COMUNE DI MELISSA

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

(Regolamento adottato ai sensi dell'art. 5 del D.P.C.M. 3/12/2013, Gazzetta Ufficiale n. 59 del 12 marzo 2014)

Adottato con Delibera di Giunta Municipale
n. 118 del 06.10.2015

Sommario

I – PRINCIPI GENERALI

Art. 1: Oggetto

1. Il presente Manuale di Gestione, adottato ai sensi della normativa vigente[1], disciplina le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici, in relazione ai procedimenti amministrativi del Comune di Melissa.

Art. 2: Definizioni

1. Ai fini del presente manuale di gestione si intende per:
a) "AMMINISTRAZIONE", il Comune di Melissa ;
b) "TESTO UNICO", il D.P.R. 20.12.2000, n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
c) "C.A.D.", il D. Lgs. 7.3.2005, n. 82 recante "Codice dell'amministrazione digitale";
d) "REGOLE TECNICHE PI", il D.P.C.M. 3.12.2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del C.A.D.";
d-bis) "REGOLE TECNICHE CONS", D.P.C.M. 3,12,2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"
e) "AOO", l'Area Organizzativa Omogenea;
f) "RPA", il Responsabile del Procedimento Amministrativo;
g) "RSP", il Responsabile per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
h) "UOP", l'Unità Organizzativa di registrazione di Protocollo, cioè l'ufficio che svolge attività di registrazione di protocollo;
i) "UU", l'Ufficio Utente, cioè l'ufficio destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali; in linea di massima ogni UU corrisponde ad un Servizio dell'Amministrazione.
2. Per le altre definizioni si rimanda all'Allegato "**A**" del presente Manuale di gestione.

Art. 3: Area Organizzativa Omogenea (AOO)

1. Per la gestione unica e coordinata dei documenti, l'Amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata Comune di Melissa, come di seguito meglio specificato.

Denominazione dell'AOO: COMUNE DI MELISSA Codice identificativo "AOO1" Nominativo del Resp. del Servizio di Protocollo Informatico, gestione documentale ed archivistica Responsabile Area Amministrativa e Demografica, cui sottende il Servizio Protocollo Bevilacqua Domenico Casella di Posta Elettronica Certificata: protocollo.melissa@asmepec.it

[1] Artt. 5 delle "REGOLE TECNICHE"

Indirizzo della sede principale dell'AOO a cui indirizzare la corrispondenza convenzionale Comune di Melissa – Via Provinciale Sud n. 109 – 88814 Melissa (KR)

Art. 4: Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

1. Ai sensi della normativa vigente[2], l'Amministrazione è dotata del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, individuandolo nella Unità Organizzativa cui afferiscono le funzioni del Protocollo e dell'Archivio.
2. Al Servizio è preposto il Responsabile della predetta Unità Organizzativa.
3. Il Servizio svolge i seguenti compiti:
a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
c) garantisce la produzione e conservazione del registro giornaliero di protocollo;
d) cura, di concerto con il Servizio Informatico, che le funzionalità del sistema, in caso di guasti o anomalie, vengano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
e) cura, di concerto con il Servizio Informatico, la conservazione delle copie di cui alla normativa vigente[3] in luoghi sicuri differenti;
f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;
g) autorizza, con appositi provvedimenti, le operazioni di annullamento delle registrazioni di protocollo;
h) vigila sull'osservanza delle disposizioni del presente Manuale di gestione da parte del personale autorizzato e degli incaricati;
i) cura, ai sensi della normativa vigente[4], il trasferimento dei documenti dagli uffici agli archivi;
j) cura il costante aggiornamento del presente Manuale di gestione e di tutti i suoi allegati.

Art. 5: Conservazione delle copie del registro informatico di protocollo

1. Ai sensi della normativa vigente[5], il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

Art. 6: Firma digitale qualificata. Abilitazione dei dipendenti

1. Per l'espletamento delle attività istituzionali, qualora se ne abbia la necessità, l'Amministrazione fornisce la firma digitale o elettronica qualificata ai dipendenti da essa delegati a rappresentarla.

2 Art. 61, cc. 1 e 2 del "TESTO UNICO"
3 Artt. 62 e 63 del "TESTO UNICO"
4 Artt. 67, 68 e 69 del "TESTO UNICO"
5 Art. 7, comma 5, delle "REGOLE TECNICHE"

Art. 7: Caselle di Posta elettronica

1. L'AOO è dotata della casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA); questa casella costituisce l'indirizzo virtuale dell'AOO e di tutti gli uffici che ad essa fanno riferimento.
2. Le caselle di Posta Elettronica Certificata sono accessibile, per l'invio e la ricezione di documenti, solo dall'Ufficio Protocollo, come specificato al successivo art. 16, mentre per la manutenzione e la gestione tecnica è accessibile al servizio Informatico.
3. Ogni Area è dotata di mail istituzionale certificata, le mail sono riportate nel sito istituzionale sezione "Trasparenza" secondo quanto stabilito dal D.L. 33/2013.

Art. 8: Sistema di classificazione dei documenti

1. A seguito dell'introduzione del protocollo unico di cui al successivo art. 43 e per garantire la corretta classificazione e organizzazione dei documenti nell'archivio, a partire dalla fase corrente, viene adottato il "Titolario di classificazione" di cui al successivo art. 42.

II – PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

Art. 9: Protocolli diversi dal protocollo informatico

1. Tutti i documenti inviati e ricevuti dall'Amministrazione sono registrati all'interno del registro di protocollo informatico.
2. Sono consentite, tuttavia, forme di registrazione particolari per alcune tipologie di documenti come specificato al successivo art. 39.

III – PIANO PER LA SICUREZZA INFORMATICA

Art. 10: Piano per la sicurezza informatica

1. Il Piano per la sicurezza informatica, redatto ai sensi della normativa vigente, è contenuto nel "Documento Programmatico sulla Sicurezza Informatica (DPS)".
2. E' messo in atto ai sensi della normativa vigente[6] il Piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi.

6 Art. 4, lett. c, delle "REGOLE TECNICHE"

Art. 11: Politiche di sicurezza

1. **Politiche accettabili di uso del sistema informativo.** Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.
2. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.
3. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati delle aziende outsourcer includendo tutto il personale affiliato con terze parti. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.
4. Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima. Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito. Le singole aree o settori o Divisioni o Direzioni sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento. Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.
5. Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni. Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni sei mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni. Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia. Non permettere ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le proprie credenziali.

6. **Politiche – antivirus.** I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni. I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia. I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.
Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.
Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.
Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato. Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati. Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura. Non scaricare mai messaggi da siti o sorgenti sospette. Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus. Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste. Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone. Evitare collegamenti diretti ad Internet via modem.
Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura. Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura. Non utilizzare i server di rete come stazioni di lavoro. Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali. Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione. Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno. Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato. È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.
In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.
7. **Politiche per le azioni consuntive**. Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

- verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
- verificare se il virus ha diffuso dati;
- identificare il virus;
- attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
- installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;

- diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

8. **Politiche - uso non accettabile**. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete). In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

- Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.
- Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.
- È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
- Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
- Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.
- Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedopornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
- Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
- Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
- Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
    - accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione, • attività di "sniffing";
    - disturbo della trasmissione;
    - spoofing dei pacchetti;
    - negazione del servizio;
    - le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
    - attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.
- Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

9. **Attività di messaggistica e comunicazione**. Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).

- Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
- Uso non autorizzato delle informazioni della testata delle e-mail,
- Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare
- Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
- Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

IV – MODALITA' DI UTILIZZO DI STRUMENTI INFORMATICI PER LA FORMAZIONE E LO SCAMBIO DI DOCUMENTI

Art. 12: Principi generali

1. Secondo quanto previsto dalla normativa vigente[7], l'Amministrazione forma gli originali dei propri documenti con mezzi informatici.
2. Fermo restando quanto previsto al comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria.
3. Ogni documento per essere inoltrato in modo formale, all'esterno o all'interno dell'Amministrazione:
a) deve trattare un unico argomento indicato in modo sintetico ma esaustivo, a cura dell'autore, nello spazio riservato all'oggetto;
b) deve riferirsi ad un solo protocollo;
c) può fare riferimento a più fascicoli.
4. Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
5. Il documento deve consentire l'identificazione dell'Amministrazione mittente attraverso le seguenti informazioni:
a) la denominazione e il logo dell'Amministrazione;
b) l'indirizzo completo dell'Amministrazione;
c) il codice fiscale dell'Amministrazione;
d) l'indicazione completa dell'ufficio dell'Amministrazione che ha prodotto il documento
corredata dai numeri di telefono e fax.
6. Il documento, inoltre, deve recare almeno le seguenti informazioni:
a) il luogo di redazione del documento;
b) la data (giorno, mese, anno);
c) il numero di protocollo;
d) il numero degli allegati (se presenti);
e) l'oggetto del documento;
f) se trattasi di documento informatico, la firma elettronica qualificata da parte del RPA e/o del responsabile del provvedimento finale;
g) se trattasi di documento cartaceo, la sigla autografa da parte del RPA e/o del responsabile del provvedimento finale.

Art. 13: Documento ricevuto dall'Amministrazione

1. Il documento informatico può essere recapitato all'Amministrazione:

7 Artt 40 e 71 del C.A.D.

a) a mezzo posta elettronica convenzionale o certificata;
b) su supporto rimovibile (cd rom, dvd, floppy disk, chiave usb, etc.) consegnato direttamente all'Amministrazione o inviato per posta convenzionale, posta raccomandata o corriere;
c) tramite servizi di e-government on line.
2. Il documento su supporto cartaceo può essere recapitato:
a) a mezzo posta convenzionale, posta raccomandata o corriere;
b) a mezzo telefax o telegramma;
c) a mezzo consegna diretta all'Amministrazione

Art. 14: Documento inviato dall'Amministrazione

1. I documenti informatici, compresi gli eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta certificata o delle e-mail istituzionali non certificate.
2. In alternativa, il documento informatico può essere riversato su supporto rimovibile non modificabile e trasmesso con altri mezzi di trasporto al destinatario.
3. I documenti su supporto cartaceo sono inviati:
a) a mezzo posta convenzionale, posta raccomandata o corriere;
b) a mezzo telefax o telegramma;
c) a mezzo consegna diretta al destinatario.

