

5.1.1.6 Corrispondenza consegnata agli sportelli dell'Ente

La corrispondenza consegnata a mano agli sportelli individuati dall'Ente, viene aperta e protocollata dagli impiegati assegnati agli sportelli medesimi con successiva consegna del documento stesso presso l'ufficio interessato.

5.1.2 Ricezione dei documenti trasmessi alla Città Metropolitana tramite fax

I documenti che vengono trasmessi alla Città Metropolitana tramite fax pervengono sulle caselle di posta elettronica ordinaria associate al sistema di fax server. Il sistema di fax server li

trasforma in file in formato .pdf. I documenti ricevuti a mezzo fax, ove rientrino nella casistica dei documenti soggetti a registrazione obbligatoria di protocollo, vanno protocollati e il file che li rappresenta deve essere associato alla registrazione di protocollo.

I documenti ricevuti a mezzo fax che non sono soggetti a registrazione obbligatoria di protocollo, possono comunque essere inseriti in una struttura aggregativa all'interno dell'archivio digitale del sistema di gestione documentale.

Ai sensi dell'art. 47, comma 2, lett. C del D. Lgs. 82/2005 (CAD) è esclusa la trasmissione di documenti tra P.A. tramite fax.

5.1.3 Ricezione dei documenti DIGITALI trasmessi alla Città Metropolitana

5.1.3.1 Ricezione tramite posta elettronica ordinaria

La ricezione dei documenti informatici è assicurata tramite caselle di posta elettronica ordinaria. All'interno dell'AOO alcune caselle sono state associate al Registro di protocollo garantendo così l'acquisizione automatica dei documenti. Quando i documenti informatici pervengono alle caselle di posta elettronica gli operatori preposti alla gestione delle caselle procedono alla registrazione di protocollo ed alla assegnazione agli uffici di competenza previa verifica della rispondenza dei documenti trasmessi ai requisiti deliberati dall'Ente e contenuti nelle linee guida in materia di dematerializzazione dei documenti, in merito ai formati ammessi, alla dimensione dei files, alla presenza di eventuali link, codici eseguibili, macro istruzioni. La fase di ricezione dei documenti comprende anche i processi di verifica delle firme digitali apposte sui documenti stessi.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente descritte.

Successivamente alla protocollazione il messaggio viene smistato al servizio competente tramite il sistema di gestione documentale.

Il personale assegnato alla gestione delle caselle di posta elettronica ordinaria controlla quotidianamente i messaggi pervenuti nella casella di posta medesima e verifica se sono da protocollare.

5.1.3.2 Ricezione tramite posta elettronica certificata

La ricezione dei documenti informatici è assicurata tramite caselle di posta elettronica certificata. All'interno dell'AOO è stata individuata la casella di posta elettronica certificata istituzionale gestita dall'ufficio Protocollo. Sono inoltre state individuate caselle di posta elettronica certificata settoriali. Le caselle sono associate al Registro di protocollo garantendo così l'acquisizione automatica dei documenti. Quando i documenti informatici pervengono alle caselle di posta elettronica certificata gli operatori preposti alla gestione delle caselle procedono alla registrazione di protocollo ed alla assegnazione uffici di competenza previa verifica della rispondenza dei documenti trasmessi ai requisiti deliberati dall'Ente e contenuti nelle linee guida in materia di dematerializzazione dei documenti e utilizzo della posta elettronica certificata in merito ai formati ammessi, alla dimensione dei files, alla presenza di eventuali link, codici eseguibili, macro istruzioni. La fase di ricezione dei documenti comprende anche i processi di verifica delle firme digitali apposte sui documenti stessi.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente descritte.

Successivamente alla protocollazione il messaggio viene smistato al servizio competente tramite il sistema di gestione documentale.

Il personale assegnato alla gestione delle caselle di posta elettronica certificata controlla quotidianamente i messaggi pervenuti nella casella di posta medesima e si occupa di tenere costantemente spazio a disposizione per la ricezione dei messaggi all'interno della stessa.

5.1.3.3 Errata ricezione di documenti digitali

Nel caso in cui pervengano sulle caselle di posta elettronica certificata e ordinaria dell'AOO messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore rispedisce il messaggio al mittente con la dicitura.

"Con la presente si comunica che la documentazione trasmessa non è di competenza di questa Città Metropolitana di Torino (ex Provincia di Torino), Cordiali saluti.

Città Metropolitana di Torino- Ufficio (nome ufficio) – (Nome operatore) (011/telefono operatore)"

Nel caso in cui pervengano sulle caselle di posta elettronica certificate e ordinarie dell'AOO messaggi non conformi ai requisiti di ricevibilità dei documenti elettronici deliberati dall'Ente, l'operatore rispedisce il messaggio al mittente utilizzando una delle seguenti formule:

“Con la presente si comunica che non è possibile acquisire la documentazione trasmessa in quanto non conforme ai requisiti di ricevibilità dei documenti elettronici deliberati con D.G.P. 13183/2011 e pubblicati sul sito istituzionale di questa Amministrazione all'indirizzo <http://www.cittametropolitana.torino.it/cms/urp/posta-elettronica-certificata>”

Si prega pertanto di ritrasmettere TUTTA la documentazione secondo i requisiti richiesti da questa Amministrazione:

- *(se trasmettono file in formati non ammessi) i file devono essere in formato Pdf, jpg, txt, tif, xml (no doc, non xls) MENTRE LA DOCUMENTAZIONE TRASMESSA CONTIENE UN FILE IN FORMATO XXX PERTANTO ESSA NON PUO' ESSERE ACQUISITA. Verranno accettati anche file in formato .zip (no .rar) purché all'interno del .zip siano presenti file nei formati di cui sopra.*
- *(se la firma digitale non è valida) se i file sono firmati digitalmente, la firma digitale dovrà essere valida al momento della ricezione da parte della Città Metropolitana di Torino, mentre il file denominato (nome file) presenta una firma non valida.*

In allegato si trasmette il rapporto di verifica della firma

- *(se trasmettono più documenti diversi con una sola mail) a ciascun messaggio trasmesso alle caselle della Città metropolitana di Torino dovrà essere associato uno e un solo documento principale (domanda, istanza, ecc. ...) eventualmente corredato dai relativi allegati (una domanda + 3 allegati = un solo messaggio PEC). Se un'impresa o un cittadino o una PA intende inviare diversi documenti principali, dovrà inviare tanti messaggi distinti quanti sono i documenti principali.*

Esempio: un cittadino che deve inviare 2 domande di partecipazione a 2 concorsi = 2 messaggi distinti, uno per ogni domanda di concorso. Si prega pertanto di reinviare i documenti con spedizioni separate.

