



COMUNE DI OLIENA



Provincia di Nuoro

MANUALE DI GESTIONE DOCUMENTALE

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 Deliberazione di Giunta n° 54/2025

Sommario

PARTE PRIMA – DISPOSIZIONI PRELIMINARI	4
1. <i>Riferimenti normativi</i>	4
2. <i>Finalità, contenuti e metodologia del documento</i>	5
3. <i>Definizioni.....</i>	5
PARTE SECONDA – ORGANIZZAZIONE.....	5
4. <i>Area organizzativa omogenea (AOO) e Unità Organizzative Responsabili (UOR).....</i>	5
5. <i>Il Responsabile della gestione documentale</i>	5
6. <i>La governance della gestione documentale</i>	6
7. <i>Livelli di accesso al sistema di protocollo</i>	6
PARTE TERZA – FORMAZIONE DEI DOCUMENTI	7
Modalità di formazione.....	7
8. <i>Modalità di formazione dei documenti informatici.....</i>	7
Sezione seconda – Disposizioni comuni a tutte le modalità di formazione	11
9. <i>Dispositivi di firma elettronica.....</i>	11
10. <i>Identificazione univoca del documento informatico</i>	11
11. <i>Associazione degli allegati al documento principale</i>	11
12. <i>Metadati del documento informatico</i>	12
13. <i>Immodificabilità e integrità del documento informatico</i>	12
PARTE QUARTA - GESTIONE DOCUMENTALE.....	13
Flussi documentali esterni	13
14. <i>Ricezione telematica di documenti informatici in entrata.....</i>	13
15. <i>Canali di ricezione.....</i>	13
16. <i>Valutazione di interoperabilità</i>	14
17. <i>Trasmissione telematica di documenti informatici in uscita</i>	14
18. <i>Comunicazioni e trasmissione di documenti con altre Pubbliche Amministrazioni</i>	14
19. <i>Disposizioni sui documenti analogici.....</i>	15
Protocollo informatico	15
20. <i>Sistema di protocollo informatico</i>	15
22. <i>Registro generale di protocollo.....</i>	16
23. <i>Documenti soggetti a registrazione di protocollo e documenti esclusi</i>	16
24. <i>Registrazione di protocollo</i>	17
25. <i>Annulloamento e modifiche della registrazione di protocollo</i>	18
26. <i>Segnatura di protocollo</i>	18
27. <i>Documenti soggetti a registrazione particolare</i>	19
28. <i>Registro di emergenza</i>	20
29. <i>Disposizioni sulla protocollazione di documenti analogici</i>	20
Classificazione	21

30. <i>Classificazione dei documenti</i>	21
Flussi documentali interni	22
31. <i>Assegnazione dei documenti in entrata agli uffici</i>	22
33. <i>Comunicazioni interne</i>	22
34. <i>Pubblicazioni nell'Albo pretorio</i>	22
PARTE QUINTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI	24
41. <i>Piano di sicurezza informatica</i>	24
42. <i>Credenziali di accesso al sistema documentale</i>	25
43. <i>Trattamento dei dati personali</i>	26
44. <i>Piano formativo del personale</i>	26
45. <i>Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza</i>	26
PARTE SETTIMA - NORME TRANSITORIE E FINALI.....	28
46. <i>Modalità di approvazione e aggiornamento del manuale</i>	28
47. <i>Pubblicità del manuale</i>	28
48. <i>Entrata in vigore</i>	28

ALLEGATI

Allegato 1.	Glossario e definizioni
Allegato 2.	Area Organizzativa Omogenea Responsabili (AOO) e Unità Organizzative (UOR)
Allegato 3.	Titolario

PARTE PRIMA – DISPOSIZIONI PRELIMINARI

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 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*”;
- la Circolare n. 2/2017 del 18 aprile 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 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 perseguitamento del principio di trasparenza dell’azione amministrativa.

3. Definizioni

Ai fini dell’utilizzo del presente manuale si applicano le definizioni del glossario di cui all’Allegato n. 1 “Glossario e definizioni” che ne costituisce parte integrante.

PARTE SECONDA – ORGANIZZAZIONE

4. Area organizzativa omogenea (AOO) e Unità Organizzative Responsabili (UOR)

Il Comune di Oliena 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.

Le UOR che afferiscono alla AOO sono riportate nell’Allegato 2 (Area Organizzativa Omogenea (AOO) e Unità Organizzative Responsabili (UOR)) al presente manuale, che potrà essere oggetto di modifiche e integrazioni per effetto di successivi interventi sulla struttura organizzativa del Comune.

