



COMUNE DI CARPEGNA

PROVINCIA DI PESARO E URBINO

MANUALE DI GESTIONE E CONSERVAZIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO

Conforme alle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici pubblicate il 10 settembre 2020 ai sensi dell'art. 71 del CAD e modificate il 18/05/2021 con determinazione n. 371/2021

Approvato con delibera di Giunta Comunale n.51 del 30/06/2025

PARTE PRIMA – DISPOSIZIONI PRELIMINARI.....	4
1. Riferimenti normativi	4
2. Finalità, contenuti e metodologia del documento.....	4
PARTE SECONDA – ORGANIZZAZIONE.....	5
3. Area organizzativa omogenea e Unità Organizzative Responsabili (UOR).....	5
4. Il Responsabile della gestione documentale.....	5
5. La governance della gestione documentale.....	6
6. Livelli di accesso al sistema di protocollo.....	6
PARTE TERZA – FORMAZIONE DEI DOCUMENTI.....	6
Modalità di formazione.....	6
7. Modalità di formazione dei documenti informatici.....	6
7.1 Creazione e redazione tramite software di documenti informatici.....	6
7.2 Acquisizione di documenti informatici.....	7
7.3 Copie per immagine su supporto informatico di documenti analogici.....	7
7.4 Duplicati, copie ed estratti informatici di documenti informatici.....	8
7.5 Acquisizione di istanze tramite moduli online.....	9
Disposizioni comuni a tutte le modalità di formazione.....	9
8. Dispositivi di firma elettronica.....	9
9. Identificazione univoca del documento informatico.....	9
10. Associazione degli allegati al documento principale.....	9
11. Metadati del documento informatico.....	10
12. Immodificabilità e integrità del documento informatico.....	10
PARTE QUARTA - GESTIONE DOCUMENTALE.....	10
Flussi documentali esterni.....	10
13. Ricezione telematica di documenti informatici in entrata.....	10
14. Canali di ricezione.....	11
15. Valutazione di interoperabilità.....	11
16. Trasmissione telematica di documenti informatici in uscita.....	11
17. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni.....	12
18. Disposizioni sui documenti analogici.....	12
Protocollo informatico.....	12
19. Sistema di protocollo informatico.....	12
20.1 Descrizione del software di protocollo.....	12
20. Requisiti minimi di sicurezza dei sistemi di protocollo informatico.....	13
21. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico.....	13
22. Registro generale di protocollo.....	13
23. Documenti soggetti a registrazione di protocollo e documenti esclusi.....	14
24. Registrazione di protocollo.....	15
25. Annullamento e modifiche della registrazione di protocollo.....	15
26. Segnatura di protocollo.....	16
27. Documenti soggetti a registrazione particolare.....	16
28. Registro di emergenza.....	17
29. Disposizioni sulla protocollazione di documenti analogici.....	17
Classificazione e fascicolazione.....	18
30. Classificazione dei documenti.....	18
31. Fascicolazione informatica dei documenti.....	19
32. Repertorio dei fascicoli.....	19
33. Aggregazioni documentali.....	20
Flussi documentali interni.....	20
34. Assegnazione dei documenti in entrata agli uffici.....	20
35. Comunicazioni interne.....	21
36. Pubblicazioni nell'Albo pretorio.....	21
PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI.....	21
37. Piano di conservazione dell'archivio.....	21

38. Responsabile della conservazione	22
39. Oggetti e formati della conservazione	22
40. Archiviazione e conservazione digitale dei documenti informatici	23
41. Selezione e scarto archivistico	23
42. Misure di sicurezza e monitoraggio	24
PARTE SESTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI	24
43. Piano di sicurezza informatica	24
44. Credenziali di accesso al sistema documentale	24
45. Trattamento dei dati personali	25
46. Piano formativo del personale	25
PARTE SETTIMA - NORME TRANSITORIE E FINALI	25
47. Modalità di approvazione e aggiornamento del manuale	25
48. Pubblicità del manuale	26
49. Entrata in vigore	26
ELENCO ALLEGATI AL MANUALE DI GESTIONE	27

1. Riferimenti normativi

Il presente Manuale di gestione documentale è adottato ai sensi delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici (d'ora in avanti "Linee guida"), emanate dall'Agenzia per l'Italia Digitale con determinazione del Direttore generale del 9 settembre 2020, n. 407 e pubblicate il 10 settembre 2020, come modificate dalla recente determinazione n. 371 del 17 maggio 2021.

Gli allegati alle Linee guida sono parte integrante delle stesse e contengono disposizioni relative a:

- a. Glossario dei termini e degli acronimi;
- b. Formati di file e riversamento;
- c. Certificazione di processo;
- d. Standard e specifiche tecniche;
- e. Metadati;
- f. Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

- le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito "CAD")
- le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 "Disposizioni legislative in materia di documentazione amministrativa" (di seguito "TUDA");
- le norme sul procedimento amministrativo di cui alla l. 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- le disposizioni sulla trasparenza di cui al d.lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento
- (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
- le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del
- 27 aprile 2016 "Regolamento generale sulla protezione dei dati" ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali";
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni.

2. Finalità, contenuti e metodologia del documento

Il Manuale della gestione documentale descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale, il Manuale è reso noto anche esternamente all'ente. In quest'ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

3. Area organizzativa omogenea e Unità Organizzative Responsabili (UOR)

Il Comune di Carpegna si configura come un'unica Area Organizzativa Omogenea ("AOO") denominata "Area Omogenea Unica". L'AOO e gli indirizzi di posta elettronica a essa associati sono indicati nell'Indice PA (codice IPA del Comune di Carpegna c_b816 – codice AOO AD31A1A).

4. Il Responsabile della gestione documentale

Il Comune di Carpegna, nell'ottica di gestire in modo integrato tutte le fasi del ciclo di vita dei documenti informatici, ha individuato un'unica figura responsabile, il "Responsabile della gestione documentale", dotata di competenze giuridiche, informatiche e archivistiche, a cui affidare le funzioni e i compiti del Responsabile per la gestione documentale e del Responsabile della conservazione.

Con riferimento all'unica AOO si prende atto che con Decreto del Sindaco n. 10 in data 17/10/2019 è stato individuato nel funzionario che riveste la qualifica di Responsabile E.Q. Area Amministrativa, il Responsabile della gestione documentale, che ha provveduto alla predisposizione del presente manuale, parimenti con il medesimo provvedimento è stato individuato il vicario nell'Istruttore Amministrativo che riveste la qualifica di Responsabile del Servizio Protocollo, archivi e flusso documentale:

Responsabile della Conservazione, del protocollo informatico, archivio e flussi documentali (nominativo in IPA):

Dott.ssa Sara Corbellotti - Responsabile E.Q. dell'Area Amministrativa
sostituto Istruttore Responsabile Amministrativo Corbellotti Giuseppina.

Responsabile del Servizio Protocollo informatico, archivio e flussi documentali:

Istruttore Amministrativo Corbellotti Giuseppina

Responsabile Transizione Digitale: Dott.ssa Maria Giulia Pratelli, Segretario Comunale, nominata con Decreto del Sindaco n.5 del 26/03/2025;

Protocollista/addetto alla registrazione del protocollo informatico in ingresso: Operatore esperto Corbellotti Erica.