- *(se contengono link) i documenti devono pervenire in formato stabile, completo, leggibile, non modificabile, privo di codici eseguibili, macro istruzioni, link (per esempio, collegamenti a siti Internet o posta elettronica). Saranno accettati preferibilmente file in formato PDF ed eventualmente anche JPG, TXT, TIFF, XML. Verranno invece rifiutati i documenti trasmessi in*

formati diversi (DOC, XLS, PPT, ZIP, DWG, ODT, ecc. ...), mentre la documentazione trasmessa contiene un link pertanto essa non può essere acquisita.

Grazie per la collaborazione.

Cordiali saluti.

Città Metropolitana di Torino- Ufficio (nome ufficio) – (Nome operatore) (011/telefono operatore)”

5.1.3.4 Rilascio di ricevute attestanti la ricezione di documenti informatici

La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata.

La ricezione di documenti sulla posta elettronica certificata comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, l'altra al servizio di protocollazione informatica.

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Nel caso di comunicazione tra AOO di documenti amministrativi protocollati, il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- *messaggio di conferma di protocollazione:* un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso del messaggio di protocollo ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento e quindi l'effettiva presa in carico da parte dell'AOO destinataria;
- *messaggio di anomalia:* un messaggio che notifica la rilevazione di una anomalia in un messaggio di protocollo ricevuto; le anomalie sono identificate dai seguenti codici 000_irricevibile, 001_ValidazioneFirma, 002_AnomaliaImpronta;
- *messaggio di annullamento di protocollazione:* un messaggio che contiene una comunicazione di annullamento di un protocollo sia da parte della AOO mittente qualora

annulli il messaggio di protocollo precedentemente inviato, sia da parte della AOO destinataria qualora annulli il messaggio di protocollo precedentemente ricevuto.

5.1.3.5 Ricezione tramite sportello telematico

I documenti informatici possono essere acquisiti mediante piattaforme telematiche con modalità operative diverse:

- gli uffici della Città Metropolitana accedono a sportelli telematici dove i documenti sono a disposizione. Essi sono soggetti a registrazione obbligatoria di protocollo.
- Gli utenti esterni autenticandosi sulla piattaforma telematica preposta alla gestione del procedimento amministrativo di proprio interesse inseriscono i documenti informatici che vogliono trasmettere alla Città Metropolitana, qualora invece non dovessero essere inseriti documenti informatici, la piattaforma memorizza su documento informatico le informazioni risultanti dalla presentazione telematica dei dati. Essi vengono protocollati e archiviati nel sistema di gestione documentale tramite integrazioni fra applicativi o altri automatismi (ad esempio Robotic Process Automation).

5.1.3.6 Ricezione tramite sistemi di cooperazione applicativa

In seguito a integrazione tra sistemi informativi il documento viene automaticamente acquisito, protocollato e archiviato nel sistema di gestione documentale.

5.1.3.7 Ricezione tramite modulistica on line

La Città Metropolitana mette a disposizione sul proprio sito istituzionale il modulo da compilare. L'accesso alla compilazione può essere libero o subordinato al riconoscimento tramite sistemi di identità digitale. In seguito alla compilazione da parte degli utenti viene prodotto un file in formato .pdf. Al modulo stesso possono a loro volta essere allegati file rispondenti ai requisiti deliberati dall'Ente e contenuti nelle linee guida in materia di dematerializzazione dei documenti e utilizzo della posta elettronica certificata relativamente ai formati ammessi e alla loro dimensione. I documenti così formati vengono protocollati e fascicolati tramite integrazione applicativa oppure vengono indirizzati verso una casella di posta ordinaria agganciata al registro di protocollo e protocollati in modalità semi automatica infine classificati nel fascicolo di riferimento

La Città Metropolitana valuta di volta in volta quale delle due metodologie di protocollazione e fascicolazione attivare a seconda della quantità di modulistica attesa.

5.1.3.8 Ricezione su supporti rimovibili

Nei casi in cui con un documento cartaceo sono trasmessi allegati su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di *file* digitali, la Città Metropolitana si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a 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 adempimenti del caso.

L'acquisizione degli allegati digitali nel sistema di gestione documentale può avvenire attualmente solo se la grandezza totale di ogni allegato non supera il limite di 100 Megabyte.

I files degli allegati digitali che rispettano le regole di ricevibilità dei documenti informatici deliberati dall'Ente devono essere associati alla registrazione di protocollo.

5.1.3.9 Assegnazione, presa in carico dei documenti e classificazione

Gli addetti alla protocollazione provvedono ad inviare il documento alla Direzione di destinazione tramite la funzionalità di smistamento del protocollo informatico.

La Direzione che riceve il documento:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, rifiuta lo smistamento;
- in caso di verifica positiva, esegue l'operazione di presa in carico eventualmente inoltrando il documento ai nodi individuati al suo interno;
- esegue la classificazione definitiva del documento sulla base del Titolario di classificazione in essere presso l'AOO, inserendo il documento nella struttura aggregativa relativa al procedimento o affare o materia cui esso si riferisce.

5.2 Flusso dei documenti in uscita dalla AOO

Per "documenti in uscita" s'intendono quelli prodotti dagli uffici della Città Metropolitana nell'esercizio delle proprie funzioni aventi rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione o a soggetti privati, sia persone giuridiche che persone fisiche.

I documenti sono prodotti in formato digitale. È prevista la copia conforme cartacea degli originali informatici firmati e protocollati solo nel caso in cui il destinatario non sia nelle condizioni di ricevere e visualizzare i documenti informatici.

5.2.1 Registrazione di protocollo e segnatrice

Le operazioni di registrazione e di associazione della segnatrice del documento in uscita sono effettuate presso il Servizio produttore del documento oppure avvengono tramite automatismi in caso di integrazione fra applicativi produttori dei documenti e il sistema di gestione documentale.

La compilazione di moduli, se prevista (ad esempio: per spedizioni per raccomandata con avviso di ricevimento) è a cura dell'ufficio produttore del documento.

5.2.2 Trasmissione di documenti informatici

Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dal DPR 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di garantire la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

La spedizione di documenti informatici è consentita anche attraverso le caselle di Posta Elettronica ordinaria.