5. Il Responsabile della gestione documentale

Con riferimento all’unica AOO si prende atto che con decreto n. 15 in data 25/06/2025 è stato individuato nel dott. Filippo Secchi, che riveste la qualifica di Responsabile dell’Area Amministrativa e Vigilanza, il Responsabile della gestione documentale e della conservazione, che ha provveduto alla predisposizione del presente manuale.

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;
- 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.

6. La governance della gestione documentale

Il responsabile della gestione documentale e della conservazione 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), acquisito il parere del responsabile della protezione dei dati personali, 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 .

7. 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, di aggiornamento e consultazione di protocolli esclusivamente attinenti alla propria area di appartenenza.

Solo gli addetti al Servizio Protocollo 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.

PARTE TERZA – FORMAZIONE DEI DOCUMENTI

Modalità di formazione

8. 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 sopra descritte

8.1. Creazione e redazione tramite software di documenti informatici

Gli uffici del Comune dispongono degli strumenti software della suite *Microsoft Office: Word, Excel, Access, Powerpoint, ecc.*, per la creazione dei documenti informatici mediante redazione.

Elementi essenziali del documento amministrativo informatico.

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. numeri di pagina;
9. indicazione degli allegati (se presenti);
10. identificazione e dati dei destinatari (se si tratta di documento in uscita);
11. dati dell'Amministrazione (compresi indirizzo e recapiti, se si tratta di documento in uscita);
12. mezzo di spedizione (se documento in uscita).

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

Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consente la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.

Una volta giunto alla sua versione definitiva, prima della sottoscrizione, il documento informatico deve essere salvato in formato PDF. I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Sindaco e degli organi collegiali, i contratti, le determini a contenuto provvidenziale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES, ad eccezione degli atti del Sindaco e degli organi collegiali, i contratti, le determini a contenuto provvidenziale, per i quali la sottoscrizione avviene con firma CADES (P7M).

Nel caso il documento definitivo assuma un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (P7M).

8.2. 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.

8.3. 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.

8.4. 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 ".doc" 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.

8.5. 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 e CNS. I dati immessi dall'istante 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. Il file di log relativi agli accessi e alle attività svolte dagli utenti sono conservati secondo le stesse modalità di conservazione delle istanze ricevute tramite PEC.

Sezione seconda – Disposizioni comuni a tutte le modalità di formazione

9. 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 del proprio settore, 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.

10. 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.

11. 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 immodificabile.

12. Metadati del documento informatico

Al documento informatico e al documento amministrativo informatico devono essere associati i metadati obbligatori previsti dall'Allegato 5 alle Linee guida dell'AgID;

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

13. 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 immodificabile 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 possono essere 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

14. 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 o CNS;
- d) sono trasmesse da un domicilio digitale PEC ai sensi dell'art. 3-bis, comma 4quinquies del CAD ed è possibile accettare 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.

15. 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 SUE e SUAPE;
- cooperazione applicativa tra pubbliche amministrazioni;
- altri canali di trasmissione, anche di posta elettronica ordinaria, indicati per specifici procedimenti.

L'indirizzo di posta elettronica certificata è riportato nell'Indice delle Pubbliche Amministrazioni e pubblicizzato 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.

16. 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”.

Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti preposti possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2, effettuando una valutazione di interoperabilità in base alle indicazioni previste nell'Allegato stesso. La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

A seguito della valutazione di interoperabilità, 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.

17. Trasmissione telematica di documenti informatici in uscita

La trasmissione di comunicazioni e documenti avviene sempre per via telematica, salvo il caso 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 della presente Parte del 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.

18. 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 (indicepa.gov.it) di cui all'art. 6-ter del CAD.

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

19. 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 indicati sul sito web istituzionale del Comune.

Le buste delle comunicazioni cartacee sono conservate insieme ai documenti in esse contenuti.

Protocollo informatico

20. Sistema di protocollo informatico

Per la gestione dei documenti è adottato un modello organizzativo che prevede la partecipazione attiva di più soggetti ed uffici, ognuno dei quali è abilitato a svolgere soltanto le operazioni di propria competenza.

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

Il servizio informatico esegue la funzione di aggiornamento dei profili di abilitazione alla protocollazione, solo su indicazione del Responsabile della gestione documentale.

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. assegna al personale addetto alla protocollazione 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.

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 successivamente.