I compiti del Responsabile della gestione documentale (di seguito "Responsabile") sono definiti nell'atto di nomina. In particolare, il Responsabile:

- è preposto, ai sensi dell'art. 61 TUDA, al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi della AOO unica del Comune;
- provvede, d'intesa con il Responsabile per la Transizione Digitale (RTD), previo parere del Responsabile per la Protezione dei Dati personali (RPD), alla predisposizione e al costante aggiornamento del presente Manuale e dei relativi allegati;
- monitora i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
- valuta e formula proposte di riprogettazione e reingegnerizzazione dei processi di cui alla lettera precedente;
- vigila sul rispetto delle norme e delle procedure durante le operazioni di registrazione di protocollo, di segnatura di protocollo, di produzione e conservazione del registro giornaliero di protocollo;
- assicura l'accesso al sistema di gestione documentale, provvedendo alla definizione delle abilitazioni di accesso, e vigila sul rispetto delle misure di sicurezza e di protezione dei dati;
- effettua un periodico censimento degli strumenti software di gestione documentale in uso presso il Comune e, di concerto con il RTD, ne verifica la conformità alla normativa vigente.

5. La governance della gestione documentale

Il responsabile della gestione documentale è preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi e, d'intesa con il responsabile per la transizione digitale (RTD) e acquisito il parere del responsabile della protezione dei dati personali (DPO), predispone il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione.

6. Livelli di accesso al sistema di protocollo

Ciascun utente che abbia accesso al Sistema di protocollo è identificato da un 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.

Di norma tutti gli utenti hanno un profilo standard di abilitazione alle funzioni di inserimento in partenza o interni, aggiornamento e consultazione di protocolli esclusivamente attinenti alla propria area di appartenenza.

Solo gli addetti al Servizio hanno una profilatura che permetta la registrazione, modifica ed accesso a tutte le registrazioni di protocollo e fascicolazioni, al fine di garantire un servizio di assistenza generale a tutti gli altri utenti.

Nei casi in cui sia necessario estendere l'abilitazione del profilo per particolari esigenze di servizio, il Responsabile dell'Area di appartenenza ne deve fare espressa e motivata richiesta al Responsabile della Gestione Documentale, che autorizzerà la modifica del Profilo. La profilatura degli accessi è costantemente monitorata dal Responsabile della Gestione Documentale.

I livelli di abilitazione con i compiti sono riportati nell'allegato 4 al presente Manuale.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Modalità di formazione

7. Modalità di formazione dei documenti informatici

Tutti i documenti sono formati in originale come documenti informatici mediante una delle seguenti modalità:

- a) creazione e redazione tramite l'utilizzo di strumenti di software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2 delle Linee Guida;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Di seguito sono fornite indicazioni specifiche per ciascuna delle modalità sopradescritte

7.1 Creazione e redazione tramite software di documenti informatici

Gli uffici del Comune dispongono dei seguenti strumenti software per la creazione dei documenti informatici mediante redazione:

- programmi della suite *Microsoft Office: Word, Excel, Access, PowerPoint, ecc.*;
- programmi della suite *Libre Office*;
- gestionale Ditta Datagraph S.r.l. di Modena per redazione atti organi collegiali e provvedimenti (decreti, ordinanze, determine...)

Ogni documento amministrativo informatico creato e redatto dal Comune deve recare obbligatoriamente i seguenti elementi:

1. denominazione dell'Amministrazione;
2. autore e ufficio responsabile;
3. numero e data di protocollo o di registrazione (se soggetto a registrazione particolare);
4. oggetto del documento;
5. riferimenti a procedimento o fascicolo;
6. sottoscrizione;
7. data e luogo;
8. indicazione degli allegati (se presenti);
9. identificazione e dati dei destinatari (se si tratta di documento in uscita);
10. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
11. mezzo di spedizione (se documento in uscita).

Scelta del formato e modalità di sottoscrizione

Il formato del documento informatico deve essere individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID.

I documenti informatici prodotti dall'Ente indipendentemente dal software utilizzato e prima della loro eventuale sottoscrizione con firma digitale, sono convertiti in formato PDF/A, standard previsto dalla normativa vigente, al fine di garantire l'inalterabilità durante le fasi di accesso, di archiviazione e di conservazione. I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES. Nel caso il documento definitivo assuma un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (*un file PDF firmato digitalmente in formato p7m è un documento PDF che è stato firmato elettronicamente utilizzando la firma digitale, e il risultato è un file con estensione p7m. Questo formato, noto come CADES, non altera il documento originale ma lo incapsula in una "busta" digitale, insieme alla firma digitale e al certificato del firmatario*).

7.2 Acquisizione di documenti informatici

La formazione di documenti informatici per acquisizione può avvenire secondo una delle seguenti modalità:

- a) acquisizione di un documento informatico per via telematica o su supporto informatico;
- b) acquisizione della copia per immagine su supporto informatico di un documento analogico;
- c) acquisizione della copia informatica di un documento analogico.

In caso di acquisizione di copia informatica del documento originale (analogico o informatico), al fine di assicurarne l'efficacia giuridico-probatoria, occorre attestare la conformità della copia all'originale da cui è estratta (con le modalità indicate nelle disposizioni successive).

In caso di acquisizione di un duplicato informatico, ai sensi dell'art. 23-bis del CAD, esso ha la stessa efficacia giuridico-probatoria del documento informatico originale; pertanto, non è richiesta l'attestazione di conformità.

7.3 Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di

processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 delle Linee Guida "Certificazione di Processo".

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

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

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD.

7.4 Duplicati, copie ed estratti informatici di documenti informatici

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

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".docx" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 delle Linee Guida "Certificazione di Processo".

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

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

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

un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

7.5 Acquisizione di istanze tramite moduli online

Le istanze provenienti dagli utenti possono essere formate anche tramite la compilazione di moduli e *form* messi a disposizione sul sito web del Comune e resi accessibili previa identificazione dell'utente con gli strumenti di identificazione SPID, CIE, CNS. I dati immessi dal richiedente sono acquisiti e memorizzati su supporto informatico. Le istanze così formate sono acquisite dal Sistema di protocollo informatico del Comune e costituiscono a tutti gli effetti documenti amministrativi informatici e sono trattati come documenti in entrata soggetti a registrazione di protocollo.

Disposizioni comuni a tutte le modalità di formazione

8. Dispositivi di firma elettronica

Il Comune garantisce che tutti i dipendenti e i titolari di cariche che firmano documenti a valenza esterna siano dotati di dispositivi di firma elettronica. A tal fine il Comune è dotato di sistemi di gestione documentale che consentono, ai dipendenti in possesso di profilo utente, l'apposizione della firma digitale.

L'utilizzo del dispositivo di firma è strettamente personale e riconducibile al suo titolare. Pertanto, il dispositivo non deve essere ceduto, né devono essere diffuse le chiavi dei certificati.

Ogni titolare di dispositivo di firma verifica periodicamente la validità e la data di scadenza del certificato di firma, al fine di provvedere tempestivamente al rinnovo.

Quando la firma è apposta utilizzando un certificato prossimo alla scadenza, il titolare ne dà avviso al Responsabile, affinché provveda a costituire un riferimento temporale giuridicamente valido tale da attestare che la firma sia stata apposta in un momento in cui il certificato era valido. In particolare, costituiscono riferimento temporale giuridicamente valido le seguenti attività sul documento firmato:

- apposizione di marca temporale;
- apposizione della segnatura di protocollo;
- versamento in conservazione.