La trasmissione di documenti informatici avviene anche tramite portali (fattura elettronica) e messa a disposizione su piattaforme telematiche.

5.2.3 Trasmissione di documenti cartacei a mezzo posta

In via residuale possono essere spediti documenti cartacei a soggetti che non dispongono di strumenti telematici per la ricezione dei documenti informatici. Ai soggetti pubblici e privati residenti all'estero ove non esistono caselle di posta elettronica certificata, vengono trasmessi tramite

raccomandata con avviso di ricevimento i documenti che necessitano di una ricevuta di consegna. La corrispondenza cartacea in partenza viene consegnata all'ufficio spedizioni che provvede alla consegna della medesima all'ufficio postale.

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dal servizio postale.

5.2.4 Conservazione delle ricevute di trasmissione

La minuta del documento cartaceo spedito e le ricevute delle raccomandate sono conservate all'interno del relativo fascicolo. Le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali sono associate sia alla registrazione di protocollo che al documento archiviato nella struttura aggregativa di riferimento.

Alcuni documenti digitali vengono spediti dalle caselle di posta elettronica certificata al di fuori del sistema di gestione documentale che consente l'associazione delle ricevute al registro di protocollo.

Si tratta in genere di inviti a procedure negoziate, di documenti che i destinatari chiedono di ricevere in formati non ammessi dal sistema di gestione documentale dell'AOO, di documenti che per l'elevato contenuto e dimensione degli allegati richiedono più spedizioni, di documenti che vengono inviati a un elevato numero di destinatari.

In caso di inviti a procedure negoziate, i documenti informatici vengono associati alla registrazione di protocollo.

In caso di spedizione di documenti in formati non ammessi dal sistema di gestione documentale, la lettera di trasmissione viene associata alla registrazione di protocollo, gli allegati vengono dettagliati nelle annotazioni della registrazione.

In caso di documenti spediti a un elevato numero di destinatari (es: tutti i Comuni, ...) i documenti informatici vengono associati alla registrazione di protocollo.

In caso di spedizione di documenti che per l'elevato numero e dimensione degli allegati richiedono più spedizioni sono comunque associati alla registrazione di protocollo tutti i documenti informatici che vengono spediti al di fuori del sistema di gestione documentale.

La mail di spedizione e le ricevute dei documenti informatici che vengono spediti al di fuori del sistema di gestione documentale vengono conservate dall'ufficio gestore della casella PEC da cui è partita la spedizione in apposite cartelle di rete.

In tutti questi casi nella registrazione di protocollo deve essere inserita la seguente annotazione formale: "I documenti vengono spediti manualmente dalla casella di posta elettronica certificata".

6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

La presente sezione contiene le regole di assegnazione adottate per i documenti in ingresso.

L'assegnazione dei documenti avviene sulla base dell'organigramma dell'AOO riportato all'interno del sistema di gestione documentale. Esso è suddiviso in Strutture (corrispondenti ai Dipartimenti e alle Direzioni dell'Ente) e Nodi. Per ogni Struttura è presente un Nodo Responsabile e possono essere presenti uno o più Nodi Operativi in base alle scelte effettuate dal responsabile di ogni Struttura che può decidere di individuare all'interno della Struttura stessa uno o più uffici.

L'assegnazione dei documenti digitali avviene sempre utilizzando la funzionalità di smistamento presente all'interno del sistema di gestione documentale. Lo smistamento è destinato al/ai Nodo/i.

L'assegnazione dei documenti cartacei avviene sulla base della Struttura destinataria del documento e ad essa consegnata tramite gli uscieri.

L'attività di assegnazione effettuata dall'operatore di protocollo consiste nell'operazione di inviare direttamente al Nodo competente il documento protocollato e nella contestuale trasmissione del materiale documentario oggetto di trattazione.

Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel Dirigente della Struttura e del/dei relativo/i Nodo/i competente per la trattazione dell'affare di cui tratta il documento.

Il Nodo ricevente verifica la competenza e, se esatta, provvede alla presa in carico del documento che gli è stato assegnato entro 10 giorni dalla ricezione dello smistamento.

L'assegnazione è fatta per competenza; l'assegnazione per conoscenza avviene esclusivamente per dare notizia del contenuto di un documento, essa non implica alcuna responsabilità nella gestione del procedimento cui il documento stesso si riferisce.

Il Nodo competente che prende in carico il documento è incaricato della gestione del procedimento cui il documento si riferisce. I termini per la definizione del procedimento amministrativo che si avvia con l'assegnazione del documento decorrono comunque dalla data di protocollazione.

Il Sistema di gestione documentale memorizza tutti i passaggi del documento fra i Nodi organizzativi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

6.1 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati al Nodo competente direttamente attraverso la funzionalità di smistamento presente all'interno del sistema di gestione documentale al termine delle operazioni di registrazione e segnatura di protocollo. Le Direzioni dell'Ente devono quotidianamente aprire la funzionalità di Gestione Smistamento del sistema di gestione documentale per prendere visione dei documenti loro smistati. Il Nodo competente è in grado di visualizzare i documenti attraverso le funzionalità del sistema di gestione documentale e, in base alle abilitazioni possedute, potrà:

- visualizzare i metadati del documento (es: numero di protocollo, data protocollo, oggetto, mittente, numero di protocollo del mittente);
- visualizzare la registrazione di protocollo;
- visualizzare il contenuto del documento;
- individuare come assegnatario l'ufficio all'interno della propria Direzione competente per la materia a cui si riferisce il documento ed assegnare il documento in questione.

La "presa in carico" o il "rifiuto" dei documenti informatici viene registrata dal sistema di gestione documentale.

I destinatari del documento per "competenza" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale.

6.2 Assegnazione dei documenti ricevuti in formato cartaceo

Al termine delle operazioni di registrazione e segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono consegnati alla Direzione competente tramite il servizio di posta interna svolto dagli uscieri.

I documenti cartacei gestiti dagli operatori di protocollo sono di norma protocollati entro il giorno successivo a quello di ricezione, salvo che vi figurino, entro detto lasso di tempo, uno o più giorni non lavorativi. In quest'ultimo caso, l'operazione di protocollazione viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

La Direzione competente è in grado di visualizzare i documenti attraverso le funzionalità del sistema di gestione documentale e, in base alle abilitazioni possedute, potrà:

- visualizzare la registrazione di protocollo;
- prendere atto che il documento perverrà in formato cartaceo;
- associare alla registrazione di protocollo la scansione del documento cartaceo;
- individuare eventualmente come assegnatario l'ufficio all'interno della propria Direzione competente per la materia a cui si riferisce il documento ed assegnare il documento in questione.