Art. 15: Documento interno formale

1. I documenti interni dell'Amministrazione sono formati con tecnologie informatiche.
2. Lo scambio tra gli uffici dell'Amministrazione di documenti informatici di rilevanza amministrativa giuridico-probatoria, quando essi non siano assistiti da procedure informatiche che ne garantiscano altrimenti la tracciabilità , avviene, di norma, per mezzo della procedura di protocollo informatico; il documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato.
3. Ove ciò risultasse necessario il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno dell'Amministrazione; in questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa e successivamente protocollato.

Art. 16: Documento interno informale

1. Per questa tipologia di corrispondenza, la cui conservazione è facoltativa, vale il disposto del precedente articolo 15, ad eccezione dell'obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

V – DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Art. 17: Ricezione di documenti informatici sulla casella di posta istituzionale

1. La casella di Posta Elettronica Certificata (protocollo.melissa@asmepec.it) è accessibile solo all'Ufficio Protocollo, che procede alla registrazione di protocollo previa verifica dell'integrità e leggibilità dei documenti stessi.
2. il Responsabile a cui è affidata la gestione della casella di posta elettronica deve trasmettere al protocollo quanto ricevuto nelle stesse per un'acquisizione formale.

3. Qualora il messaggio di posta elettronica non sia conforme agli standard indicati dalla normativa vigente[8], la valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quella di una missiva non sottoscritta e comunque valutabile dal RPA.
4. Le disposizioni di cui al precedente comma 3 si applicano anche a tutte le caselle di posta elettronica non certificata istituite per i vari Servizi per consentire a tutti i cittadini l'accesso e la comunicazione dall'esterno.
5. Per le caselle di posta elettronica non certificata è a discrezione del Responsabile del Servizio o del dipendente a cui è affidata la gestione della casella di posta elettronica la trasmissione al protocollo per un'acquisizione formale.

Art. 18: Ricezione di documenti informatici su supporti rimovibili

1. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, l'Amministrazione si riserva la facoltà di acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decifrare e interpretare con le tecnologie a sua disposizione; superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.
2. Qualora il documento informatico su supporto rimovibile venga consegnato direttamente all'Amministrazione e sia accompagnato da una lettera di trasmissione, è quest'ultima ad essere protocollata; qualora, invece, manchi la lettera di trasmissione, sarà protocollato previa la compilazione dell'interessato di un documento autografo di presentazione.

Art. 19: Ricezione di documenti cartacei a mezzo posta convenzionale

1. Il personale dell'Ufficio Protocollo provvede a ritirare dagli uffici postali la corrispondenza.
2. Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti, e successivamente aperti per gli ulteriori controlli preliminari alla registrazione; la busta o contenitore si allega al documento per la parte relativa ai timbri postali.
3. La corrispondenza relativa a procedure negoziali aperte o ristrette è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.
4. La corrispondenza recante la dicitura "RISERVATA" o "PERSONALE" viene trattata con le modalità stabilite al successivo articolo 66;
5. La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, viene trattata con le modalità descritte nei successivi artt. 50 e 51.

Art. 20: Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali

1. Il personale preposto all'apertura e alla registrazione della corrispondenza deve essere regolarmente autorizzato al trattamento dei dati personali.
2. Qualora la corrispondenza riservata personale venga recapitata per errore ad un ufficio dell'Amministrazione quest'ultimo, a tutela dei dati personali eventualmente contenuti, non apre le buste o i contenitori e li rinvia, nella stessa giornata, all'Ufficio Protocollo.

Art. 21: Errata ricezione di documenti digitali

1. Nel caso in cui pervengano sulle caselle di posta elettronica certificata messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore di protocollo rispedisce il

8 Art. 16 delle "Regole tecniche"

messaggio al mittente con la dicitura : “MESSAGGIO PERVENUTO PER ERRORE – NON DI COMPETENZA DI QUESTA AOO”.
2. La stesso comportamento si applica alla ricezione delle e-mail istituzionali non pec da parte degli addetti alla loro gestione.

Art. 22: Errata ricezione di documenti cartacei

1. Nel caso in cui pervengano erroneamente al Protocollo dell’Amministrazione documenti indirizzati ad altri soggetti le buste o i contenitori si restituiscono alla posta.
2. Qualora la busta o il contenitore venga aperto per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto la nota: “PERVENUTO PER ERRORE” e si invia al mittente apponendo sulla busta la diciture “PERVENUTO ED APERTO PER ERRORE”.

Art. 23: Rilascio di ricevute attestanti la ricezione di documenti informatici

1. Nel caso di ricezione di documenti informatici mediante la casella di posta elettronica certificata, la notifica al mittente dell’avvenuto recapito del messaggio è assicurata dagli specifici standard del servizio di posta elettronica certificata dell’AOO.
2. Nel caso di ricezione di documenti informatici mediante la casella di posta elettronica non certificata, la notifica al mittente dell'avvenuto recapito del messaggio è a discrezione del dipendente che gestisce la casella di posta .

Art. 24: Rilascio di ricevute attestanti la ricezione di documenti cartacei

1. Gli addetti al protocollo non possono rilasciare ricevute per i documenti che non sono soggetti a protocollazione.
2. Quando il documento cartaceo non soggetto a protocollazione è consegnato direttamente ad una UOP ed è richiesto il rilascio di una ricevuta attestante l’avvenuta consegna, la UOP che lo riceve è autorizzata a fotocopiare gratuitamente la prima pagina del documento e apporvi il timbro dell’Amministrazione con la data e l’ora d’arrivo e la sigla dell’operatore.
3. La semplice apposizione del timbro dell’Amministrazione con la data e l’ora d’arrivo e la sigla dell’operatore sulla copia non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell’UOP in merito alla ricezione e all’assegnazione del documento.
4. Nel caso, invece, si tratti di documenti soggetti a protocollazione, quando il documento cartaceo è consegnato direttamente ad una UOP ed è richiesto il rilascio di una ricevuta attestante l’avvenuta consegna, la UOP che lo riceve deve rilasciare la ricevuta in questione o in alternativa l’UOP è autorizzata a fotocopiare gratuitamente la pagina del documento su cui è stata apposta la segnatura di protocollo.

Art. 25: Archiviazione dei documenti informatici

1. I documenti informatici sono archiviati, secondo le norme vigenti, su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.
2. I documenti ricevuti in via telematica sono resi disponibili agli uffici dell’Amministrazione, attraverso la rete interna, subito dopo l’operazione di smistamento e di assegnazione.

Art. 26: Classificazione e presa in carico dei documenti

1. Gli addetti alla UOP a seguito di una verifica di congruità in base alle proprie competenze, classificano il documento sulla base del titolario.

Art. 27: Verifica formale dei documenti da spedire

1. Tutti i documenti da spedire, siano essi in formato digitale o analogico, sono inoltrati all'Ufficio Protocollo secondo le procedure opportune.
2. In ogni caso i documenti sono sottoposti, a cura degli uffici mittenti, a verifica formale dei loro requisiti essenziali ai fini della spedizione: oggetto sintetico ed esaustivo, corretta indicazione del mittente, corretta indicazione del destinatario e del suo indirizzo fisico o pec, sottoscrizione digitale o autografa, presenza di allegati se dichiarati, etc.
3. Se il documento è completo, esso è protocollato e su di esso viene apposta la segnatura di protocollo; in caso contrario è rispedito all'ufficio mittente con le osservazioni del caso.
4. In nessun caso gli operatori dell'Ufficio Protocollo sono tenuti a prendere cognizione del contenuto dei documenti da spedire e quindi essi non devono operare alcun controllo nel merito dei contenuti dei documenti stessi.

Art. 28: Registrazioni di protocollo e segnatura dei documenti in partenza e interni

1. Le operazioni di registrazione e di apposizione della segnatura del documento in partenza sono effettuate presso l'Ufficio Protocollo.
2. In nessun caso gli operatori di protocollo sono autorizzati a prenotare numeri di protocollo per documenti non ancora resi disponibili.
3. La compilazione dei moduli se prevista (ad esempio: ricevute di ritorno per raccomandate, posta celere, corriere) è a cura dell'ufficio Utente.
4. I documenti cartacei in partenza o interni, dopo le operazioni di registrazione e segnatura di protocollo, prima della spedizione o dell'inoltro all'ufficio competente vengono acquisiti digitalmente, il formato da usare ai fini della conservazione è il pdf/a.
5. L'Ufficio protocollo verifica la leggibilità, la accessibilità e la qualità del file acquisito e verifica che il file sia associato alla rispettiva registrazione di protocollo.
6. Tutti i tipi di documenti in formato A4, comunque separabili o leggibili dal supporto tecnico vengono digitalizzati con lo scanner. In caso di planimetrie o volumi non sperabili si potrà comunque procedere a digitalizzare con lo scanner il frontespizio. La digitalizzazione con lo scanner potrà comunque avvenire anche in un secondo tempo rispetto alle procedure di protocollazione.