Documenti, dati e altre informazioni trasmesse in cooperazione applicativa non richiedono la sottoscrizione digitale o l'apposizione della marca temporale.

9. Identificazione univoca del documento informatico

Ogni documento informatico deve essere identificato in modo univoco e persistente.

L'identificazione univoca dei documenti è effettuata con l'associazione al documento dell'impronta crittografica *hash*. Per i documenti soggetti a registrazione di protocollo, l'associazione è effettuata tramite le apposite funzioni del Sistema di protocollo informatico del Comune. Per i documenti non protocollati, l'associazione è effettuata tramite le apposite funzioni degli strumenti software in uso per la formazione degli atti. In ogni caso l'impronta crittografica deve essere basata su una funzione di hash conforme alle tipologie di algoritmi previste nell'allegato 6 alle Linee guida.

10. Associazione degli allegati al documento principale

Gli allegati sono congiunti in modo univoco al documento informatico principale tramite l'associazione delle impronte hash dei documenti allegati al documento principale.

Al documento principale, inoltre, devono essere associati i seguenti metadati:

- numero allegati;
- indice allegati;

- identificativo del documento allegato (IdDoc);
- titolo dell'allegato (Descrizione).

A ciascun allegato, invece, deve essere associato il metadato identificativo del documento principale (IdDoc).

Le operazioni di associazione degli allegati, quando possibile, sono effettuate in modo automatizzato dal sistema di gestione documentale adoperato per la formazione del documento principale.

In alternativa, è possibile associare gli allegati al documento principale manualmente, riportando in calce al documento stesso l'elenco degli allegati, indicando per ciascuno l'oggetto e la relativa impronta hash. L'associazione sarà assicurata una volta che il documento informatico principale sia divenuto imm modificabile.

11. Metadati del documento informatico

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa. In merito, l'articolo 53, comma 1, del TUDA indica le informazioni che caratterizzano il registro di protocollo, a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.

I metadati devono essere associati prima che il documento informatico acquisisca le caratteristiche di imm modificabilità e integrità, dunque prima della memorizzazione nel sistema o del versamento in conservazione.

12. Immodificabilità e integrità del documento informatico

Affinché sia garantito il valore giuridico-probatorio del documento informatico, ne deve essere assicurata l'immodificabilità e l'integrità.

Il documento informatico è imm modificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nelle fasi di accesso, gestione e conservazione.

L'immodificabilità e l'integrità dei documenti informatici dell'ente sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

PARTE QUARTA - GESTIONE DOCUMENTALE

Flussi documentali esterni

13. Ricezione telematica di documenti informatici in entrata

I documenti informatici in entrata, pervenuti tramite i canali di ricezione previsti, sono oggetto di registrazione di protocollo secondo quanto previsto nella sezione successiva. Una volta che ne sia accertata la provenienza, i documenti sono validi ai fini del procedimento amministrativo.

Le istanze, le dichiarazioni e le comunicazioni trasmesse per via telematica, in ogni caso, devono ritenersi valide a tutti gli effetti di legge quando:

- a) sono contenute in documenti sottoscritti con firma digitale o firma elettronica qualificata;
- b) sono trasmesse a mezzo posta elettronica certificata da un indirizzo PEC iscritto in uno degli elenchi di domicili digitali previsti dalla normativa vigente;
- c) sono trasmesse attraverso un sistema informatico che consente la previa identificazione dell'utente con i sistemi SPID, CIE, CNS, eIDAS;
- d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma 4-quinquies del CAD ed è possibile accertare la provenienza della trasmissione. Tale modalità di trasmissione costituisce elezione di domicilio digitale speciale per quel singolo procedimento o affare;
- e) sono contenute in copie digitali di documenti originali cartacei sottoscritti e presentati unitamente a copia del documento d'identità dell'autore;
- f) è comunque possibile accertarne la provenienza secondo la normativa vigente o, comunque, in base a criteri di attendibilità e riconducibilità al mittente dichiarato.

14. Canali di ricezione

La ricezione di comunicazioni e documenti informatici è assicurata tramite i seguenti canali:

- casella PEC;
- acquisizione di istanze, redatte anche tramite form;
- acquisizione tramite servizio online, accessibile previa identificazione dell'utente, delle istanze e dei documenti informatici relativi alle pratiche degli sportelli attivati dall'Amministrazione (ad es. SUE);
- cooperazione applicativa tra pubbliche amministrazioni;
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti. Gli indirizzi di posta elettronica certificata devono essere riportati nell'Indice delle Pubbliche Amministrazioni e pubblicizzati sul sito web istituzionale.

Nel caso in cui un soggetto tenuto a effettuare comunicazioni esclusivamente in via telematica (imprese, professionisti, altre PP.AA., salvi i casi di cui all'art. 2, comma 6, CAD) faccia pervenire agli uffici del Comune comunicazioni e documenti in modalità analogica, questi non saranno ritenuti validamente trasmessi. In tali casi, la circostanza è segnalata in nota alla registrazione di protocollo. Il responsabile dell'UO assegnataria della comunicazione, o comunque il soggetto individuato quale responsabile del procedimento, ai sensi dell'art. 5, comma 3, l. n. 241/1990, provvede a comunicare al mittente il motivo della mancata accettazione dei documenti e a indicare modalità di trasmissione valide. La comunicazione, quando possibile, è trasmessa al domicilio digitale del mittente estratto dagli indici di cui agli articoli 6-bis e 6-ter del CAD.

15. Valutazione di interoperabilità

Sono accettati, e conseguentemente registrati al protocollo, documenti informatici esclusivamente nei formati previsti dall'allegato 2 alle Linee guida "Formati di file e riversamento".

A seguito della valutazione di interoperabilità effettuata dalla Regione Marche, Conservatore accreditato per l'Ente, che nel manuale di conservazione ha indicato elenco dei formati ricevibili (All. 6), il responsabile della gestione documentale valuta l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 delle Linee guida.

16. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso di trasmissione a soggetti privati privi di domicilio digitale ai sensi degli artt. 6 e ss. del CAD.

Per la trasmissione telematica di documenti a imprese e professionisti tenuti obbligatoriamente all'iscrizione in albi o elenchi, il domicilio digitale è estratto dall'indice INI-PEC (www.inipec.gov.it).

I documenti informatici in uscita sono trasmessi a mezzo PEC solo dopo essere stati classificati, fascicolati e protocollati secondo le disposizioni del presente Manuale.

La trasmissione di dati e altre informazioni in cooperazione applicativa è soggetta a protocollazione o a registrazione particolare secondo le medesime regole per la registrazione di protocollo dei documenti.

17. Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni

La trasmissione di comunicazioni e documenti verso altre pubbliche amministrazioni avviene sempre per via telematica, agli indirizzi di posta elettronica, anche ordinaria, dei singoli uffici. Gli indirizzi di spedizione sono rilevati tramite la consultazione dell'Indice delle Pubbliche Amministrazioni (www.indicepa.gov.it) di cui all'art. 6-ter del CAD o su indicazione dell'Amministrazione interessata..

I documenti che devono essere prodotti entro un determinato termine sono sempre trasmessi a mezzo PEC.