I documenti cartacei trasmessi tramite posta raccomandata vengono protocollati e consegnati alla Direzione competente con foglio di accompagnamento che la Direzione ricevente dovrà firmare e datare per ricevuta.

6.3 Modifica delle assegnazioni

Nel caso di assegnazione errata, il Nodo che riceve il documento rifiuta lo smistamento, eventualmente comunicando al mittente dello smistamento stesso il Nodo competente corretto. Il mittente dello smistamento procederà ad una nuova assegnazione.

Il sistema di gestione informatica dei documenti tiene traccia di tutti i passaggi memorizzando l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.

Nel caso di assegnazione errata di documenti cartacei, essi vengono restituiti all'ufficio Protocollo che provvede a riassegnarli alla Direzione corretta.

7. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Sono esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del DPR 28 dicembre 2000, n. 445

- le gazzette ufficiali;
- i bollettini ufficiali;
- i notiziari della Pubblica Amministrazione;
- le note di ricezione delle circolari e altre disposizioni;
- i materiali statistici;
- gli atti preparatori interni;
- i giornali, le riviste, i libri;
- i materiali pubblicitari;
- gli inviti a manifestazioni;
- tutti i documenti già soggetti a registrazione particolare dell'Amministrazione.

A titolo di esempio, gli atti amministrativi, i contratti, le convenzioni, i documenti contabili come le fatture attive, i contratti di assunzione.

La registrazione particolare consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione documentale avuto riguardo, nello specifico, all'assegnazione, alla classificazione, alla fascicolazione.

8. SERVIZIO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

Il Servizio Archivistico è il servizio responsabile delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO.

8.1 Servizio Archivistico

Il Servizio Archivistico è competente a gestire l'intera documentazione archivistica - ovunque trattata, distribuita o conservata - ai fini della sua corretta collocazione, classificazione e conservazione.

Al Servizio Archivistico è preposto il Responsabile della Gestione Documentale in possesso di idonei requisiti professionali tecnico archivistici ed è individuato dall'ente ai sensi dell'art. 44 comma 1bis del D.Lgs. n.82/07.03.2005 - Codice dell'amministrazione digitale (CAD) e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici.

9.SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E CONSERVAZIONE DEI DOCUMENTI

9.1 Protezione e conservazione degli archivi pubblici

9.1.1 Caratteristiche generali

La presente sezione illustra il sistema di classificazione dei documenti, di formazione del fascicolo e di tenuta dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti sostitutivi e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del Piano di classificazione (Titolario). Il Titolario è definito come un "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti". Il Titolario è predisposto, verificato e confermato antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta dello strumento che consente la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione.

Il Titolario è adottato dall'amministrazione con atto formale.

9.1.2 Misure di protezione e conservazione degli archivi pubblici

Gli artt. 822 e 824 del Codice Civile stabiliscono che gli archivi e i documenti degli enti pubblici sono soggetti al regime del **demanio pubblico** e pertanto sono inalienabili; inoltre, il "Codice dei beni culturali" (d.lgs. n. 42/2004) stabilisce che tutti i documenti e archivi degli enti pubblici appartengono al **Patrimonio culturale** nazionale (artt. 2 e 10). Secondo tali norme, gli archivi e i documenti pubblici sono sempre da **culturali**, indipendentemente dalla loro età, tipologia o contenuto; dunque, tutti i documenti prodotti, ricevuti o conservati a qualsiasi titolo da una Pubblica Amministrazione possiedono fin dall'origine la duplice natura di *atti pubblici* e di *beni culturali*.

L'archivio non può essere smembrato e deve essere conservato nella sua organicità. L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della Soprintendenza Archivistica e Bibliografica per il Piemonte e la Valle d'Aosta.

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta Soprintendenza Archivistica e Bibliografica.

Lo scarto dei documenti conservati nell'archivio dell'AOO è subordinato all'autorizzazione della Soprintendenza Archivistica e Bibliografica per il Piemonte e la Valle d'Aosta. Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

9.1.3 Conservazione dei documenti digitali

La scelta sul modello di conservazione in Città Metropolitana è in fase di revisione.

Le modalità di conservazione saranno indicate all'interno del Manuale di conservazione.

9.2 Titolario o Piano di classificazione

9.2.1 Titolario

Il Titolario di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'ente.

Il Piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi o, più in generale, in voci di I livello, II livello, III livello.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo.

Titoli, classi, sottoclassi non sono modificabili né nel numero né nell'oggetto, se non con atto formale.

Il Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali.

La revisione, anche parziale, del Titolario viene proposta dal Responsabile della Gestione Documentale.

Dopo ogni modifica del Titolario, il Responsabile della Gestione Documentale provvede ad informare tutti i soggetti abilitati all'operazione di protocollazione e/o classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

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

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

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

9.2.2 Classificazione dei documenti

La classificazione è l'operazione finalizzata all'organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.

Essa è eseguita in base al Titolario di classificazione.

Tutti i documenti ricevuti e prodotti dai servizi e dagli uffici dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati secondo le voci del Titolario vigente.

Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse), il numero del fascicolo e, eventualmente, del sottofascicolo.

Le operazioni di classificazione sono svolte interamente dai servizi e uffici destinatari/istruttori di documenti.

9.3 Strutture aggregative dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o inseriti in archivio indipendentemente dal supporto sul quale sono formati, sono riuniti in strutture aggregative.

Ogni documento classificato viene inserito nella struttura aggregativa di riferimento.

Le strutture aggregative dei documenti sono:

- **il fascicolo:** è l'unità di base indivisibile di un archivio; raggruppamento organico di documenti relativo a uno stesso oggetto (procedimento, affare, attività). Il fascicolo può essere articolato in sottofascicoli;
- **il dossier:** è un insieme di fascicoli e/o di documenti che afferiscono ad un unico soggetto (persona fisica, persona giuridica, comune, ...);
- **la serie:** è un raggruppamento omogeneo di documenti, fascicoli o dossier;
- **volume:** è la suddivisione di strutture aggregative realizzata per ragioni di ergonomia. Il volume viene creato per risolvere problematiche di gestione di strutture aggregative particolarmente voluminose o per suddividere temporalmente delle strutture aggregative che rimangono aperte per lunghi intervalli temporali.