Ai sensi dell'articolo 53 del TUDA sono esclusi dalla registrazione di protocollo:

- Gazzette Ufficiali, Bollettini Ufficiali, notiziari della Pubblica Amministrazione;
- 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.

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.

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 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.

A suddetti metadati registrati in forma non modificabile, inoltre, possono essere aggiunti (a seconda dei casi) i seguenti ulteriori metadati:

- a) tipologia di documento;
- b) classificazione (titolo e classe) sulla base del Titolario e del Prontuario di Classificazione;
- c) fascicolo di appartenenza;
- d) assegnazione interna (per competenza o per conoscenza);
- e) data e ora di arrivo;
- f) allegati;
- g) livello di riservatezza;
- h) mezzo di ricezione o invio;
- i) annotazioni;
- j) (eventualmente) estremi del provvedimento di differimento della registrazione;
- k) (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:

- 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 es. 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. In tal caso, la comunicazione formale di autorizzazione resa dal delegato deve indicare gli estremi del 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 posso essere svolte dal personale addetto alla protocollazione, anche senza 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

- CORRISPONDENZA RISERVATA

La corrispondenza personale indirizzata al dipendente va evidenziata con l'apposizione della dicitura "personale" o "riservata" sulla busta chiusa. Conseguentemente la busta va consegnata integra direttamente al destinatario, il quale valuterà l'opportunità di sottoporre il documento alla registrazione.

- FAX

I documenti ricevuti tramite fax sono giuridicamente validi ai sensi dell'art. 45 del D. Lgs 82/2005 e s. m. i. e vanno quindi protocollati e la segnatura viene effettuata sulla prima pagina del documento; sull'eventuale originale cartaceo ricevuto per posta ordinaria deve essere apposto lo stesso numero e data di protocollo del corrispondente documento anticipato via fax.

- DOCUMENTI INFORMATICI E POSTA ELETTRONICA CERTIFICATA

I documenti informatici inviati con posta elettronica certificata, quelli sottoscritti con firma elettronica, quelli inviati alla casella istituzionale dell'ente, del settore o del responsabile del procedimento, sono soggetti a registrazione di protocollo utilizzando le funzioni del sistema che prevedono l'indicazione del mezzo di trasmissione e l'esplicitazione che si tratta di un documento originale digitale, come specificato nei manuali tecnici del sistema di protocollo.

Il Responsabile di Settore o il responsabile del procedimento amministrativo valuta comunque l'opportunità di registrare il documento in funzione della rilevanza dello stesso per l'attività amministrativa dell'Ente.

- DOCUMENTI INERENTI A GARE D'APPALTO E PROCEDURE CONCORSUALI;

La corrispondenza riportante l'indicazione "offerta", "gara d'appalto", "concorso" o simili o comunque dalla cui confezione si evinca la partecipazione ad una gara, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo, della data e dell'ora di arrivo direttamente sulla busta (plico o simili).

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 si rinnova ogni anno solare, pertanto inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

Si applicano le seguenti modalità di registrazione e di recupero dei dati:

- sul registro di emergenza sono riportate le cause, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema;
- per ogni giornata di registrazione in emergenza è riportato sul registro il numero totale di operazioni registrate;
- la sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO;
- le informazioni relative ai documenti protocollati in emergenza sono inserite immediatamente nel sistema di protocollo informatico ripristinato;
- durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, annotando nella scheda di protocollo gli elementi necessari a mantenere stabilmente la correlazione univoca con il numero attribuito in emergenza.

29. Disposizioni sulla protocollazione di documenti analogici

Il personale addetto a effettuare la registrazione informatica di protocollo in entrata è competente anche per la protocollazione dei documenti analogici in entrata (consegnati a mano o pervenuti tramite servizio postale). Di tale documentazione è effettuata una copia per immagine su supporto informatico (scansione in formato pdf/A) prima della registrazione.

Qualora il documento analogico sia consegnato direttamente dal mittente o da altra persona a ciò delegata e sia richiesto il rilascio di una ricevuta attestante l'avvenuta consegna del documento, è cura del personale del Servizio di Protocollo rilasciare la ricevuta di avvenuta protocollazione prodotta direttamente dal protocollo informatico. La ricevuta di avvenuta protocollazione prodotta dal sistema di protocollo riporta i seguenti dati:

- il numero e la data di protocollo;
- l'indicazione dell'AOO;

- il mittente;
- l'oggetto;
- numero e descrizione degli allegati se presenti;
- l'indicazione della UOR cui è assegnato il documento per competenza;
- l'operatore di protocollo che ha effettuato la registrazione.