18. Disposizioni sui documenti analogici

I documenti su supporto analogico possono pervenire al Comune attraverso:

- il servizio postale;
- la consegna diretta agli uffici agli addetti alle attività di sportello;
- il fax, nei soli casi di esclusione dell'applicazione della normativa previsti dall'art. 2, comma 6, D.lgs. n. 82/2005.

Gli orari definiti per la presentazione della documentazione analogica sono quelli di apertura al pubblico e indicati sul sito web istituzionale del Comune.

Protocollo informatico

19. Sistema di protocollo informatico

Il modello organizzativo adottato è di tipo centralizzato con protocollazione in entrata effettuata dall'ufficio protocollo e protocollazione in uscita decentrata e prevede che tutte le strutture e il personale abilitato abbiano accesso al sistema di gestione informatica dei soli documenti di propria competenza.

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei documenti, l'identificazione degli uffici utenti e del personale abilitati allo svolgimento delle operazioni di registrazione di protocollo, l'organizzazione ed archiviazione dei documenti dell'AOO, sono individuate dal Responsabile del servizio di protocollo informatico che tiene conto delle richieste e delle esigenze dei responsabili delle UOR.

20.1 Descrizione del software di protocollo

La strategia Cloud della Pubblica Amministrazione italiana prevede la migrazione verso il cloud di dati e servizi digitali delle PA, con l'obiettivo di migliorare l'efficienza, la sicurezza e l'innovazione. Questo processo è regolato da diverse normative e documenti, tra cui il Piano Triennale per l'Informatica nella Pubblica Amministrazione, la Strategia Cloud Italia e il nuovo Regolamento Cloud per la PA.

L'Ente utilizza il gestionale di protocollo e flusso documentale della softwarehouse DATAGRAPH S.r.l. di Modena, Sistema di protocollo informatico conforme al D.P.R. 28 dicembre 2000, n. 445 "Disposizioni legislative in materia di documentazione amministrativa" e successive integrazioni del CAD - versione 8.5.6 - reso disponibile in cloud modalità SaaS (*SaaS*, acronimo di *Software as a*

Service, è un modello di distribuzione del software in cui il software e i dati relativi vengono ospitati su server remoti, appunto in cloud, e resi disponibili agli utenti tramite internet). Il sistema consente la completa gestione cartacea e digitale dei documenti dell'amministrazione, permette l'emissione di protocolli, l'identificazione di documenti interni, dematerializzazione cartacea, classificazione, firma digitale, tracciatura dei flussi documentali e gestione dei dati di archiviazione e scarto. Tiene traccia con evidenza degli eventuali annullamenti di protocollo e delle modifiche. Il sistema di flusso documentale permette anche l'invio automatico in conservazione del registro giornaliero di protocollo (giornaliera) e dei documenti informatici in arrivo e in partenza (settimanale) al sistema di conservazione regionale DigiP al quale il Comune di Carpegna ha aderito (vedi All.3 Manuale di Conservazione).

20. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID di cui al paragrafo 3.9 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

- a) l'univoca identificazione ed autenticazione degli utenti;
- b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
- c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

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

21. Funzioni del Responsabile della Gestione Documentale in materia di protocollo informatico

La corretta tenuta del protocollo informatico è garantita dal Responsabile della gestione documentale. In particolare, il Responsabile, nella veste di responsabile del protocollo informatico:

- a) coordina la gestione del Sistema di protocollo informatico;
- b) assegna al personale addetto alla protocollazione l'abilitazione all'utilizzo delle funzioni di protocollo del Sistema;
- c) esercita il controllo generale sui flussi documentali esterni e interni;
- d) assicura la corretta esecuzione delle attività di protocollazione;
- e) autorizza l'attivazione del protocollo di emergenza;
- f) autorizza con comunicazione formale le operazioni di annullamento delle registrazioni di protocollo;
- g) vigila sull'osservanza della normativa e delle disposizioni del presente Manuale da parte del personale addetto.

Le attività di protocollazione sono eseguite dagli utenti delegati dal Responsabile.

22. Registro generale di protocollo

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

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

Nell'ambito della AOO il Registro generale di protocollo è unico, al pari della numerazione progressiva delle registrazioni di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche. La numerazione è progressiva, si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo è associato in modo univoco e immodificabile al documento; pertanto, esso individua un unico documento e, di conseguenza, ogni documento reca un solo numero di

protocollo, anche se i documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione “a fronte”, cioè l’utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata sul protocollo viene considerata giuridicamente inesistente presso l’amministrazione. Non è consentita la protocollazione di un documento già protocollato. Qualora ciò avvenisse per errore, la seconda protocollazione va annullata.

Il Registro giornaliero di protocollo è costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Esso è prodotto automaticamente dal Sistema di protocollo informatico, che provvede altresì al versamento automatico al Sistema di conservazione.

23. Documenti soggetti a registrazione di protocollo e documenti esclusi

Tutti i documenti prodotti e ricevuti dall’Ente, indipendentemente dal supporto sul quale sono formati, sono registrati al protocollo, ad eccezione di quelli indicati dall’articolo 53 comma 5 del TUDA che sono esclusi dalla registrazione di protocollo:

- note di ricezione delle circolari e altre disposizioni;
- materiale statistico;
- atti preparatori interni;
- giornali, riviste, materiale pubblicitario, stampe varie, plichi di libri;
- biglietti augurali, inviti a manifestazioni e documenti di occasione vari che non attivino procedimenti amministrativi;
- bolle accompagnatorie;
- richiesta/invio comunicazioni informali.
- pubblicità conoscitiva di convegni;
- pubblicità in generale;
- offerte, i listini prezzi e i preventivi di terzi non richiesti;
- ricevute di ritorno delle raccomandate A.R.;
- tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico amministrativa presente o futura.

Le ricevute di accettazione e di consegna di un messaggio inviato tramite PEC non devono essere protocollate, ma devono essere associate alla registrazione di protocollo del documento trasmesso/ricevuto a cui la ricevuta stessa si riferisce: all’associazione provvede il software di protocollo.

Sono altresì esclusi dalla registrazione di protocollo i documenti già soggetti a registrazione mediante registri particolari dell’Amministrazione come ad esempio:

- Registro delle proposte di Deliberazioni di Giunta e di Consiglio Comunale;
- Registro delle delibere della Giunta Comunale;
- Registro delle delibere del Consiglio Comunale;
- Registro delle determinazioni;
- Registro degli impegni, liquidazioni, mandati di pagamento e reversali di incasso

Si specifica che i documenti soggetti a registrazione particolare possono essere esclusi dalla registrazione a Protocollo, a condizione che venga garantita univoca identificazione oltre che il requisito di immodificabilità e un riferimento temporale certo, mediante repertori tenuti con le stesse modalità di sicurezza del protocollo informatico.

Sono parimenti esclusi dalla registrazione a protocollo in quanto atti interni e già gestiti da applicazioni informatiche con registrazione:

- richieste permessi e congedi del personale dipendente
- richieste di rimborso spese e missioni.

24. Registrazione di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare in forma non modificabile al fine di garantirne l'identificazione univoca e certa. Ai sensi dell'art. 53, comma 1, TUDA, metadati di registrazione di protocollo obbligatori sono:

- a) numero di protocollo del documento, generato automaticamente dal sistema;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema;
- c) il mittente, per i documenti ricevuti, e il destinatario (o i destinatari), per i documenti spediti;
- d) oggetto del documento;
- e) data e protocollo del documento ricevuto, se disponibili;
- f) l'impronta del documento informatico;
- g) tipologia di documento;
- h) classificazione (titolo e classe) sulla base del Titolario e del Prontuario di Classificazione;
- i) fascicolo di appartenenza;
- j) assegnazione interna (per competenza o per conoscenza).