Documenti, fascicoli e dossier possono essere raccolti in serie, avremo quindi:

- la serie tipologica di documenti;
- la serie di fascicoli;
- la serie di dossier.

I singoli documenti sono inseriti in:

- fascicoli;
- sottofascicoli;
- dossier;
- serie tipologiche di documenti;
- volumi.

Le serie di fascicoli e le serie di dossier non contengono direttamente documenti ma sono formate rispettivamente ed esclusivamente da strutture aggregative quali i fascicoli (eventualmente raccolti in volumi) e i dossier.

Ogni struttura aggregativa dei documenti è corredata da un set di metadati necessario per ottemperare ai principi di interoperabilità, trasparenza e conoscenza approfondita del contesto documentale.

Metadati della Serie Tipologica di Documenti:

- Tipologia serie;
- Codice Identificativo;
- Descrizione;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;
- Tipologia di dati contenuti;
- Modalità di calcolo progressivo documenti;
- Responsabile Materia (AOO-Struttura-Nodo);
- Responsabile conservazione (AOO-Struttura-Nodo);
- Responsabile creazione (AOO-Struttura-Nodo);
- Indice di classificazione esteso;
- Data creazione;
- Data attivazione;
- Data ultima modifica;
- Data chiusura.

Metadati della Serie di Fascicoli:

- Tipologia serie;
- Codice Identificativo;
- Descrizione;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;
- Tipologia di dati contenuti;
- Tipologia numerazione fascicoli contenuti nella serie;
- Responsabile Materia (AOO-Struttura-Nodo);
- Responsabile conservazione (AOO-Struttura-Nodo);
- Responsabile creazione (AOO-Struttura-Nodo);
- Indice di classificazione esteso;
- Data creazione;
- Data attivazione;

- Data ultima modifica;
- Data chiusura.

Metadati della Serie di Dossier:

- Tipologia serie;
- Codice Identificativo;
- Descrizione;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;
- Tipologia di dati contenuti;
- Responsabile Materia (AOO-Struttura-Nodo);
- Responsabile conservazione (AOO-Struttura-Nodo);
- Responsabile creazione (AOO-Struttura-Nodo);
- Indice di classificazione esteso;
- Data creazione;
- Data attivazione;
- Data ultima modifica;
- Data chiusura;

Metadati del fascicolo:

- Tipologia numerazione;
- Numero,
- Oggetto;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;
- Tipologia dati contenuti;
- Grado di vitalità;
- Responsabile Materia (AOO-Struttura-Nodo);
- Responsabile conservazione (AOO-Struttura-Nodo);
- Responsabile creazione (AOO-Struttura-Nodo);
- Indice di classificazione esteso;
- Data apertura;

- Data chiusura;
- Data ultima modifica.

Metadati del sottofascicolo:

- Numero del fascicolo padre;
- Numero del sottofascicolo;
- Descrizione;
- Conservazione in archivio generale;
- Tipologia dati contenuti;
- Indice di classificazione esteso;
- Data creazione;
- Data ultima modifica.

Metadati del dossier:

- Numero;
- Descrizione;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;
- Tipologia dati contenuti;
- Responsabile Materia (AOO-Struttura-Nodo);
- Responsabile conservazione (AOO-Struttura-Nodo);
- Responsabile creazione (AOO-Struttura-Nodo);
- Indice di classificazione esteso;
- Data attivazione;
- Data chiusura;
- Data ultima modifica;

Metadati del volume:

- Codice;
- Descrizione;
- Conservazione in archivio corrente;
- Conservazione in archivio generale;

- Indice di classificazione esteso;
- Data apertura;
- Data chiusura;
- Data ultima modifica.

9.3.1 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, a un nuovo affare o a una nuova attività, la Direzione responsabile del procedimento/affare/attività provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione;
- numero del fascicolo;
- oggetto del fascicolo;
- data di apertura del fascicolo;
- AOO, Struttura e Nodo responsabile della materia;
- livello di riservatezza, se diverso da quello standard applicato dal sistema;
- eventuali annotazioni (formali o informali).

9.3.2 Modifica dell'assegnazione dei fascicoli

Nell'eventualità si verifichi una variazione nelle competenze e attività delle Strutture e dei relativi nodi operativi (es. riorganizzazioni) e sia necessario modificare l'assegnazione di un fascicolo, il Servizio Archivistico provvede a variare la responsabilità del fascicolo. Il sistema documentale tiene traccia di questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'operatore/operatrice che effettua la modifica, la data e l'ora dell'operazione, storicizzando i diversi passaggi di responsabilità.

9.3.3 Apertura del dossier

La formazione di un nuovo dossier avviene attraverso l'operazione di "apertura", che prevede l'inserimento delle seguenti informazioni essenziali:

- indice di classificazione;
- il numero del dossier;
- la descrizione o l'oggetto del dossier;
- la data di attivazione;
- AOO, Struttura e Nodo responsabile della materia;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

9.3.4 Chiusura delle strutture archivistiche

La chiusura delle strutture archivistiche è effettuata alla fine della relativa attività e il sistema congela la data dell'azione di chiusura.

Nell'eventualità si verificasse l'esigenza di inserire ulteriori documenti le strutture archivistiche possono essere riaperte e nell'azione di chiusura il sistema storicizza la data.

9.4 Consultazione e movimentazione dell'archivio corrente e di deposito

9.4.1 Principi generali

La richiesta di consultazione, e di conseguenza la movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione, oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

9.4.2 Consultazione ai fini giuridico-amministrativi

La consultazione a fini giuridico amministrativi è disciplinata dal Regolamento in materia di accesso generalizzato, civico e documentale approvato dall'Ente.

La domanda di accesso può essere presentata alla Direzione responsabile del procedimento, all'Ufficio Relazioni con il Pubblico o al Servizio Archivistico nel caso di documenti liberamente consultabili ai sensi dell'art. 122 del D.Lgs. 42/2004.

9.4.3 Consultazione per scopi storici

La consultazione a scopi storici è disciplinata dal Regolamento in materia di accesso generalizzato, civico e documentale approvato dall'Ente. e dal Regolamento di Protocollazione e Archiviazione dei documenti approvati dall'Ente.

La consultazione a scopi storici è quella che persegue finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato.

La domanda di consultazione può essere presentata all'Ufficio Relazioni con il Pubblico, al Servizio Archivistico o direttamente alle singole Direzioni dell'Ente in cui siano conservati i documenti.