Art. 29: Trasmissione di documenti informatici

1. I documenti informatici da inviare all'esterno dell'Amministrazione sono trasmessi, a cura degli uffici interni mittenti, previa la verifica di cui al precedente articolo 27, mediante le caselle di posta elettronica certificata di cui al precedente art. 7.
2. Se il documento informatico è inoltrato all'Ufficio Protocollo su supporto rimovibile, la trasmissione avviene a mezzo posta ordinaria, salvo diversa indicazione da parte dell'ufficio interno mittente.

Art. 30: Spedizione di documenti cartacei a mezzo posta

1. L'Ufficio Protocollo provvede direttamente a tutte le operazioni necessarie alla spedizione della corrispondenza.
2. Al fine di consentire il regolare svolgimento di tali operazioni gli uffici dell'Amministrazione devono far pervenire la posta in partenza all'Ufficio Protocollo nelle ore stabilite dall'Ufficio stesso.
3. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

Art. 31: Ricezione e trasmissione di documenti cartacei a mezzo telefax

1. Il documento ricevuto o trasmesso mediante telefax soddisfa il requisito della forma scritta e, pertanto, ad esso, di norma, non deve far seguito la trasmissione dell'originale.
2. Qualora al documento faccia seguito l'originale, su quest'ultimo viene apposta la seguenti dicitura; "GIA' PERVENUTO VIA FAX IL GIORNO…".
3. Il documento trasmesso dall'Amministrazione mediante telefax reca una delle seguenti diciture:
a) "ANTICIPATO VIA TELEFAX", se il documento originale viene successivamente inviato al destinatario;
b) "LA TRASMISSIONE VIA FAX DEL PRESENTE DOCUMENTO NON PREVEDE L'INVIO DEL DOCUMENTO ORIGINALE", nel caso in cui l'originale non venga spedito.
4. L'ufficio è, comunque, tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta.

Art. 32: Ricevute di trasmissione

1. L'Ufficio Protocollo cura anche l'invio delle ricevute di trasmissione o di ritorno (fax - raccomandate A/R) all'ufficio interno mittente che si fa carico di archiviarle nel relativo fascicolo fisico, per quanto riguarda le ricevute pec l'archiviazione avviene in modo automatico tramite la procedura di protocollo, associando a ciascuna pec le relative ricevute di consegna ed accettazione.

VI – REGOLE DI ASSEGNAZIONE E SMISTAMENTO DEI DOCUMENTI RICEVUTI

Art. 33: Regole generali

1. Con l'assegnazione si procede all'individuazione dell'UU destinatario del documento, mentre l'attività di smistamento consiste nell'inviare (tramite il sistema di protocollo elettronico) il documento protocollato e segnato all'UU medesimo, come meglio specificato negli articoli successivi.
2. L'assegnazione può essere estesa a tutti i soggetti ritenuti interessati.
3. L'UU, mediante il sistema di protocollo informatico, provvede alla presa in carico dei documenti assegnati o al rinvio alla UOP degli stessi se non di competenza.
4. Nel caso di assegnazione errata, l'UU che riceve il documento, lo restituisce all'UOP che procede ad una nuova assegnazione e ad un nuovo smistamento.
5. I termini per la definizione del procedimento amministrativo che, eventualmente, prende avvio dal documento, decorrono, comunque, dalla data di protocollazione.
6. Il sistema di gestione informatica dei documenti memorizza tutti i singoli passaggi conservandone, per ciascuno di essi, l'identificativo dell'operatore, la data e l'ora di esecuzione.

7. La traccia risultante dalle operazioni di cui al comma precedente definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità

Art. 34: Assegnazione e smistamento di documenti ricevuti in formato digitale

1. I documenti ricevuti dall'Ufficio Protocollo per via telematica, o comunque disponibili in formato digitale, sono assegnati e smistati all'UU competente attraverso canali telematici interni al termine delle operazioni di registrazione, segnatura di protocollo e memorizzazione su supporti informatici in forma non modificabile.
2. L'UU competente ed il Responsabile d'Area a cui sottendono i vari UU hanno notizia, immediatamente, al termine della procedura di protocollazione, dell'arrivo della posta indirizzata agli UU, direttamente o per conoscenza, tramite il sistema informatico (Sezione Comunicazioni della procedura in dotazione all'Ente).
3. Gli addetti all'UU possono visualizzare i documenti attraverso l'utilizzo dell'applicazione di protocollo informatico e, in base alle abilitazioni previste, potranno:
a) visualizzare gli estremi del documento;
b) visualizzare il contenuto del documento.
4. La presa in carico dei documenti informatici viene registrata dal sistema di protocollo informatico in modo automatico e la data di ingresso dei documenti negli UU competenti coincide con la data di assegnazione degli stessi.
5. Ogni responsabile degli UU ha la possibilità di archiviare e/ sub assegnare le pratiche al personale dell'UU che ritiene più opportuno.

Art. 35: Assegnazione e smistamento di documenti ricevuti in formato cartaceo

1. Per l'assegnazione e lo smistamento dei documenti ricevuti in forma cartacea, la procedura sarà la seguente:
a) La compilazione/firma per ricevuta dei moduli se prevista (ad esempio: ricevute di ritorno per raccomandate, posta celere, corriere) è a cura dell'ufficio Protocollo.
b) I documenti cartacei ricevuti, dopo le operazioni di registrazione e segnatura di protocollo, prima dell'inoltro all'ufficio competente vengono acquisiti digitalmente, il formato da usare ai fini della conservazione è il pdf/a.
b.1) L'Ufficio protocollo verifica la leggibilità, la accessibilità e la qualità del file acquisito e verifica che il file sia associato alla rispettiva registrazione di protocollo.
b.2) Tutti i tipi di documenti in formato A4, comunque separabili o leggibili dal supporto tecnico vengono digitalizzati con lo scanner. In caso di planimetrie o volumi non sperabili si potrà comunque procedere a digitalizzare con lo scanner il frontespizio. La digitalizzazione con lo scanner potrà comunque avvenire anche in un secondo tempo rispetto alle procedure di protocollazione.
c) al termine delle operazioni di cui al punto precedente, il sistema di protocollo informatico trasmette (in formato digitale) automaticamente ai vari UU ed ai loro Responsabili i documenti assegnati ;
d) dopo lo svolgimento delle operazioni di cui al precedente punto b), b.1) e b.2) da parte dell'Ufficio Protocollo, i documenti vengono conservati a cura dell'ufficio protocollo.

VII – U.O. RESPONSABILI DELLE ATTIVITA' DI REGISTRAZIONI DI PROTOCOLLO, DI ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

Art. 36: Ufficio Protocollo e Archivio comunale

1. Secondo quanto stabilito al precedente articolo 4, è istituito il Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi, individuandolo nell'Area Amministrativa e Demografica – Servizio "Affari generali";
2. Nell'ambito della predetta Area Amministrativa e demografica, il Servizio Protocollo e Albo Pretorio svolge le funzioni relative alla tenuta e alla gestione del protocollo informatico, dei flussi documentali, ampiamente descritte in tutto il presente Manuale di gestione; esso inoltre:
a) costituisce il punto centralizzato di apertura al pubblico per il ricevimento della corrispondenza indirizzata all'Amministrazione;
b) costituisce il punto centralizzato di spedizione della corrispondenza in partenza dall'Amministrazione;
c) cura il ritiro della corrispondenza indirizzata all'Amministrazione;
d) cura la consegna agli uffici postali della corrispondenza in partenza dall'Amministrazione;
e) cura lo smistamento agli uffici competenti di destinazione della corrispondenza ricevuta dall'Amministrazione e di quella interna tra gli uffici;
f) gestisce le caselle di Posta Elettronica Certificata dell'AOO, relativamente alla posta in arrivo ed in partenza;
g) gestisce il ricevimento delle gare;
h) gestisce la corrispondenza delle persone residenti presso la Casa comunale.

Art. 37: Servizio per la conservazione elettronica dei documenti

1. Il Servizio per la conservazione elettronica dei documenti è svolto dal "Servizio Informatico" dell'Amministrazione che cura la gestione del Server in cui sono memorizzati i dati dell'Ente.
2. Il Sistema informatico, per la conservazione dei dati, garantisce che le informazioni in esso memorizzate siano sempre consultabili ed estraibili.
3. E' nominato un responsabile per la conservazione che sovrintende al processo di conservazione dei documenti informatici, secondo quanto previsto dalla normativa vigente[9]; egli inoltre, d'intesa con il RSP e valutati i costi e i benefici, può proporre l'operazione di conservazione sostitutiva dei documenti analogici su supporti di memorizzazione sostitutivi del cartaceo, in conformità alle disposizioni vigenti[10].

VIII – DOCUMENTI ESCLUSI DALLA REGISTRAZIONE O SOGGETTI A REGISTRAZIONE PARTICOLARE

Art. 38: Documenti esclusi dalla registrazione di protocollo

1. Le tipologie di documenti esclusi dalla registrazione di protocollo fanno riferimento al comma 5 dell'art. 53 del D.P.R. 28.12.2000, n. 445, che recita:

"Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e 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 e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

Inoltre, sono escluse dalla protocollazione le seguenti categorie di documenti:

• Le comunicazioni d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);

9 D.P.C.M. 3-12-2013 Regole tecniche in materia di sistema di conservazione

10 Art. 4 della Deliberazione CNIPA n. 11 del 19.2.2004

• Le richieste di ferie ed altri permessi;
• Le richieste di rimborso spese e missioni;
• Gli allegati, se accompagnati da lettera di trasmissione, compresi gli elaborati tecnici;
• La pubblicità conoscitiva di convegni;
• La pubblicità in generale;
• Le offerte, i listini prezzi e i preventivi di terzi non richiesti;
• Le ricevute di ritorno delle raccomandate A.R.;
• Tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico amministrativa presente o futura.