Ai suddetti metadati registrati in forma non modificabile (dalla lettera "a" alla lettera "f"), inoltre, possono essere aggiunti (a seconda dei casi) i seguenti ulteriori metadati:

- a) data e ora di arrivo;
- b) allegati;
- c) livello di riservatezza;
- d) mezzo di ricezione o invio;
- e) annotazioni;
- f) (eventualmente) estremi del provvedimento di differimento della registrazione;
- g) (se necessario) elementi identificativi del procedimento amministrativo.

25. Annullamento e modifiche della registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo non può essere modificata né integrata, né cancellata, ma soltanto annullata attraverso l'apposita procedura conforme all'art. 54 del TUDA. In particolare, i metadati non sono modificabili, ma eventualmente annullabili.

Ogni annullamento della registrazione deve:

- essere autorizzato con comunicazione formale del Responsabile;
- comportare la memorizzazione di data, ora e estremi della comunicazione formale di annullamento;
- consentire sempre la memorizzazione e la visibilità delle informazioni oggetto di annullamento.

Le richieste di annullamento rivolte al Responsabile devono essere motivate. Le richieste sono accolte, di norma, in casi di mero errore materiale (quali ad esempio la doppia registrazione, la registrazione di documenti che non diano seguito a procedimenti o ad attività amministrative proprie dell'ente, la registrazione errata che necessiterebbe di modifiche sostanziali dei campi obbligatori). Solo il Responsabile ha il potere di autorizzare l'annullamento delle registrazioni di protocollo, ovvero di dare disposizioni in tal senso. Il Responsabile può delegare il personale addetto al Servizio di Protocollo ad autorizzare le operazioni di annullamento, che deve risultare in modo esplicito nel provvedimento di delega.

Come previsto dal par. 3.1.5. delle Linee Guida AgID, le uniche informazioni modificabili di una registrazione di protocollo sono quelle relative a:

- classificazione (titolo e classe);
- assegnazione interna all'amministrazione (per competenza o per conoscenza).

Le operazioni di modifica possono essere svolte dal personale addetto alla protocollazione, previa autorizzazione del Responsabile.

L'annullamento e le modifiche avvengono in modo da consentire di mantenere traccia di ogni operazione, così come richiesto dalla normativa.

26. Segnatura di protocollo

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa, come indicate all'art. 53, comma 1, TUDA.

Le operazioni di segnatura sono effettuate contemporaneamente alla registrazione di protocollo o ad altra registrazione cui il documento è soggetto.

I requisiti necessari di ciascuna segnatura di protocollo sono:

- a) indicazione della Amministrazione mittente;
- b) codice identificativo dell'AOO mittente;
- c) codice identificativo del registro;
- d) numero progressivo di protocollo;
- e) data di registrazione;
- f) oggetto del messaggio di protocollo;
- g) classificazione del messaggio di protocollo;
- h) indicazione del fascicolo in cui è inserito il messaggio di protocollo.

Per i documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file XML conforme alle indicazioni previste dall'Allegato 6 alle Linee guida dell'AgID.

27. Documenti soggetti a registrazione particolare

Documenti con dati sensibili

I documenti contenenti dati sensibili e giudiziari (art. 4 del D. Lgs 196/2003) (es. certificati medici, permessi L. 104/92, provvedimenti disciplinari, relazioni relative ai minori, ecc.), sono soggetti a registrazione con la procedura informatica selezionando il campo "riservato" nel profilo del documento in modo tale da non permettere la visibilità del documento ai ruoli gerarchicamente superiori. Tale categoria di documenti non è soggetta obbligatoriamente ad acquisizione ottica.

Documentazione di gare d'appalto

La registrazione della documentazione riferita a gare telematiche, gestite tramite le piattaforme dei mercati elettronici della Pubblica Amministrazione, è effettuata, per completezza dei flussi documentali e secondo l'apprezzamento dei Responsabili dei procedimenti, registrando gli atti pubblicati ai fini di alimentare i relativi fascicoli presso il sistema documentale dell'Ente.

Documenti con mittente o autore non identificabile, posta personale

I documenti, analogici o digitali, ricevuti e indirizzati al personale dell'Ente e quelli di cui non sia identificabile l'autore sono regolarmente aperti ed eventualmente registrati al protocollo.

Non si registra la posta indirizzata nominalmente se sulla busta è indicata la dicitura "personale" o "riservata personale". Il destinatario di posta elettronica su indirizzo personale rilasciato dall'Ente potrà richiederne la registrazione inoltrando il messaggio al protocollo.

Documenti informatici con certificato di firma scaduto o revocato

Nel caso in cui l'Ente riceva documenti informatici firmati digitalmente il cui certificato di firma risulta scaduto o revocato prima della sottoscrizione, questi verranno protocollati e inoltrati al responsabile di procedimento che farà opportuna comunicazione al mittente.

Casi specifici riferiti a documenti analogici

- La normativa vigente prevede l'esclusione della corrispondenza via fax fra pubbliche amministrazioni. La trasmissione di documenti via fax con cittadini o altri soggetti privati non aventi l'obbligo di comunicazione in forma telematica con la pubblica amministrazione richiede la registrazione di protocollo.
- I documenti ricevuti via fax sono in ogni caso sottoposti alla registrazione di protocollo. Qualora questi anticipino documenti originali che perverranno successivamente, a questi ultimi sono attribuiti lo stesso numero e la stessa data di protocollo assegnati al fax cui si riferiscono e viene evidenziata la dicitura "già pervenuti via fax".
- I documenti anonimi e quelli pervenuti con mittente non riconoscibile sono soggetti alla registrazione di protocollo, alla classificazione e all'assegnazione ai responsabili di area i quali valuteranno la sussistenza delle motivazioni per una eventuale attivazione del procedimento amministrativo. Nel campo relativo al mittente sarà registrata la dicitura "Anonimo" o "Mittente non riconoscibile".
- Degli originali plurimi di documenti cartacei in entrata, ad esempio comunicazioni identiche indirizzate a più destinatari interni all'Ente, che pervengono in tempi successivi, viene protocollato solo il primo esemplare pervenuto che viene trasmesso trasformato in documento informatico a tutti i destinatari segnalati sul documento.

Trasmissioni telematiche e procedimenti gestiti in interoperabilità

I documenti, trasmessi/ricevuti dall'Ente, con immissione diretta dei dati nel sistema dell'Ente destinatario possono essere trasmessi senza firma digitale in quanto inviati tramite linee di comunicazione sicure, riservate e ad identificazione univoca attivati con i singoli destinatari. Gli invii telematici sostituiscono integralmente gli invii cartacei della medesima documentazione.

28. Registro di emergenza

Il responsabile del servizio di protocollo informatico autorizza lo svolgimento delle operazioni di registrazione di protocollo sull'apposito registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.

Il registro di emergenza è unico ed è gestito dall'Ufficio Protocollo. Tutti i servizi comunali, in caso di necessità, fanno quindi riferimento a questo ufficio per ottenere l'assegnazione di un numero di protocollo di emergenza, in entrata o in uscita.