Il responsabile del Servizio Archivistico dell'Ente provvede al servizio di accesso, sentito il Dirigente competente, per i documenti non liberamente consultabili, ai sensi dell'art. 122, comma 2, del D. Lgs. 42/2004.

L'ingresso ai depositi dell'archivio è consentito solo agli addetti del Servizio Archivistico. La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti conservati in archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.

9.4.4 Consultazione da parte di personale interno all'amministrazione

Le Direzioni dell'AOO, per motivi di consultazione, possono richiedere in ogni momento al Servizio Archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica. La richiesta avviene tramite e-mail all'indirizzo preposto.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico, ad un ufficio dell'Ente, avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Una stampa della richiesta di consultazione pervenuta via e-mail viene conservata nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile del Servizio Archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di

consegna e quella di restituzione, nonché eventuali note sullo stato della documentazione, in modo da riceverla nello stesso stato in cui è stata consegnata.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine degli stessi rispettandone la sedimentazione archivistica e il vincolo.

In ogni caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

9.4.5 Gestione e organizzazione dei documenti e dei fascicoli nell'archivio corrente

Ciascuna Direzione è tenuta alla organizzazione e gestione dei fascicoli informatici di propria competenza (corretta classificazione, apertura e chiusura di fascicoli e dossier, corretta archiviazione dei documenti al loro interno), secondo i criteri indicati nell'*Allegato 2 – Titolario di classificazione*. Ogni Direzione deve gestire il proprio archivio corrente per la conservazione della documentazione riguardante i procedimenti/affari/attività in corso. I fascicoli cartacei dell'archivio corrente sono conservati a cura dei responsabili dei procedimenti amministrativi negli uffici di competenza.

9.4.6 Archivio di deposito

L'archivio di deposito è l'archivio nel quale vengono conservati i fascicoli chiusi relativi a procedimenti definiti.

Le singole Direzioni collaborano con il Responsabile del Servizio Archivistico nella selezione dello scarto, nel versamento all'archivio di deposito e nella redazione dei relativi elenchi.

10. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

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

10.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. Il numero di protocollo individua un documento principale e i suoi eventuali allegati. 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.

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 a favore o a danno delle parti.

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

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione aventi rilevanza giuridico-probatoria ² e tutti i documenti informatici, fanno eccezione i documenti elencati all'art. 53 del Testo Unico n. 445/2000.

² cfr. Regolamento di Protocollazione e Archiviazione dei documenti approvato con DCP 340512/2003.

Sono parimenti soggetti alla registrazione di protocollo gli atti interni che si inseriscono nel procedimento amministrativo e sono tra loro coordinati e preordinati all'adozione del provvedimento quale atto finale del procedimento. Rientrano in tale categoria gli atti preparatori, quali i pareri, gli accordi preliminari, le designazioni, gli esiti di istruttorie tecniche o amministrative ³.

10.2 Registro giornaliero di protocollo

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso viene prodotto automaticamente dal sistema di protocollo informatico in formato .XML con annesso foglio di stile e reso disponibile in formato .PDF. Al fine di garantire la non modificabilità delle operazioni di registrazione, il Registro giornaliero di protocollo è archiviato nel sistema di gestione documentale. Tale operazione viene espletata automaticamente dal sistema di protocollo informatico.

10.3 Registrazione di protocollo

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

Per 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;

³ cfr. Regolamento di Protocollazione e Archiviazione dei documenti approvato con DCP 340512/2003.

- il mittente che ha spedito il documento registrato in forma non modificabile;
- il destinatario del documento registrato in forma non modificabile;
- l'oggetto del documento registrato in forma non modificabile;
- l'indice di classificazione riferito all'indicazione delle sole voci di Titolare.

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

10.3.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi, in modo formale, sulle/dalle caselle di posta elettronica certificata dell'AOO e dalle caselle di posta elettronica ordinaria. La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i *file* allegati al messaggio di posta elettronica ricevuto, o inviato. La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio che ad uno dei *file* ad esso allegati che può assumere la veste di documento principale. Tali documenti sono memorizzati nel sistema, in modo non modificabile.

I documenti informatici ricevuti e trasmessi tramite portali vengono protocollati generalmente in modalità automatica, qualora venissero protocollati in modalità manuale l'operatore provvederà ad agganciare i documenti informatici alla registrazione di protocollo e li memorizzerà nel sistema di gestione documentale in modo non modificabile.

10.3.2 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita la Direzione produttrice del documento esegue la registrazione di protocollo e invia la copia dell'originale informatico sottoscritto digitalmente e protocollato.

10.3.3 Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa è possibile inserire nella registrazione di protocollo alcuni elementi facoltativi.

In caso di necessità, i dati facoltativi sono modificabili senza bisogno di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Per quanto concerne i campi integrativi facoltativi presenti nel sistema di protocollo, sono previste specifiche funzionalità che consentono di gestire:

- Il numero di protocollo del mittente e la data del documento se presenti;
- ulteriori informazioni sul/sulla mittente/destinatario/destinataria, soprattutto se persona giuridica;
- l'indirizzo completo del/della mittente/destinatario/destinataria (via, numero civico, CAP, città, provincia);
- il codice fiscale;
- il numero della partita IVA;
- il recapito telefonico;
- gli indirizzi di posta elettronica;
- il collegamento alla registrazione precedente;
- la data timbro postale;
- il mezzo di trasmissione.

10.4 Segnatura di protocollo dei documenti

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

La segnatura di protocollo è l'apposizione (per i documenti analogici), o l'associazione (per i documenti informatici) all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.

Essa consente di individuare ciascun documento in modo univoco e certo.

10.4.1 Documenti informatici

I dati della segnatura di protocollo di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio, in *un file* conforme alle specifiche *dell'Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) reso disponibile dagli organi competenti.

Le informazioni minime incluse nella segnatura sono le seguenti:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro nell'ambito del quale è stata effettuata la registrazione;
- data di registrazione;
- numero progressivo di protocollo;
- oggetto;
- mittente;
- destinatario/destinatari;
- l'impronta del documento principale e degli allegati, se presenti;
- la classificazione del messaggio di protocollo.

La struttura ed i contenuti del *file* di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

L'AOO che riceve il messaggio di protocollo può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo dei documenti ricevuti.

10.4.2 Documenti cartacei ricevuti

La segnatura di protocollo di un documento cartaceo ricevuto è apposta manualmente sul documento principale.