Art. 39: Documenti soggetti a registrazione particolare

1. Le tipologie di documenti soggetti a registrazione particolare sono le seguenti:
• Atti rogati o autenticati dal Segretario Generale;
• Contratti e convenzioni;
• Verbali delle sedute del Consiglio comunale;
• Verbali delle sedute della Giunta Municipale;
• Verbali delle sedute delle Commissioni Consiliari permanenti e speciali;
• Verbali delle Commissioni istituite per legge;
• Atti di stato civile;
• Pubblicazioni di matrimonio;
• Carte d'identità;
• Certificati anagrafici;
• Tessere elettorali;
• Atti di liquidazione;
• Mandati di pagamento;
• Reversali d'incasso;
• Verbali di violazione al Codice della strada;
• Verbali di violazioni amministrative;
• Delibere del Consiglio comunale,
• Delibere della Giunta Municipale;
• Ordinanze;
• Ordinanze prefettizie relative a procedimenti sanzionatori;
• Atti pubblicati all'Albo Pretorio e le relative richieste e conferme di avvenuta pubblicazione;
• Atti depositati alla casa comunale;
• Notifiche.

2. Tale tipo di registrazione consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione documentale, in particolare la classificazione, la fascicolazione, la repertoriazione.

IX – SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

Art. 40: Generalità

1. La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge[11] e si avvale del piano di conservazione di cui al successivo articolo 41 e del titolario di cui al successivo articolo 42.
2. Ai sensi della normativa vigente:
a) gli archivi e i singoli documenti dell'Amministrazione sono beni culturali inalienabili[12];
b) gli archivi non possono essere smembrati a qualsiasi titolo e devono essere conservati nella loro organicità[13];
c) lo spostamento della sede dell'archivio storico e dell'archivio di deposito è soggetto ad autorizzazione[14];
d) lo spostamento della sede dell'archivio corrente non è soggetto ad autorizzazione[15];
e) lo scarto dei documenti degli archivi dell'Amministrazione è soggetto ad autorizzazione[16].

Art. 41: Piano di conservazione

1. Il piano di conservazione definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio dell'Amministrazione.
2. Il piano di conservazione adottato dall'Amministrazione corrisponde a quanto elaborato dal Ministero per i beni e le attività culturali.

Art. 42: Titolario di classificazione

1. Il titolario di classificazione è lo schema logico utilizzato per organizzare i documenti di archivio in base alle funzioni e alle materie di competenza dell'ente e si suddivide in titoli, classi, sottoclassi.
1.1. E' adottato il seguente "Schema riassuntivo del piano di classificazione per l'archivio comunale";

11 Art. 30, comma 4 del D. Lgs. 22.1.2004, n. 42 recante "Codice dei beni culturali"

12 Art. 54, comma 1, lett. d) e comma 2, lett. c) del D. Lgs. 42/2004

13 Art. 29 e art. 30, comma 1 del D. Lgs. 42/2004

14 Art. 21, comma 2, del D. Lgs. 42/2004

15 Art. 21, comma 3, del D. Lgs. 42/2004

16 Art. 21, comma 1, lett. d) del D. Lgs. 42/2004

Schema riassuntivo del piano di classificazione per l'archivio comunale	
I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana 17. Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario ad acta 14. Organi di controllo interni 15. Organi consultivi 16. Consigli circoscrizionali (se presenti) 17. Presidente dei Consigli circoscrizionali (se presenti) 18. Organi esecutivi circoscrizionali (se presenti) 19. Commissioni dei Consigli circoscrizionali (se presenti) 20. Segretari delle circoscrizioni (se presenti) 21. Commissario ad acta delle circoscrizioni (se presenti) 22. Conferenza dei Presidenti di quartiere (se presenti)

III	Risorse umane 1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo 8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari 14. Formazione e aggiornamento professionale 15. Collaboratori esterni
IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni
V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni 3. Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze

VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio 10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive 7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale 2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio 3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri

XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi

2. I titoli in cui è suddiviso il titolario individuano le funzioni primarie e di organizzazione dell'Amministrazione; le successive partizioni corrispondono a specifiche competenze che rientrano concettualmente nella macro funzione descritte dal titolo.
3. Tutti i documenti ricevuti e prodotti dall'Amministrazione, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolario.
4. Il titolario può essere aggiornato a seguito di modifiche intervenute nelle funzioni e nelle competenze dell'Amministrazione in forza di leggi e regolamenti statali e/o regionale, ovvero rivisto qualora sorgesse l'esigenza di riorganizzarne la struttura interna.
5. Il RSP, anche in accordo con gli uffici eventualmente interessati, cura l'aggiornamento e/o la revisione del titolario provvedendo, dopo ogni modifica, ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.
6. Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello della loro approvazione e valgono almeno per l'intero anno.
7. Il sistema di protocollo informatico garantisce che per ogni modifica di una voce del titolario venga riportata la data di introduzione e la data di variazione della stessa; il sistema, inoltre, 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 rispetto al momento della produzione degli stessi.

X – MODALITA' DI PRODUZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO

Art. 43: Unicità del protocollo informatico

1. Nell'ambito della AOO l'Amministrazione istituisce un unico registro di protocollo generale, articolato in modo tale che sia possibile determinare se il documento sia in arrivo o in partenza, ovvero se si tratti di un documento interno.
2. La numerazione progressiva delle registrazioni di protocollo è unica, si chiude al 31 dicembre di ogni anno e ricomincia dal 1° gennaio dell'anno successivo.

3. Ai sensi della normativa vigente[17], il numero di protocollo e costituito da almeno sette cifre numeriche; esso individua un solo documento e, pertanto, ogni documento deve recare un solo numero di protocollo.
4. Non è consentita la protocollazione di documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatica ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.
5. Non è consentita, in nessun caso, né la protocollazione di un documento già protocollato, né la cosiddetta "registrazione a fronte", vale a dire l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.
6. Il registro di protocollo è un atto pubblico che fa fede dell'effettivo ricevimento o spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici; esso, pertanto, è soggetto alle forme di pubblicità e di tutela delle situazioni giuridicamente rilevanti previste dalle norme.

Art. 44: Registro giornaliero di protocollo

1. La produzione del registro giornaliero di protocollo avviene, quotidianamente, mediante creazione automatica, su supporto informatico, dell'elenco dei protocolli e delle informazioni ad essi connesse, registrati nell'arco di uno stesso giorno.
2. Come già stabilito al precedente art. 5, il contenuto del registro informatico di protocollo è conservato a cura del responsabile del servizio per la conservazione elettronica dei documenti di cui al precedente articolo 37.

Art. 45: Registrazioni di protocollo

1. Ai sensi della normativa vigente[18] e con le eccezioni previste ai precedenti artt. 37 e 38, su ogni documento ricevuto o spedito dall'AOO e sui documenti interni formali, viene effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei seguenti dati obbligatori:
a) il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
b) la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
c) il mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
d) l'oggetto del documento, registrato in forma non modificabile;
e) la data e il numero di protocollo del documento ricevuto, se disponibili;
f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
2. La registrazione di protocollo di un documento informatico viene effettuata a seguito della procedura previste ai precedenti articoli 13, 17, 18, 21 e 27.
3. La registrazione di protocollo di un documento cartaceo viene effettuata a seguito delle procedure previste ai precedenti articoli 13, 19, 21, 22 e 27.

Art. 46: Elementi facoltativi delle registrazioni di protocollo

1. La registrazione di protocollo di un documento, oltre ai dati obbligatori di cui al precedente articolo 46, può contenere i seguenti elementi facoltativi:

17 Art. 57 del "TESTO UNICO

18 Artt. 53, comma 1, e 56 del "TESTO UNICO"

a) la classificazione del documento;
b) il luogo di provenienza o di destinazione del documento;
c) il mezzo di ricezione/spedizione del documento (ad esempio: raccomandata o fax);
d) il collegamento ad altri documenti;
e) il riferimento agli allegati;
f) il nominativo dei destinatari delle copie per conoscenza;
g) l'UU competente;
h) il nominativo del RPA.
2. In caso di errore di registrazione gli elementi facoltativi di cui al comma precedente sono modificabili senza ricorrere alla procedura di cui al successivo articolo 56, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Art. 47: Segnatura di protocollo dei documenti

1. La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso.
2. L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
3. I dati della segnatura di protocollo di un documento informatico sono contenuti in un file conforme alla specifiche tecniche previste dalla normativa vigente[19].
4. La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un segno grafico il quale, di norma, è realizzato con un'etichetta autoadesiva corredata da codice a barre o, in alternativa, con un timbro tradizionale.
5. La segnatura di protocollo sia per i documenti informatici che per quelli cartacei deve contenere obbligatoriamente, ai sensi della normativa vigente[20] le seguenti informazioni:
a) l'indicazione in forma sintetica dell'Amministrazione;
b) data e numero di protocollo del documento.
6. Ad integrazione degli elementi obbligatori di cui al precedente comma 5, la segnatura di protocollo può contenere le seguenti informazioni facoltative:
a) denominazione dell'AOO;
b) indice di classificazione.
c) la tipologia di protocollo Arrivo/Partenza
7. L'acquisizione dei documenti cartacei in formato immagine è effettuata solo dopo che l'operazione di segnatura di protocollo è stata eseguita in modo da acquisire con l'operazione di scansione, come immagine, anche il segno sul documento; in tali casi il segno deve essere apposto sulla prima pagina dell'originale.