Il registro di emergenza è fornito dalla softwarehouse Datagraph, è uno specifico programma da eseguire da una postazione. Non richiede che la rete funzioni né utilizza Database. Si inseriscono nel programma i dati minimi della registrazione. Una volta che il protocollo informatico è di nuovo disponibile sarà necessario procedere ad importare i dati dal registro di emergenza PRIMA di ricominciare con l'uso del registro di protocollo.

29. Disposizioni sulla protocollazione di documenti analogici

I documenti analogici in entrata sono soggetti alla scansione e alla trasformazione in documenti informatici, secondo il processo descritto nel successivo articolo, per tutte le necessità di trattamento amministrativo e per le attività di archiviazione e di conservazione.

Il documento informatico derivato dal processo di scansione è sottoposto alla registrazione di protocollo e alla relativa segnatura ed è assegnato agli uffici per le attività di competenza.

L'originale cartaceo, sul quale vengono apposti gli estremi della segnatura e della classificazione, è consegnato all'ufficio competente per la custodia dei documenti pervenuti.

Tali documenti saranno archiviati e conservati presso l'Ente fino all'assunzione di diverse determinazioni riferite alla gestione dei fascicoli informatici e dei relativi procedimenti amministrativi di selezione e di scarto da sottoporsi alla competente Soprintendenza archivistica.

Qualora per ragioni organizzative o tecniche non sia possibile protocollare immediatamente il documento, l'addetto al protocollo comunica al mittente o ad altra persona incaricata il termine entro il quale il documento verrà protocollato, impegnandosi – se richiesto – a far pervenire la

ricevuta all'indirizzo o recapito indicato dal mittente stesso (anche tramite e-mail). La ricevuta può essere altresì ritirata dall'interessato o da persona espressamente delegata nei giorni successivi.

L'Ente, per mezzo della scansione dei documenti, produce copie informatiche di documenti analogici secondo le prescrizioni fornite dalle Linee Guida e dal CAD.

Processo di scansione:

- Acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file in un formato standard abilitato alla conservazione.
- Verifica della correttezza dell'acquisizione delle immagini e della esatta corrispondenza delle immagini ottenute con gli originali cartacei.
- Collegamento delle immagini alla rispettiva registrazione di protocollo, in modo non modificabile.
- Memorizzazione delle immagini, in modo non modificabile.
- La scansione dei documenti cartacei viene eseguita integralmente se questi pervengono in formato A4 e A3.
- I documenti soggetti a scansione sono conservati e condivisi con gli uffici cui pervengono in assegnazione.

La conformità è garantita dal recepimento dell'art. 2.2 delle Linee Guida AGID:

“la copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia”.

Classificazione e fascicolazione

30. Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle competenze, alle funzioni e alle attività dell'Amministrazione. Lo strumento per classificare i documenti è il Titolario di Classificazione. Il piano di classificazione si suddivide in titoli e classi:

- Il titolo (o la voce di I livello) individua funzioni primarie e di organizzazione dell'ente (macro funzioni);
- la classe corrisponde a specifiche competenze che rientrano concettualmente nella macro funzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato.

Il Piano di classificazione o Titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'AOO in forza di leggi e regolamenti vigenti. Il Titolario adottato dal Comune di Carpegna è quello elaborato dal Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni "Piano di classificazione (=Titolario) per gli archivi dei Comuni italiani-seconda edizione, dicembre 2005" e riassunto nell'allegato 1. Il titolare non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione. Viene garantita la storicizzazione delle variazioni di titolare e la possibilità di ricostruire i diversi titoli e classi nel tempo mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolare vigente al momento della produzione degli stessi. Per ogni modifica di titolo e/o classe viene riportata la data di introduzione e la data di variazione. Di norma le variazioni vengono introdotte a partire dal 1° gennaio dell'anno successivo a quello di approvazione del nuovo titolare.

Tutti i documenti ricevuti, spediti e anche quelli scambiati internamente, fanno parte del sistema documentario dell'Ente, a prescindere dal supporto utilizzato, dalla modalità di registrazione (protocollazione o repertoriazione particolari) e pertanto sono soggetti a classificazione (Art.64 DPR 445/2000). Se necessario, uno stesso documento può essere classificato più volte in base alle diverse funzioni alle quali si riferisce, evitando comunque una produzione eccessiva di copie

documentarie.

Tutti i documenti ricevuti e prodotti dall'Ente, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.

31. Fascicolazione informatica dei documenti

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

I fascicoli sono informatici e sono costituiti con le regole espresse come sopra, contengono pertanto tutta la documentazione originale della pratica prodotta in formato elettronico e le copie per immagine dei documenti cartacei.

Il protocollista, in fase di protocollazione in arrivo, assegna il Titolo e la classe mentre i Responsabili dei singoli uffici interni dell'AOO, assegnatari del documento, creano i fascicoli e forniscono le indicazioni operative per la gestione dei fascicoli e assicurano che la costituzione dei fascicoli avvenga secondo modalità uniformi, sia per quanto riguarda i criteri da adottare per la denominazione della pratica al fine di identificare il fascicolo in modo univoco che di quelli adottati per la descrizione del fascicolo.

L'apertura di un nuovo fascicolo è effettuata da parte dell'assegnatario o da parte del Responsabile del procedimento. Per ogni documento in entrata, l'assegnatario stabilisce se esso si colloca nell'ambito di un procedimento in corso oppure se dà avvio ad un nuovo procedimento, in tal caso procede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso un'operazione automatica di apertura che prevede la registrazione nel sistema informatico, oltre ai metadati, delle seguenti informazioni:

- estremi della classificazione, numero del fascicolo, oggetto del fascicolo, data di apertura, ufficio competente, livello di riservatezza, tempo previsto di conservazione, titolare del procedimento amministrativo.

I fascicoli vengono creati secondo le esigenze di servizio con riferimento ad una specifica voce del Titolario:

- per oggetto/soggetto: fascicolo che raccoglie documenti di varia natura e tipologia relativi ad un argomento specifico o a una persona fisica o giuridica;
- per procedimento amministrativo: fascicolo che raccoglie documenti relativi ad uno stesso procedimento amministrativo;
- per tipologia del documento: fascicolo che raccoglie documenti sciolti raggruppati in base alla loro tipologia o forma.

Il fascicolo può essere suddiviso in sotto-fascicoli. Questa suddivisione è posta gerarchicamente al di sotto del numero di fascicolo. Il sotto-fascicolo, essendo riferito ad un sub-procedimento o essendo interno al procedimento stesso, può essere chiuso prima del fascicolo. Il numero del fascicolo è riportato su tutti i documenti.

I fascicoli informatici devono recare i metadati obbligatori delle aggregazioni documentali previsti nell'allegato 5 alle Linee guida AgID.

32. Repertorio dei fascicoli

I fascicoli sono annotati nel repertorio dei fascicoli. Il repertorio dei fascicoli è ripartito per ciascun titolo e classe del Piano di classificazione e rappresenta lo strumento di gestione dei fascicoli. Con il Piano di classificazione sono descritte le funzioni svolte e le competenze dell'Ente, con il repertorio dei fascicoli sono rappresentate le attività effettivamente svolte e sono raccolti i relativi documenti.