Essa riporta le seguenti informazioni relative alla registrazione:

- codice identificativo della Direzione protocollante;
- data e numero di protocollo del documento.

10.5 Annullamento delle registrazioni di protocollo

Solo il Responsabile del Servizio Archivistico è autorizzato ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo deve essere richiesto con specifica mail, adeguatamente motivata, indirizzata al Responsabile del Servizio Archivistico.

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, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal Responsabile del Servizio Archivistico. In tale ipotesi, la procedura riporta la dicitura "annullato" in posizione visibile e tale da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuto annullamento, la data ed il soggetto che è intervenuto.

10.6 Livelli di visibilità sulle registrazioni di protocollo

I livelli di visibilità delle registrazioni di protocollo sono gestiti da appositi profili che assegnati ad utenti individuati permettono di etichettare le registrazioni di protocollo come riservate qualora ad esse siano associati documenti riservati.

Non devono comunque essere inserite informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo

10.6.1 Livello di riservatezza dei documenti associati alle registrazioni di protocollo

Il sistema di protocollo garantisce un livello di riservatezza di base prevedendo la visibilità dei documenti in base ai profili assegnati agli/alle utenti. Per i documenti che richiedono una maggiore

riservatezza la procedura dispone delle funzioni di riservato/sensibile da poter selezionare in base alla tipologia di dato da tutelare.

In modo analogo, il/la Responsabile del procedimento amministrativo che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.

Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti invece che hanno un livello di riservatezza superiore lo mantengono.

10.7 Documenti non firmati

L'operatore di protocollo attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, con la dicitura "mittente sconosciuto o anonimo".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali. È poi compito del Servizio di competenza e, in particolare, del Responsabile del procedimento valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

10.8 Protocollazione dei messaggi di posta elettronica ordinaria

Considerato che l'attuale sistema di posta elettronica ordinaria non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata come segue:

- caso di invio, come allegato, di un documento scansionato munito di firma autografa: fermo restando che il Responsabile del procedimento deve verificare la provenienza certa dal documento, in caso di mittente non verificabile, il Responsabile del procedimento valuta, caso per caso, l'opportunità di protocollare il documento inviato via *e-mail*;
- caso di invio, in allegato, di un documento munito di firma digitale: il documento è un documento informatico riconducibile con certezza al suo autore e va protocollato;

- caso di invio di una *e-mail* contenente un testo non sottoscritto: il Responsabile del procedimento valuta l'opportunità di protocollare il documento dopo averne verificato la provenienza.

10.9 Protocollo di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'AOO, l'addetto al protocollo annulla lo smistamento, inserisce un'annotazione formale dove segnala la non competenza dell'AOO, risponde al messaggio pec/mail del mittente con la seguente comunicazione:

*“Con la presente si comunica che la documentazione trasmessa non è di competenza di questa Città Metropolitana di Torino (ex Provincia di Torino), ma di (indicazione dell'ente destinatario).
Cordiali saluti.*

Città Metropolitana di Torino- Ufficio (nome ufficio) – (Nome operatore) (011/telefono operatore)

10.10 Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'AOO, il personale assegnato all'ufficio protocollo provvede a redigere una lettera di restituzione al mittente, a protocollare tale lettera in uscita, indicando nell'oggetto "restituzione documento protocollato per errore".

Il personale dell'ufficio protocollo contestualmente richiama la registrazione di protocollo del documento ricevuto erroneamente e inserisce un'annotazione formale dove segnala la non competenza dell'AOO.

Il documento oggetto della rettifica con la lettera di accompagnamento viene restituito al mittente.

10.11 Documenti ricevuti per conoscenza

I documenti ricevuti per conoscenza sia in formato digitale che in formato cartaceo vanno protocollati e smistati ai servizi competenti.

10.12 Documenti cartacei in entrata con più destinatari

Qualora le Direzioni destinatarie di un documento cartaceo siano in numero maggiore di una, il personale assegnato all'ufficio protocollo provvede a scansionare il documento, ad associarlo alla registrazione di protocollo e a smistarlo tramite il sistema di gestione documentale a ogni Direzione destinataria.

10.13 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti sono, di norma, effettuate nella giornata di arrivo e comunque entro la giornata lavorativa successiva al ricevimento di detti documenti ⁴.

Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo ad esempio per un imprevisto ed eccessivo carico di lavoro si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del Responsabile del Servizio Archivistico, che autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.

Il protocollo differito consiste nel rinvio dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per le motivazioni che il Responsabile del servizio di protocollo descrive nel provvedimento sopra citato.

I documenti destinati alla Città Metropolitana, ma inseriti su piattaforme Nazionali o comunque su piattaforme non gestite direttamente dalla Città Metropolitana stessa, si intendono ricevuti ai fini dell'acquisizione al protocollo dopo il download anche massivo dei medesimi. La registrazione di protocollo può essere effettuata anche diversi giorni dopo l'acquisizione dei medesimi in quanto essa

⁴ cfr. Regolamento di Protocollazione e Archiviazione dei documenti approvato con DCP 340512/2003.

comporta un controllo preventivo dei documenti fisici (file) e la strutturazione di un file per la metadatazione degli stessi.

10.14 Registrazioni di protocollo

10.14.1 Attribuzione del protocollo

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il sistema di protocollo informatico.

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il sistema di protocollo informatico appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente.

Il sistema di protocollo informatico assicura l'esattezza del riferimento temporale (UTC) con l'acquisizione periodica del tempo ufficiale di rete.

10.14.2 Modalità di produzione e archiviazione del registro giornaliero di protocollo informatico

Di seguito sono descritte le modalità di produzione e di archiviazione, entro la giornata lavorativa successiva, del Registro giornaliero di protocollo informatico.

Il sistema di protocollo informatico provvede all'estrazione automatica del registro giornaliero di protocollo consistente in un file in formato .XML al quale viene applicato il relativo foglio di stile che rappresenta graficamente le informazioni contenute nel file .XML. Si visualizza quindi il registro giornaliero in un file in formato .PDF, generato dall'applicazione del foglio di stile sul file .XML.

Il documento così creato riporta su un unico file il riepilogo di tutte le registrazioni di protocollo eseguite nell'ambito della stessa giornata e, a seguire, le registrazioni dei giorni precedenti che sono state annullate o modificate.