Art. 48: Annullamento delle registrazioni di protocollo

1. Ai sensi della normativa vigente[21], l'annullamento e/o la modifica anche di uno solo dei dati obbligatori della registrazione di protocollo di cui al comma 1 del precedente articolo 45 devono essere richieste, con specifica nota motivata, al RSP o suoi delegati che sono i soli che possono autorizzare lo svolgimento delle relative operazioni; le modifiche effettuate direttamente dal RSP o dai suoi delegati equivalgono implicitamente ad autorizzazione, fermo restando che, in ogni caso, per l'annullamento di un numero di protocollo, occorre comunque l'adozione di apposito atto.
2. I dati annullati e/o modificati rimangono memorizzati nella procedura del protocollo informatico unitamente alle informazioni relative all'ora, alla data, al nominativo dell'operatore che effettua l'operazione.

19 REGOLE TECNICHE" e Circolare AIPA n. 28 del 7.5.2001

20 Art. 55, comma 1, del "TESTO UNICO"

21 Artt. 54 e 61 del "TESTO UNICO"

3. L'annullamento del numero di protocollo comporta l'annullamento di tutta la registrazione di protocollo.

Art. 49: Documenti con più destinatari

1. Le circolari, le disposizioni generali e tutte le altre comunicazioni interne che abbiano più destinatari si registrano con un solo numero di protocollo generale; i destinatari, se in numero consistente, sono contenuti in appositi elenchi allegati alla minuta del documento.
2. Le stesse disposizioni di cui al comma precedente si applicano per i documenti in partenza con più destinatari.
3. Qualora il testo dei documenti in partenza con più destinatari sia analogo, ma presenti differenze in alcuni campi variabili, l'elenco dei destinatari di cui ai commi precedenti contiene anche, per ogni singolo destinatario, i dati relativi ai campi variabili.

Art. 50: Protocollazione di telegrammi

1. I telegrammi ricevuti dall'Amministrazione, ad eccezione di quelli esclusi dalla registrazione di cui all'articolo 38, sono regolarmente protocollati e su di essi viene apposta la segnatura di protocollo.
2. I telegrammi spediti dall'Amministrazione, con le medesime eccezioni di cui al comma precedente, vengono anch'essi protocollati, tuttavia, poiché su di essi non è possibile apporre la segnatura di protocollo, gli elementi obbligatori di tale segnatura, di cui al comma 5 del precedente articolo 47, faranno parte del testo del telegramma medesimo.

Art. 51: Protocollazione di telefax

1. Qualora al documento ricevuto mediante telefax faccia seguito l'originale, l'operatore addetto alla registrazione di protocollo deve attribuire all'originale la stessa segnatura del documento ricevuto mediante telefax.
2. Qualora, invece, si riscontri una differenza, anche minima, tra il documento ricevuto mediante telefax e il successivo originale, quest'ultimo deve essere ritenuto un documento diverso e, pertanto, si deve procedere ad una nuova registrazione di protocollo.
3. La segnatura di protocollo deve essere apposta sul documento e non sulla copertina di trasmissione.
4. La copertina del telefax e il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

Art. 52: Protocollazione di corrispondenza digitale già pervenute cartacea

1. Qualora il documento ricevuto in formato cartaceo sia seguito da un invio digitale dello stesso, l'operatore addetto alla registrazione di protocollo deve in ogni caso apporre una nuova registrazione di protocollo, e, nel caso abbia già protocollato il documento cartaceo, indicare "ARRIVATO CARTACEO E PROTOCOLLATO IN DATA --- AL N. ----"

Art. 53: Protocollazione di un numero consistente di documenti

1. Qualora si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso che in uscita, l'ufficio interessato deve darne comunicazione all'UOP di riferimento con sufficiente anticipo, al fine di concordare tempi e modi di protocollazione e di spedizione.

Art. 54: Corrispondenza relativa alle gare d'appalto

1. La corrispondenza relativa alla partecipazione alle gare d'appalto o dal cui involucro è possibile evincere che si riferisca alla partecipazione ad una gara, non deve essere aperta ma protocollata con l'apposizione della segnatura e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili e deve essere inviata all'ufficio competente che la custodisce sino all'espletamento della gara stessa.
2. Per motivi organizzativi, tutti gli uffici sono tenuti ad informare preventivamente il RSP in merito alla scadenza di concorsi, gare e bandi di ogni genere.

Art. 55: Corrispondenza pervenuta per posta raccomandata

1. Tutta la corrispondenza pervenuta tramite posta raccomandata viene sottoposta alle operazioni di registrazione di protocollo e di segnatura anche nel caso in cui la tipologia rientri nel novero dei documenti esclusi dalla registrazione di protocollo, o dei documenti soggetti a registrazione particolare.

Art. 56: Protocolli urgenti

1. Relativamente alla posta in arrivo, il RSP può disporre la protocollazione immediata dei documenti urgenti o perché ritenuti tali dal RSP medesimo o perché il carattere d'urgenza è reso evidente dal contenuto del documento stesso.
2. Analogamente si procede per la posta in partenza, anche su richiesta motivata dagli uffici mittenti, avendo cura che la protocollazione può avvenire solo per documenti resi effettivamente disponibili, come già stabilito in tal senso al comma 2 dell'articolo 63.

Art. 57: Documenti anonimi o non firmati

1. I documenti anonimi sono sottoposti alle operazioni di registrazione di protocollo e di segnatura e su di essi viene apposta la dicitura "MITTENTE ANONIMO".
2. Analogamente si procede per i documenti in cui vi è l'indicazione del mittente ma manca la sottoscrizione, e su di essi viene apposta la dicitura "DOCUMENTO NON SOTTOSCRITTO".
3. Relativamente ai documenti di cui ai commi precedenti, spetta al Segretario Comunale valutare la loro validità e trattarli di conseguenza.

Art. 58: Corrispondenza personale o riservata

1. La corrispondenza personale è regolarmente aperta dall'ufficio protocollo, a meno che sulla busta non sia riportata la dicitura "RISERVATA" o "PERSONALE" o formula equivalente;
2. La corrispondenza recante la dicitura "RISERVATA" o "PERSONALE" viene consegnata in busta chiusa al destinatario, accompagnata dalla ricevuta di cui al seguente articolo.
3. Il destinatario, se reputa che i documenti ricevuti debbano essere, comunque, protocollati, provvede a trasmetterli all'ufficio protocollo.

Art. 59: Corrispondenza consegnata con ricevuta

1. In casi particolari, a giudizio del RSP, la corrispondenza in arrivo può essere consegnata agli uffici interni di destinazione, dopo le operazioni di registrazione di protocollo e di segnatura, unitamente ad una ricevuta, appositamente predisposta dall'ufficio protocollo, in duplice copia,

delle quali una viene trattenuta dall'ufficio di destinazione e l'altra, firmata da un addetto alla ricezione, viene restituita all'ufficio protocollo.

Art. 60: Integrazioni documentarie

1. Gli addetti al ricevimento della corrispondenza e alle registrazioni di protocollo non sono tenuti a verificare la completezza formale e sostanziale della documentazione pervenuta, ma unicamente a verificare la corrispondenza fra gli eventuali allegati dichiarati e gli allegati effettivamente presentati con la pratica.
2. La verifica di cui al comma 1 spetta all'ufficio competente o al RPA che, qualora ritenga necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente con le comunicazioni del caso.

XI – DESCRIZIONE FUNZIONALE ED OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO

Art. 61: Descrizione del sistema di protocollo informatico

1. La descrizione funzionale ed operativa del sistema di protocollo informatico in uso presso l'AOO è contenuta nell'allegato "B" del presente Manuale di gestione.

XII – RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

Art. 62: Generalità

1. Il controllo degli accessi è attuato al fine di garantire l'impiego del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.
2. Gli utenti ed operatori del servizio di protocollo hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni richieste dall'ufficio di appartenenza e alle rispettive competenze.
3. Ad ogni operatore di protocollo è assegnata, oltre alla credenziale di accesso al sistema delle procedure in uso presso l'Ente , consistente in "userID" e "password", una autorizzazione d'accesso, definita "profilo" al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

Art. 63: Profili di accesso

1. Sulla base delle richieste avanzate dagli uffici dell'Amministrazione, i diversi livelli di autorizzazione ed i conseguenti differenti profili sono assegnati agli utenti dal RSP il quale, inoltre, provvede all'assegnazione di eventuali nuove autorizzazioni, alla revoca o alla modifica di quelle già assegnate.
2. A tal fine sono individuati i seguenti tre profili di accesso, cui corrispondono altrettanti livelli diversificati di accesso alle funzioni del sistema di protocollo informatico:
a) Amministratore di sistema;
b) Responsabile di protocollo;

c) Operatore di protocollo;
d) Utente di consultazione.

Art. 64 : Rete delle comunicazioni di avvenuta protocollazione.

1. In relazione alla struttura organizzativa dell'Ente, su indicazione del Responsabile di Area, è individuata la corrispondenza fra gli UU e gli operatori che ricevono la comunicazione di avvenuta protocollazione di un documento diretto o in partenza da quella UU.
2. I responsabili di Area ricevono la comunicazione di avvenuta protocollazione di ogni documento partito o arrivato agli UU che sottendono alla propria Area.

XIII – MODALITA' DI UTILIZZO DEL REGISTRO DI EMERGENZA

Art. 65: Registro di emergenza

1. Qualora si verificassero interruzioni, accidentali o programmate, nel funzionamento del sistema di protocollo informatico, l'AOO è tenuta, ai sensi della normativa vigente[22], ad effettuare le registrazioni di protocollo su un registro di emergenza.
2. Presso l'Ufficio Protocollo il registro di emergenza viene predisposto su indicazione del RSP e a secondo delle particolari condizioni o in forma cartacea oppure in forma digitale;
3. Al ripristino della funzionalità del sistema di protocollo informatico tutte le registrazioni effettuate mediante i registri di emergenza vengono recuperate dal sistema, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.
4. 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.