Il repertorio dei fascicoli è gestito mediante la procedura informatica ed è aggiornato automaticamente. Alla chiusura di ogni esercizio viene generato il repertorio annuale e viene conservato secondo le vigenti prescrizioni normative.

Nel repertorio sono indicati:

- la data di apertura;
- il numero del fascicolo e, se previsto, del sotto-fascicolo;
- gli estremi di classificazione completo (titolo e classe);
- l'oggetto del fascicolo e, se previsto, del sotto-fascicolo;
- la data di chiusura.

La chiusura del fascicolo compete al responsabile del procedimento contestualmente alla chiusura del fascicolo informatico e all'aggiornamento del repertorio dei fascicoli da parte del protocollista.

La chiusura di un fascicolo viene effettuata:

- quando si conclude il relativo procedimento;
- nel momento in cui cessa il rapporto del soggetto con l'Ente (es. i fascicoli personali dei dipendenti).
- quando decorre il termine scelto per la fascicolazione dei documenti (il semestre, l'anno solare, il biennio e simili).
- sul sistema di protocollo occorre completare nell'apposita maschera, le informazioni necessarie al passaggio del fascicolo dallo stato corrente/aperto a quello di chiusura e successivamente di deposito.

Si ritiene opportuno effettuare verifiche periodiche per controllare e aggiornare lo stato di apertura/chiusura dei fascicoli.

Il responsabile del procedimento alla chiusura del fascicolo provvede al controllo della documentazione contenuta. In particolare verifica la completezza della pratica:

- estrae eventuali documenti non pertinenti;
- inserisce se necessario i documenti relativi a fasi del procedimento che sono state curate da altri funzionari.
- elimina copie, fotocopie di cui non si richieda la conservazione;
- aggiorna l'etichetta del fascicolo, specificandone la data di chiusura.

33. Aggregazioni documentali

Le aggregazioni documentali, diverse dai fascicoli, sono serie archivistiche che aggregano documenti e serie archivistiche che aggregano fascicoli.

Ogni aggregazione raccoglie documentazione con caratteristiche formalmente omogenee, quali la natura e la forma dei documenti, eppure diversificate con riguardo ai contenuti (esempio: deliberazioni, determinazioni ecc.). Ogni aggregazione documentale è gestita per mezzo di un repertorio che prevede una numerazione progressiva.

Nel repertorio generale, generato alla chiusura di ogni esercizio, protocollato e inviato in conservazione, sono riportati i seguenti elementi obbligatori riferiti al singolo documento: numero di repertorio, data, estremi di classificazione, oggetto del documento.

Flussi documentali interni

34. Assegnazione dei documenti in entrata agli uffici

L'assegnazione dei documenti in entrata, quando possibile, è effettuata con modalità automatizzate. In particolare, sono automaticamente assegnati alle UO Responsabili preventivamente individuate i documenti provenienti dai portali dei servizi online (SUAP, SUE, ecc.) e le fatture provenienti dal Sistema di Interscambio (SDI). Ulteriori criteri di assegnazione automatica sono definiti dal

Responsabile, sentite le UOR interessate.

I documenti non assegnati automaticamente sono assegnati ai servizi dal personale addetto alla protocollazione in base all'oggetto del documento e alla classificazione. Quando un documento è di interesse anche per più UOR, si provvede a più assegnazioni, sia "per competenza" che "per conoscenza".

La procedura informatica di protocollo consente, all'interno dell'AOO, la trasmissione del documento in formato o supporto elettronico evitando così la circolazione di documenti interni su supporto cartaceo, per i seguenti scopi o ragioni:

- . **TRASMISSIONE:** assegnazione per competenza per cui è richiesta l'accettazione o il rifiuto del destinatario.
- . **INCARICATO:** seconda assegnazione per competenza per cui è richiesta l'accettazione o il rifiuto.
- . **CONOSCENZA:** trasmissione per visione, in tale circostanza non è possibile inserire nuove informazioni nella registrazione quali la classificazione, ed effettuare nuove trasmissioni con ragione diversa da visione.

Nel caso di un'assegnazione errata, la struttura che riceve il documento provvederà immediatamente ad assegnare lo stesso alla struttura effettivamente competente o a restituirla all'unità di protocollazione. Il sistema di gestione informatica dei documenti tiene traccia dei passaggi di cui sopra, memorizzando per ciascuno di essi l'identificativo dell'operatore agente, data e ora di esecuzione.

35. Comunicazioni interne

Tutte le comunicazioni interne sono effettuate esclusivamente in modalità telematiche, ivi compresa la pubblicazione di avvisi e comunicazioni a carattere informativo.

Le comunicazioni personali sono trasmesse a mezzo posta elettronica ordinaria. Quando la comunicazione indirizzata a più destinatari, in ragione del contenuto e degli invii multipli, potrebbe comportare la divulgazione di dati personali, il mittente provvede a invii individuali o in copia conoscenza nascosta (ccn).

36. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dal Comune che, ai sensi della normativa vigente, sono soggetti a pubblicazione all'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo che il documento sia divenuto imm modificabile. Gli atti oggetto di notificazione tramite pubblicazione ai sensi del codice di procedura civile, una volta ricevuti e scansionati, sono inseriti manualmente dal personale abilitato.

PARTE QUINTA – CONSERVAZIONE DEI DOCUMENTI

37. Piano di conservazione dell'archivio

Il Comune di Carpegna, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale del sistema di conservazione di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al manuale di conservazione del di cui all'Allegato 3 al presente Manuale nonché al manuale del Conservatore e agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione reperibili alla pagina <https://www.regione.marche.it/Regione-Utile/Agenda-Digitale/Polo-di-conservazione-regionale#Documentazione>.

Per quanto attiene la conservazione dei documenti contabili l'Ente si avvale, tramite il supporto della Ditta contrattualizzata per i gestionali, del Conservatore certificato Unimatica con il prodotto UNIMONEY per la gestione telematica degli Ordinativi Informatici (mandati di pagamento e reversali di incasso) con l'uso della firma digitale a norma AGID il cui manuale di Conservazione è reperibile alla pagina <https://www.unimaticaspa.it/it/manuale-del-sistema-di-conservazione>

38. Responsabile della conservazione

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD dell'ente.

Il Responsabile, sotto la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

In particolare, il responsabile della conservazione:

- a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare, della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede a versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali;
- m) predispone il manuale di conservazione in collaborazione con il Conservatore e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

39. Oggetti e formati della conservazione

Gli oggetti della conservazione sono:

- i documenti informatici formati dal Comune e i rispettivi metadati (conformi all'allegato 5 alle

Linee guida dell'AgID);

- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico generale e giornaliero;
- gli altri registri e repertori tenuti dall'ente.

Gli oggetti della conservazione sono trattati dal sistema di conservazione del Conservatore in pacchetti informativi che si distinguono in:

- a) pacchetti di versamento;
- b) pacchetti di archiviazione;
- c) pacchetti di distribuzione.

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie di documentarie oggetto del servizio di conservazione sono dettagliatamente descritte nel Manuale di Conservazione.

All'inizio di ogni anno i responsabili del procedimento individuano i fascicoli che sono da versare nell'archivio di deposito in quanto relativi ad affari o procedimenti conclusi o comunque non più necessari allo svolgimento delle attività correnti.