I metadati associati al registro di cui sopra sono suddivisi in:

Dati del documento registro:

- Codice identificativo del registro;
- Anno a cui il registro si riferisce;
- Indicazione del numero della prima registrazione effettuata sul registro;
- Indicazione della data della prima registrazione effettuata sul registro;
- Indicazione del numero dell'ultima registrazione effettuata sul registro;
- Indicazione della data dell'ultima registrazione effettuata sul registro.

Dati di identità:

- Il soggetto che ha l'autorità e la competenza a produrre il documento informatico;
- indicazione della denominazione del sistema informatico che ha generato automaticamente il registro.

La produzione del registro giornaliero di protocollo avviene entro le ore 02:00:00 del primo giorno lavorativo successivo al giorno sul quale si considera l'estrazione.

Il registro giornaliero viene archiviato automaticamente nel sistema di gestione documentale nella apposita Voce di Titolario in una serie tipologica di documenti suddivisa in volumi annuali di cui è responsabile il Servizio Archivistico.

11. MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

La presente sezione illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente.

11.1 Il registro di emergenza

Qualora non fosse possibile fruire del sistema di protocollo informatico per una interruzione totale del sistema che potrebbe protrarsi nei giorni l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza.

Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul registro di protocollo generale.

Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio. A tale registrazione sono associati anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale.

La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo. In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo.

Il registro di emergenza è un registro cartaceo in dotazione presso l'ufficio Protocollo Generale.

11.2 Modalità di apertura del registro di emergenza

Il responsabile del servizio di protocollo assicura che, ogni qualvolta si presentino gravissime cause tecniche e non sia possibile utilizzare la procedura informatica per più giorni, le operazioni di protocollo siano svolte sul registro di emergenza cartaceo.

Sul registro di emergenza sono riportate: la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

11.3 Modalità di utilizzo del registro di emergenza

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

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

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono gli stessi previsti dal protocollo generale.

11.4 Modalità di chiusura e di recupero del registro di emergenza

Una volta ripristinata la piena funzionalità del servizio di protocollo informatico, il responsabile del servizio di protocollo provvede alla chiusura del registro di emergenza, annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico di protocollo generale a cura del personale assegnato all'ufficio protocollo generale.

12. REGISTRI PARTICOLARI

12.1 Registri delle fatture attive e dei corrispettivi

I registri delle fatture attive e dei corrispettivi vengono prodotti dal sistema gestionale di Contabilità.

I registri delle fatture attive sono 8, i registri dei corrispettivi sono 2, ogni registro è assegnato alla Direzione preposta all'emissione di fatture attive e di corrispettivi. I registri sono identificati con un codice.

Il numero di repertorio dei documenti (fatture e corrispettivi) in essi registrati è formato dal numero progressivo del documento all'interno del registro e dal codice del registro. La numerazione dei documenti si rinnova ogni anno.

I registri delle fatture attive e dei corrispettivi alla chiusura vengono prodotti in formato .PDF e sono stati predisposti per essere archiviati automaticamente nel sistema di gestione documentale nella apposita Voce di Titolario in una serie tipologica di documenti suddivisa in volumi annuali.

12.2 Registri degli Atti Amministrativi

I registri degli atti amministrativi vengono prodotti dal sistema gestionale di produzione e gestione degli atti stessi.

Viene prodotto un registro per ogni tipologia di atto: Deliberazioni di Consiglio, Decreti, Determinazioni Dirigenziali, Atti di Liquidazione. Per ciascuna tipologia di atto la numerazione si rinnova annualmente.

Le Determinazioni Dirigenziali e gli Atti di Liquidazione prendono una seconda numerazione, con rinnovo annuale, specifica per Direzione proponente.

I registri degli Atti Amministrativi alla chiusura vengono prodotti in formato .PDF e predisposti per essere archiviati automaticamente nel sistema di gestione documentale nella apposita Voce di Titolario in una serie tipologica di documenti suddivisa in volumi annuali.

12.3 Registro dei Documenti pubblicati all'Albo Pretorio

Il registro dei documenti pubblicati sull'Albo Pretorio viene prodotto dal sistema gestionale dell'Albo Pretorio.

La numerazione dei documenti si rinnova ogni anno.

Il registro dei documenti pubblicati sull'Albo Pretorio alla chiusura viene prodotto in formato .PDF e predisposto per essere archiviato automaticamente nel sistema di gestione documentale nella apposita Voce di Titolario in una serie tipologica di documenti suddivisa in volumi annuali.

12.4 Registro dei Contratti

Il registro dei contratti, in qualsiasi forma stipulati (lettera commerciale, scrittura privata, atto pubblico) è prodotto dalla procedura gestionale dei contratti. La numerazione dei documenti si rinnova ogni anno.

Il registro viene prodotto tramite estrazione di un report in formato .XLS. Tale report dovrà essere trasformato in formato .PDF e archiviato nel sistema di gestione documentale.

12.5 Repertorio del Segretario Generale

Il Repertorio del Segretario Generale è un registro cartaceo la cui numerazione segue il numero progressivo attribuito alla data della sua creazione (1° gennaio 2015).

Il registro cartaceo è conservato presso la Direzione che gestisce il Repertorio, la quale lo ha riprodotto anche su un file .XLS, che tiene costantemente aggiornato.

12.6 Registri delle Convenzioni

I registri delle convenzioni sono prodotti su file .XLS la cui gestione è accentrata presso la Direzione preposta a registrare tutte le convenzioni stipulate dalle Direzioni dell'AOO. La numerazione dei documenti si rinnova ogni anno.

Tali registri dovranno essere trasformati in formato .PDF e archiviati nel sistema di gestione documentale.

12.7 Registro dei Contratti di Assunzione

Il registro dei contratti di assunzione è prodotto su file .XLS gestito dalla Direzione Risorse Umane. La numerazione dei documenti si rinnova ogni anno.

Tale registro dovrà essere trasformato in formato .PDF e archiviato nel sistema di gestione documentale.

13. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

13.1 Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di gestione documentale" su proposta del Dirigente responsabile della Direzione cui afferisce il servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza.

13.2 Pubblicità del presente Manuale

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

Copia del presente manuale è:

- fornita a tutto il personale dell'AOO e resa disponibile nella intranet dell'Ente;
- pubblicato sul sito istituzionale dell'amministrazione.

13.3 Operatività del presente manuale

Il presente manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

14 ALLEGATI

14.1 Elenco caselle di posta elettronica certificata

14.2 Titolario di Classificazione

14.3 Elenco dei formati ammessi