Art. 66: Apertura del registro di emergenza

1. Il RSP autorizza, con proprio provvedimento, l'avvio dell'attività di protocollo sul registro di emergenza.
2. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del sistema informatico di protocollo.
3. Qualora l'interruzione nel funzionamento del sistema di protocollo informatico si prolunghi per più di ventiquattro ore, il RSP, ai sensi della normativa vigente[23], autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana; in tali casi sul registro di emergenza, oltre alle notizie di cui al precedente comma 2, vengono riportati gli estremi del provvedimento di autorizzazione.

Art. 67: Utilizzo del registro di emergenza

1. La sequenza numerica utilizzata su un registro di emergenza può essere liberamente scelta ma deve comunque garantire l'identificazione univoca dei documenti registrati.

22 Art. 63 del "TESTO UNICO"

23 Art. 63, comma 2, del "TESTO UNICO"

2. Il formato delle registrazione di protocollo di emergenza, ovvero i campi obbligatori delle registrazioni sono gli stessi previsti per il sistema di protocollo informatico di cui al comma 1 del precedente articolo 45

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

Art. 68: Chiusura e recupero del registro di emergenza

1. Quando viene ripristinata la piena funzionalità del sistema di protocollo informatico, l'Ufficio Protocollo provvede alla chiusura del registro di emergenza, annotando sullo stesso il numero delle registrazioni effettuate e la data e l'ora di ripristino della funzionalità del sistema.
2. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico di protocollo.
3. Durante la fase di recupero dei dati a ciascun documento registrato in emergenza viene attribuito un numero di protocollo generale che deve mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

XIV - NORME GENERALI PER LA PRESENTAZIONE DI PRATICHE DE-MATERIALIZZATE

Art. 69 – Definizioni

Ai fini del presente regolamento si intende per:
a) Codice dell'Amministrazione Digitale (o Codice): il D.Lgs. 7-3-2005 n. 82
b) posta elettronica certificata (PEC): sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi, di cui all'art. 48 del Codice.
c) Carta di Identità Elettronica (CIE): Il documento di identità elettronico di cui all'art. 66 comma 1 del Codice.
d) Carta Nazionale dei Servizi (CNS): Il documento di identità elettronico di cui all'art. 66 comma 2 del Codice.
e) Istanza: una richiesta in forma scritta indirizzata al Comune per l'attivazione di una procedura amministrativa, finalizzata all'emanazione di un provvedimento e all'attivazione di un'azione;
f) Comunicazione: la trasmissione di un documento, di qualunque natura, al Comune nell'ambito di un procedimento amministrativo o di altre attività proprie dell'ente;
g) Pratica: insieme di atti e documenti necessari all'avvio, processamento e completamento di una procedura amministrativa nelle materie di competenza dell'ente;
h) Firma digitale: Firma elettronica di cui all'Art. 1 comma 1 lettera s) del Codice.

Art. 70 – Modalità di invio telematico

1. L'invio di istanze o di comunicazioni relative ai procedimenti amministrativi informatici può avvenire mediante le seguenti modalità:
a) Utilizzo di un servizio dedicato on-line all'indirizzo reperibile sul sito del Comune, se disponibile per lo specifico procedimento amministrativo;
b) Mediante invio da una casella PEC commerciale all'indirizzo PEC reperibile sul sito del Comune

2. L'invio di istanze o comunicazioni, secondo una delle modalità sopra riportate, può anche essere effettuato da un delegato cui il diretto interessato abbia conferito la procura speciale, se prevista dalla specifica procedura da avviare;
3. L'istanza o la comunicazione è da considerarsi validamente presentata se inviata secondo una delle seguenti procedure:
a) con la sua compilazione e sottoscrizione, da parte del diretto interessato, su supporto cartaceo e successivo invio, da parte di un procuratore, con una delle modalità di invio telematiche di cui ai commi precedenti;
b) con la sua compilazione in formato elettronico seguita dall'apposizione della firma digitale dell'interessato e la trasmissione, sempre da parte del diretto interessato, con una delle modalità di invio telematico di cui ai commi precedenti;
c) con la sua compilazione in formato elettronico, seguita dall'apposizione di firma digitale del diretto interessato, e successivo invio, da parte di un procuratore speciale, con una delle modalità di invio telematico di cui ai commi precedenti;
Nel caso si sia seguita la modalità di presentazione di cui al punto a) del precedente comma, il procuratore è tenuto a conservare l'originale cartaceo, firmato dal diretto interessato, limitandosi a spedire, con la modalità scelta, la versione scansionata di tale documentazione originale. In questo caso l'originale cartaceo dovrà essere conservato, a cura del procuratore, per un periodo di tempo congruo e comunque fino a quando non il provvedimento finale della procedura attivata non si sia consolidato.
Il procuratore dovrà in ogni momento consentire al Comune di poter accedere a tale documentazione originale a scopo di verifica.
Nel caso si sia seguita la modalità di presentazione di cui al punto b) del precedente comma, se il diretto interessato è un semplice cittadino, ed il canale scelto per la spedizione è costituito da:
1. utilizzo di un servizio dedicato on-line previa propria autenticazione ottenuta con l'uso di Carta di identità elettronica e/o Carta nazionale dei servizi, la firma digitale della documentazione non è indispensabile visto il valore di firma attributivo a tali modalità di trasmissione dall'art. 65 del Codice dell'Amministrazione Digitale.
Nel caso di Professionisti e/o imprese resta l'obbligo dell'apposizione della firma digitale.
Nel caso si sia seguita la modalità di presentazione di cui al punto c) del precedente comma, il diretto interessato deve compilare la documentazione in formato elettronico, firmandola digitalmente e conferendo procura speciale al soggetto (procuratore) che provvede all'invio telematico di tale documentazione elettronica.
Nel caso in cui l'invio avvenga, sia da parte dell'interessato che da parte di un procuratore, mediante messaggio PEC con uno dei sistemi di cui ai punti b) e c) del primo comma del presente articolo, il messaggio di posta elettronica dovrà essere formato in modo da:
a) Contenere una sola istanza o comunicazione
b) Essere conforme ai formati ed alle regole tecniche indicate nella normativa nazionale e regionale;
I messaggi PEC non conformi a quanto disposto nei precedenti commi **potranno** essere respinti da parte del Comune e le relative pratiche risulteranno come "non presentate".
Del respingimento dell'istanza e/o comunicazione, per difformità alle regole di invio stabilite dal presente regolamento, l'ufficio interessato o l'ufficio protocollo, nel caso di impossibilità assoluta di trasmissione attraverso il protocollo interno, darà opportuna comunicazione all'interessato o al suo procuratore entro un termine congruo, in relazione allo specifico procedimento, nel caso che non vi siano norme specifiche e comunque entro un termine non superiore a 15 gg;

Art. 71 - Procedure d'emergenza

In caso di mancato funzionamento degli strumenti e dei dispositivi informatici, messi a disposizione per l'effettuazione dell'invio di istanze secondo le modalità previste dal comma 1 del precedente articolo, per un periodo superiore alle tre ore consecutive durante l'orario di apertura degli uffici competenti, l'utente è autorizzato ad utilizzare la modalità di cui all'articolo 38 del D.P.R. 28 dicembre 2000 n. 445. Di tale interruzione si da atto in apposito provvedimento del Responsabile del servizio interessato.

Nell'ipotesi di cui al precedente comma, entro cinque giorni dal venir meno della causa che ha generato l'impedimento, l'interessato o il suo procuratore, è tenuto a provvedere, utilizzando una delle modalità previste dal precedente articolo, all'invio telematico di ogni documento analogico già trasmesso, comunicando gli estremi del protocollo assegnato o, in mancanza, gli estremi di tale trasmissione. In tal caso, l'utente è esentato dal ripetere il versamento di imposte e diritti e di ogni altra somma a tale titolo corrisposta.
Qualora l'invio elettronico successivo contenga materiale difforme da quanto inviato avvalendosi delle facoltà di cui al primo comma, valgono le regole per gli invii multipli di cui agli articoli seguenti.

Art. 72 - Oggetto del messaggio di posta elettronica

Qualora l'istanza o la comunicazione venga inviata mediate posta elettronica, ed indipendentemente dal tipo di cassetta postale utilizzata, tra quelle ammesse dal presente regolamento, l'oggetto del messaggio dovrà contenere tutti gli elementi necessari ad individuare in modo univoco il contenuto.
A tale oggetto sono da applicarsi in aggiunta le regole sugli invii successivi e multipli di cui agli articoli seguenti.

Art. 73- Invii multipli e successivi

Qualora le dimensioni complessive del materiale da trasmettere siano eccessive e tali da richiedere l'invio di più messaggi consecutivi. Gli stessi messaggi dovranno essere singolarmente composti e deve essere assolutamente chiaro che trattasi di invii multipli di un unico argomento. A tale proposito l'oggetto dei messaggi dovrà essere unico e ognuno dovrà differire solo per la scritta "INVIO x di n" con x progressivo da 1 ad n ed n costante, pari al totale degli invii.
Qualora, in relazione ad una medesima istanza, si effettuino invii successivi degli stessi documenti, l'invio successivo si intende ad integrazione o in sostituzione degli invii precedenti in base alle dizioni contenute nel nuovo messaggio.