40. Archiviazione e conservazione digitale dei documenti informatici

Per la conservazione dei propri documenti informatici e delle loro aggregazioni documentali con i metadati a essi associati, il Comune di Carpegna si attiene a quanto disposto dal conservatore accreditato Regione Marche che cura la gestione, l'accessibilità e le operazioni di scarto dell'archivio digitale dell'ente, secondo le normative di legge e le modalità indicate dal Manuale della conservazione.

Per quanto riguarda la conservazione dei mandati e delle reversali in formato digitale ci si avvale del conservatore accreditato UNIMATICA-RGI S.p.A.

41. Selezione e scarto archivistico

I documenti che hanno esaurito ogni valore e ogni interesse amministrativo e in assenza di un interesse storico, sono soggetti a scarto.

Lo scarto dei documenti degli archivi dell'ente, indipendentemente dal loro formato o supporto, deve essere autorizzato dalla Soprintendenza Archivistica competente per territorio (D. Lgs. 42/2004, art. 21, comma 1, lettera d).

Le operazioni di scarto possono essere effettuate:

- in modo preordinato e periodico (annuo, biennio, ecc.), una volta trascorsi i tempi di conservazione previsti dal massimario;
- prima del versamento all'archivio di deposito, se i tempi di conservazione sono già decorsi;
- prima del passaggio dei documenti all'archivio storico.

Prima del passaggio all'archivio di deposito, le procedure di scarto devono essere svolte dal responsabile di unità organica che ha prodotto la documentazione in accordo con quella competente in materia di archivio in modo da garantire una gestione unitaria della procedura, criteri valutativi coerenti ed una semplificazione dei rapporti con la Soprintendenza Archivistica.

Con riguardo alle procedure di scarto, anche per le unità archivistiche informatiche, si fa riferimento al "Piano di conservazione/Massimario" dei documenti (Allegato 2). Nel Piano vengono definiti, secondo le indicazioni fornite da parte della SA nazionale, i tempi di permanenza nell'archivio comunale delle diverse tipologie documentali. La procedura prevede che venga inoltrata alla

competente Soprintendenza Archivistica una specifica e documentata richiesta di autorizzazione allo scarto.

Per il Comune di Carpegna quale Ente produttore dei documenti da inviare in conservazione è stato individuato formalmente il Responsabile della conservazione che coincide con il Responsabile del protocollo informatico, flusso documentale e archivi identificato nel Responsabile E.Q. dell'Area Amministrativa.

42. Misure di sicurezza e monitoraggio

Il Manuale di conservazione e il piano della sicurezza descrivono le modalità con cui il Conservatore assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i backup degli archivi e il Disaster recovery. Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

PARTE SESTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI

43. Piano di sicurezza informatica

I dati acquisiti tramite l'applicativo del Protocollo Informatico e flussi documentali e la banca dati del protocollo informatico sono ubicati su Cloud gestito dalla softwarehouse e i dati e i documenti gestiti dall'Amministrazione sono correttamente memorizzati e gestiti nei data base localizzati nel cloud assegnato, secondo i requisiti di integrità e sicurezza stabiliti dalla legge.

Il Responsabile della gestione documentale ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza prestabilita durante la fase di esercizio;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale.

44. Credenziali di accesso al sistema documentale

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di gestione documentale e protocollo informatico nel rispetto di modalità prestabilite. Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione).

Gli utenti del programma di gestione documentale e protocollo, in base alle rispettive competenze, dispongono di autorizzazioni di accesso differenziate.

Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente pubblica che permette l'identificazione dell'utente da parte del sistema (userID), e da una componente privata o riservata di autenticazione (password);
- una autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e work flow effettuabili alle sole funzioni necessarie.

La visibilità normalmente attribuita ad un utente si limita alla documentazione relativa ai servizi di competenza. La visibilità su altri documenti può essere attribuita dal responsabile della pratica o del procedimento.

L'accesso diretto alla banca dati, l'inserimento di nuovi utenti, la modifica dei diritti e le impostazioni sui documenti sono consentiti esclusivamente agli amministratori del sistema.

I diversi livelli di autorizzazione sono assegnati agli utenti dal Responsabile del servizio protocollo, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

45. Trattamento dei dati personali

Ai fini dell'applicazione della normativa sul trattamento dei dati personali, in relazione al ruolo funzionale svolto, gli addetti all'ufficio protocollo sono nominati incaricati dal designato al Trattamento dei dati per il trattamento dei dati personali in ambito di Banche dati informatizzate e cartacee inerenti alla gestione del flusso documentale della corrispondenza in arrivo e in partenza.

È disponibile software con accesso riservato e condiviso tra tutti i Responsabili designati al trattamento dei dati personali, come previsto dal Regolamento Europeo n. 679/2016 e decreti attuativi, aggiornata in tempo reale contenente sia i registri di trattamento che dell'accesso agli atti e dell'attività, anche in linea con le direttive del Segretario Generale e del RPD, nonché secondo appositi modelli predisposti ai sensi di legge.

Al seguente link del sito istituzionale è disponibile l'informativa in ordine al trattamento dei dati personali: <https://www.comune.carpegna.pu.it/home/informativa-privacy>

46. Piano formativo del personale

In conformità a quanto disposto dall'art. 13 del D.lgs. 82/2005, ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, il Responsabile verifica la necessità di apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo del Sistema di Gestione Informatica dei Documenti;
- fascicolazione dei documenti informatici;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative alla gestione documentale;
- legislazione in materia di protezione dei dati personali;
- aggiornamento sui temi suddetti.

Periodicamente è cura del Responsabile rilevare necessità formative in accordo con i vari responsabili di Area, ed effettuare dei controlli a campione sulla congruità delle registrazioni, sulla corretta sequenza della catena documentale e sull'utilizzo di un unico registro informatico, verificando, attraverso controlli nei vari uffici, la classificazione e la fascicolazione archivistica nonché le modalità di gestione dei documenti informatici.

PARTE SETTIMA - NORME TRANSITORIE E FINALI

47. Modalità di approvazione e aggiornamento del manuale

Il Manuale sarà aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevata nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi.

Il Manuale viene approvato con deliberazione della Giunta comunale su proposta del Responsabile della gestione documentale e dell'RTD.

48. Pubblicità del manuale

Il presente Manuale, ai sensi della normativa vigente, è reso disponibile alla consultazione del pubblico mediante pubblicazione nel sito internet dell'Amministrazione, sezione Amministrazione trasparente inoltre, copia del presente Manuale:

- a) è resa disponibile a tutto il personale dell'Amministrazione mediante la rete intranet ed internet;
- b) è inviata alla Soprintendenza Archivistica.

49. Entrata in vigore

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

ELENCO ALLEGATI AL MANUALE DI GESTIONE

<i>Allegato 1</i>	<i>Titolario di classificazione</i>
<i>Allegato 2</i>	<i>Piano di conservazione e massimario di scarto</i>
<i>Allegato 3</i>	<i>Manuale di conservazione</i>
<i>Allegato 4</i>	<i>Tabella riassuntiva dei compiti</i>
<i>Allegato 5</i>	<i>Elenco indirizzi PEC dell'Ente</i>
<i>Allegato 6</i>	<i>Formati file accettati per la protocollazione</i>
<i>Allegato 7</i>	<i>Schema registro protocollo di emergenza</i>
<i>Allegato 8</i>	<i>Procedura di Data Breach</i>