Art. 74 – Arrivi multipli e successivi

Qualora le dimensioni complessive del materiale trasmesso abbiano necessitato l'invio di più messaggi consecutivi da cui si evince che trattasi della stessa pratica, l'oggetto dei messaggi multipli dovrà essere integrato con la scritta "ARRIVO x di n" con x progressivo da 1 ad n ed n costante, pari al totale degli invii.
Ognuno degli invii multipli avrà un numero di protocollo diverso e dovrà contenere nella nota che trattasi di invio multiplo e se possibile dovrà essere riportato il numero di tutti gli altri protocolli dello stesso invio multiplo.
Qualora, in relazione ad una medesima istanza, si abbiano arrivi successivi degli stessi documenti, l'invio successivo si intende ad integrazione o in sostituzione degli invii precedenti in base alle dizioni contenute nel nuovo messaggio; l'ufficio protocollo procederà in ogni caso alla protocollazione, sarà cura dell'UU procedere all'archiviazione dello stesso qualora ritenga che trattasi di duplicato.

Art. 75 - Pratiche inviate su supporto cartaceo

Per le pratiche in corso di esame presentate in forma cartacea, il procedimento si conclude in forma cartacea.

Art. 76 - Bolli, imposte e diritti.

Per il pagamento delle imposte diritti e altre imposte, in occasione di invio di istanze o comunicazioni per via telematica, sarà effettuato secondo le modalità previste dalle specifiche procedure e indicate dagli uffici competenti, fra le seguenti:
a) Pagamento on line con calcolo direttamente effettuato dalla procedura web
b) Pagamento del bollo mediante bollettino postale da effettuarsi alle coordinate indicate sulle pagine internet relative al servizio
c) Pagamento con altro canale indicato specificatamente nelle informazioni relative all'istanza.
Nel caso di pagamento di diritti, tasse o bolli mediante bollettino, copia scansionata della ricevuta o attestazione dello stesso dovrà essere inclusa nella documentazione presentata per via telematica.
Per il calcolo dell'imposta di bollo dovuta si seguono le stesse regole valide per i documenti cartacei facendo riferimento alle pagine di cui sono composti i vari documenti.
Nel caso del bollo lo stesso si ritiene pagato, come sopra, in modalità virtuale e sarà riversato agli organi competenti a cura del Comune

XV – NORME TRANSITORIE E FINALI

Art. 77: Norma transitoria relativa alla irretroattività del titolario

1. Il titolario di classificazione, di cui al precedente articolo 42, sarà in uso dal **1 Gennaio 2016**.

Art. 78: Pubblicità del presente manuale

1. Copia del presente Manuale di gestione è pubblicata sul sito internet dell'Amministrazione.

Art. 79: Entrata in vigore

1. Il presente Manuale di gestione entra in vigore il primo giorno successivo a quello della sua approvazione.

Allegato "A"

Definizioni

AMMINISTRAZIONI CERTIFICANTI
Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti (art. 1, comma 1 lett. p) del DPR n. 445/2000);
AMMINISTRAZIONI PROCEDENTI
Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio (art. 1, comma 1 lett. o) del DPR n. 445/2000);
AMMINISTRAZIONI PUBBLICHE
Quelle indicate nell'art. 1, comma 2 del D. Lgs. 30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI
Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 (art. 1, comma 1 lett. z) del D. Lgs. n. 82/2005);
ARCHIVIO
L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione sono collegati tra loro in un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, esso viene diviso in tre sezioni: corrente, di deposito e storico;
ARCHIVIO CORRENTE
E' costituito dal complesso dei documenti relativi ad affari e procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;
ARCHIVIO DI DEPOSITO
E' costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;
ARCHIVIO STORICO
E' costituito da complessi di documenti relativi ad affari e procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa effettuazione delle operazioni di scarto, alla conservazione perenne;
ARCHIVIAZIONE ELETTRONICA
Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (art. 1 della Deliberazione CNIPA 19 febbraio 2004, n. 11);
ASSEGNAZIONE
L'operazione dell'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE
L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (art. 1, comma 1, lett. i) del DPR n. 445/2000);
AUTENTICAZIONE INFORMATICA

La validazione dell'insieme dei dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso (art. 1, comma 1, lett. b) del D. Lgs. n. 82/2005);

BANCA DI DATI

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art. 4, comma 1, lett. o) del D. Lgs. n. 196/2003);

BLOCCO

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento; (art. 4, comma 1, lett. d) del D. Lgs. n. 196/2003);

CARTA NAZIONALE DEI SERVIZI

Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni (art. 1 del D. Lgs. n. 82/2005);

CARTA D'IDENTITA' ELETTRONICA

Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare (art. 1, comma 1, lett. c) del D. Lgs. n. 82/2005);

CASELLA DI POSTA ELETTRONICA ISTITUZIONALE

La casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del DPCM 31.10.2000, articolo 15, comma 3) – (art. 1 dell'allegato A della circolare AIPA 7 maggio 2001, n. 28);

CERTIFICATI ELETTRONICI

Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi (art. 1, comma 1, lett. e) del D. Lgs. n. 82/2005);

CERTIFICATO QUALIFICATO

Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art. 1, comma 1, lett. f) del D. Lgs. n. 82/2005);

CERTIFICATO

Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (art. 1, comma 1, lett. f) del D.P.R. n. 445/2000);

CERTIFICATORE

Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art. 1, comma 1, lett. g) del D. Lgs. n. 82/2005);

CLASSIFICAZIONE

L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;

COMUNICAZIONE

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4, comma 1, lett. l) del D. Lgs. n. 196/2003);

CONSERVAZIONE SOSTITUTIVA

Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004, n. 11;

CREDENZIALI DI AUTENTICAZIONE

I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art. 4, comma 3, lett. d) del D. Lgs. n. 196/2003);

DATI GIUDIZIARI

I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u), del D.P.R. 13 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4, comma 1, lett. e) del D. Lgs. n. 196/2003);

DATI IDENTIFICATIVI
I dati personali che permettono l'identificazione diretta dell'interessato (art. 4, comma 1, lett. c) del D. Lgs. n. 196/2003);
DATI SENSIBILI
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4, comma 1, lett. ddd) del D. Lgs. n. 196/2003);
DATO ANONIMO
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art. 4, comma 1, lett. n) del D. Lgs. n. 196/2003);
DATO PERSONALE
Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4, comma 1, lett. b) del D. Lgs. n. 196/2003);
DATO PUBBLICO
Il dato conoscibile da chiunque (art. 1, comma 1, lett. n. del D.Lgs. n. 82/2005);
DATO A CONOSCIBILITA' LIMITATA
Il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. 1, comma 1, lett. l) del D. Lgs. n. 82/2005);
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA'
Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti che siano a diretta conoscenza di questi , resa nelle forme previste dall'art. 1, comma 1 lett. h) del D.P.R. 28 dicembre 2000, n. 445;
DICHIARAZIONE SOSTITUTIVA DI DICHIARAZIONE
Il documento sottoscritto dall'interessato, prodotto in sostituzione del certificato (art. 1, comma 1, lett. g) del D.P.R. n. 445/2000);
DIFFUSIONE
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 del D. Lgs. n. 196/2003);
DOCUMENTO
Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (art. 1, comma 1, lett. a) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
DOCUMENTO AMMINISTRATIVO
Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (art. 1, comma 1, lett. a) del D.P.R. n. 445/2000);
DOCUMENTO ANALOGICO
Documento formato utilizzato una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art. 1, comma 1, lett. b) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
DOCUMENTO ANALOGICO ORIGINALE
Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1 della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
DOCUMENTO ARCHIVIATO
Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (art. 1, comma 1, lett. h) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
DOCUMENTO CONSERVATO
Documento sottoposto al processo di conservazione;
DOCUMENTO DI RICONOSCIMENTO

Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consentano l'identificazione personale del titolare (art. 1, comma 1, lett. c) del D.P.R. n. 445/2000);

DOCUMENTO D'IDENTITA'

La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare (art. 1, comma 1, lett. d) del D.P.R. n. 445/2000);

DOCUMENTO D'IDENTITA' ELETTRONICO

Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno d'età (art. 1, comma 1, lett. e) del D.P.R. n. 445/2000);

ESIBIZIONE

Operazione che consente di visualizzare un documento conservato e di ottenerne copia (art. 1, comma 1, lett. n) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

EVIDENZA INFORMATICA

Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1, comma 1, lett. f) del D.P.C.M. 13 gennaio 2004);

FASCICOLAZIONE

L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;

FASCICOLO

Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se non è infrequente la creazione di fascicoli formati da insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc);

FIRMA DIGITALE

Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, comma 1, lett. s) del D. Lgs. n. 82/2005);

FIRMA ELETTRONICA

L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lett. q) del D. Lgs. n. 82/2005);

FIRMA ELETTRONICA QUALIFICATA

La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1, comma 1, lett. r) del D. Lgs. n. 82/2005);

FORMAZIONE DEI DOCUMENTI INFORMATICI

Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa (art. 1 della Deliberazione AIPA del 23 novembre 2000, n. 51);

FUNZIONE DI HASH

Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit) una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una

sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (art. 1, comma 1, lett. e) del D.P.C.M. 13 gennaio 2004);

GARANTE (della Privacy)

L'autorità di cui all'articolo 153 del D. Lgs. 30 giugno 2003, n. 196, istituita dalla legge 31 dicembre 1996, n. 675 (art. 4, comma 1, lett. q) del D. Lgs. n. 196/2003);

GESTIONE INFORMATICADEI DOCUMENTI

L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1, comma 1, lett. l) del D. Lgs. n. 82/2005);

INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;

INSERTO

E' un sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;

LEGALIZZAZIONE DI FIRMA

L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (art. 1, comma 1, lett. l) del D.P.R. n. 445/2000); 32

LEGALIZZAZIONE DI FOTOGRAFIA

L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato (art. 1, comma 1, lett. n) del D.P.R. n.445/2000);

MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE

Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizione e sottoripartizioni del titolario e indica quali documenti debbano essere conservati permanentemente (e quindi versati dopo quaranta anni nella sezione storica dell'archivio) e quali, invece, possono essere destinati al macero dopo cinque, dieci, quindici, venti anni, ecc. o secondo le esigenze dell'Amministrazione. Ne consegue il Piano di Conservazione periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;

MEMORIZZAZIONE

Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del D.P.R. n. 445/2000 così come modificato dall'articolo 6 del D. Lgs. 23 gennaio 2002, n. 10 (art. 1 comma 1, lett. f) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

MISURE MINIME DI SICUREZZA

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del D. Lgs. 30 giugno 2003, n. 196 (art. 4, comma 3, lett. a) del D. Lgs. n. 196/2003);

PAROLA CHIAVE Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri e altri dati in forma elettronica (art. 4, comma 3, lett. e) del D. Lgs. n. 196/2003);

ORIGINALI NON UNICI I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1, comma 1, lett. v) del D. Lgs. n. 82/2005);

PROFILO DI AUTORIZZAZIONE

L'insieme delle informazioni, univocamente associate ad una persona che consente di individuare a quali dati essa può accedere, nonché i trattamenti ed essa consentiti (art. 4, comma 3, lett. f) del D. Lgs. n. 196/2003);

PUBBLICO UFFICIALE

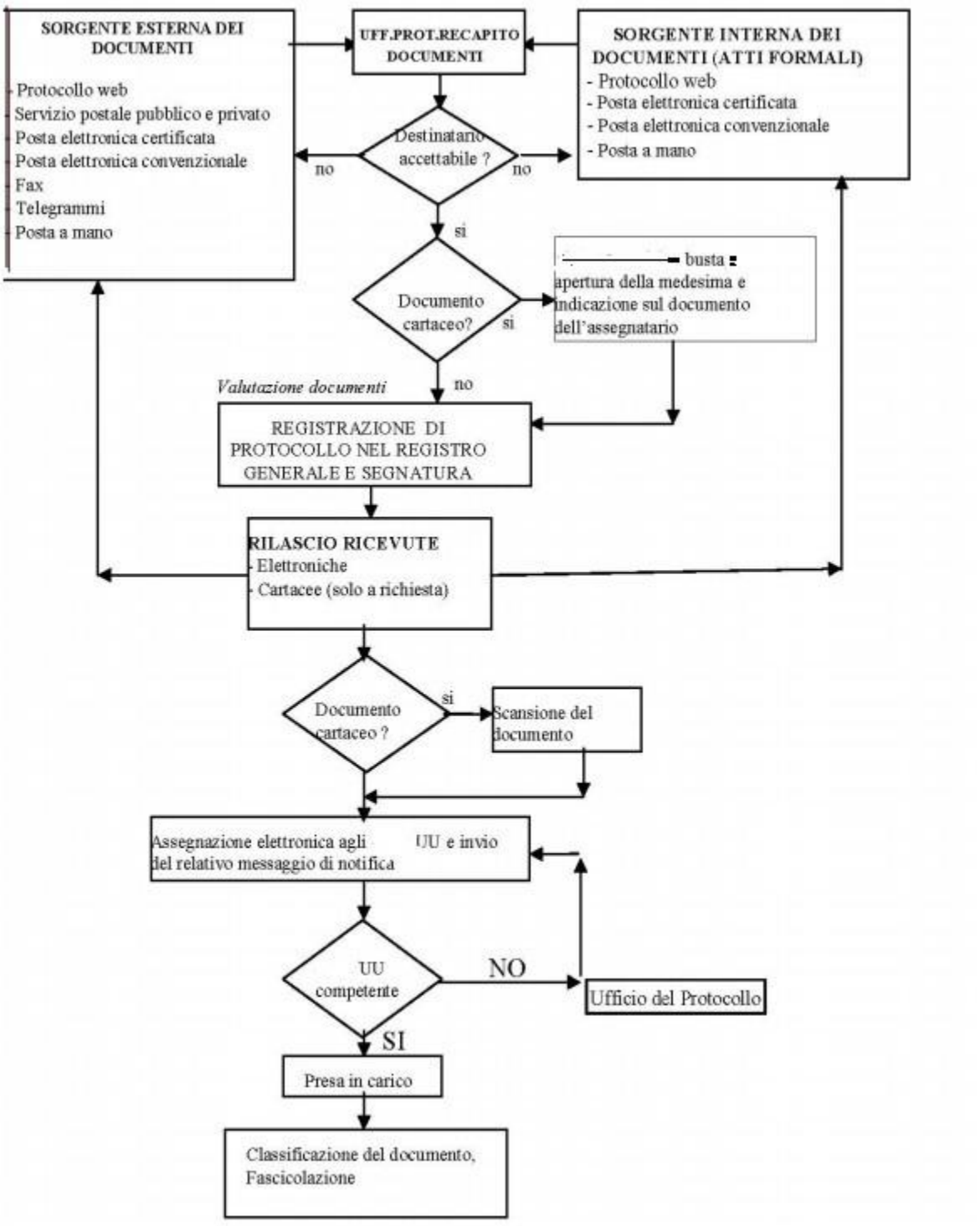
Il notaio, salvo quanto previsto dall'art. 5 , comma 4, della presente deliberazione e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del D.P.R. n. 445/2000 (art. 1, lett. q) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

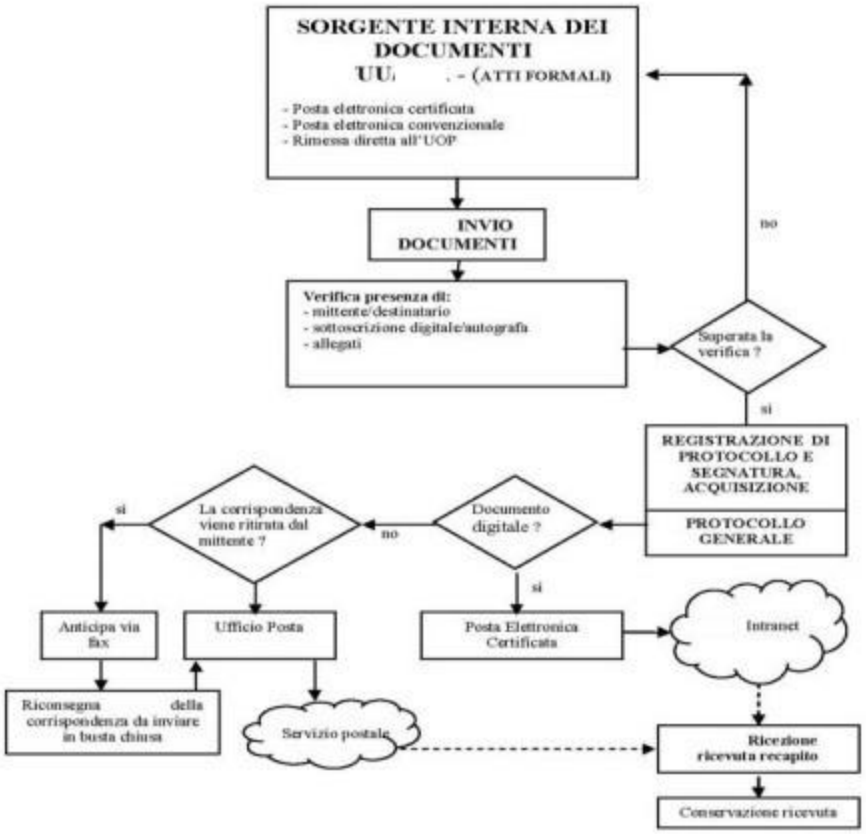
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, comma 1, lett. g) del D. Lgs. n. 196/2003);
RIFERIMENTO TEMPORALE
Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, comma 1, lett. g) del D.P.C.M. 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (art. 1, comma 1, lett. i) del D.P.R. n. 68/2005);
RIVERSAMENTO DIRETTO
Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (art. 1. comma 1, lett. n) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
RIVERSAMENTO SOSTITUTIVO
Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (art. 1, comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
SEGNATURA INFORMATICA
L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML, ed incluse in un messaggio protocollato, come previsto dall'art. 18, comma 1 del D.P.C.M. 31 ottobre 2000 (art. 1 dell'allegato A della Circolare AIPA del 7 maggio 2001, n. 28);
SEGNATURA DI PROTOCOLLO
L'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (Glossario dell'IPA – Indice delle Pubbliche Amministrazioni);
SISTEMA DI CLASSIFICAZIONE
Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (art. 2, comma 1, lett. h) del D.P.C.M. 31 ottobre 2000);
SISTEMA DI AUTORIZZAZIONE
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art. 4, comma 3, lett. g) del D. Lgs. n. 196/2003);
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI
L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1, comma 1, lett. r) del D.P.R. n. 445/2000).

ALLEGATO "B"

Descrizione funzionale ed operativa del sistema di protocollo informatico

FLUSSO IN INGRESSO




SORGENTE INTERNA DEI DOCUMENTI
UU. . - (ATTI FORMALI)
- Posta elettronica certificata
- Posta elettronica convenzionale
- Rimessa diretta all'UOP
INVIO DOCUMENTI
Verifica presenza di:
- mittente/destinatario
- sottoscrizione digitale/autografa
- allegati
Superata la verifica ?
no
si
REGISTRAZIONE DI PROTOCOLLO E SEGNATURA, ACQUISIZIONE
PROTOCOLLO GENERALE
Documento digitale ?
no
si
La corrispondenza viene ritirata dal mittente ?
si
Anticipa via fax
Ufficio Posta
Posta Elettronica Certificata
Intranet
Riconsegna della corrispondenza da inviare in busta chiusa
Servizio postale
Ricezione ricevuta recapito
Conservazione ricevuta

FLUSSO IN USCITA