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.

Classificazione

30. Classificazione dei documenti

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (Titolario – Allegato 3).

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

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

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

La revisione anche parziale del Titolario viene proposta dal Responsabile quando necessaria e opportuna.

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

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

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

Il Titolario adottato dall'amministrazione è composto da 3 livelli. Le voci di Categorie, le classi e le sottoclassi individuano le funzioni primarie e di organizzazione dell'ente.

Le categorie, le classi e le sottoclassi sono già forniti nel sistema informatico di protocollo e gestione documentale.

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

I livelli di classificazione (categorie-classe-sottoclasse) vengono attribuiti nella fase di protocollazione.

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

Flussi documentali interni

31. 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 alle UO Responsabili 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".

Lo scambio di documenti tra il Servizio di Gestione Documentale e le diverse UOR del Comune è effettuato per mezzo di posta elettronica, tramite protocollazione interna, così come lo scambio di documenti tra le UOR del Comune. Scambi di documenti tra gli uffici possono essere effettuati anche attraverso rete intranet e cartelle condivise. In ogni caso, nelle attività di trasmissione e scambio dei documenti tutto il personale deve utilizzare esclusivamente gli strumenti di comunicazione messi a disposizione dal Comune.

33. 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).

34. Pubblicazioni nell'Albo pretorio

Tutti gli atti prodotti dal Comune che, ai sensi della normativa vigente, sono soggetti a pubblicazione nell'Albo pretorio online dell'ente, sono trasmessi per la pubblicazione in modo automatizzato solo dopo

che il documento sia divenuto immodificabile. 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.

Per le specifiche dei documenti soggetti a pubblicazione, si rimanda al Regolamento per la gestione dell'albo pretorio on line approvato, con deliberazione della giunta comunale n. 143 del 12/12/2024, che disciplina l'organizzazione e la gestione dell'Albo pretorio on-line del Comune di Oliena in relazione agli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale ai sensi dell'art. 32 della Legge 18 giugno 2009, n. 69.

PARTE QUINTA – MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI

41. Piano di sicurezza informatica

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici sono garantiti dall'applicazione informatica adottata dall'Ente.

Il piano di sicurezza informatica del sistema informativo dell'amministrazione è definito dall'organizzazione dell'Ente che gestisce il sistema informatico generale.

A tale fine l'Ente definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui alla Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni*;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

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;
- piano di continuità del servizio, con particolare riferimento sia all'esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP (prodotto di protocollo informatico);
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);

- 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;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l’arco della giornata, comprese le operazioni di backup e manutenzione del sistema. I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal Responsabile della gestione documentale e dal titolare dei dati e, ove previsto, dalle forze dell’ordine.

42. 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);
- un’autorizzazione di accesso (profilo) che limita le operazioni di protocollo, gestione documentale e workflow 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 della gestione documentale, in base alle indicazioni fornite dai Responsabili dei servizi di appartenenza.

Gli accessi esterni a documenti, dati e informazioni non divulgabili sono subordinati alla registrazione sul sistema e al possesso di apposite credenziali, rilasciate previa identificazione diretta da parte di un dipendente abilitato.

Gli accessi esterni a documenti, dati e informazioni divulgabili sono consentiti anche senza autenticazione all'accesso, garantendo comunque il diritto alla riservatezza e all'oblio, e la tutela dei dati personali in conformità alle disposizioni vigenti.

Gli accessi esterni vengono di norma gestiti attraverso il sito web dell'Ente. I dati in libera consultazione vengono esposti in formato aperto (con dovute eccezioni, indotte anche da considerazioni di carattere tecnico, organizzativo o gestionale) che ne consenta il riutilizzo.

43. 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 designati 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.

44. 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, l'Ente predispone le 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 dei Responsabili della Gestione Documentale, rilevare necessità formative in accordo con i vari responsabili di settore, 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 nonché le modalità di gestione dei documenti informatici.

45. Monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza

Il fornitore del software di gestione documentale controlla giornalmente i log di sistema e li mantiene per 6 mesi, al fine di verificare eventuali violazioni del Sistema.

Il Responsabile della gestione documentale dell'ente effettua periodiche verifiche sul corretto funzionamento del sistema di gestione informatica dei documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti alla gestione documentale.

PARTE SETTIMA - NORME TRANSITORIE E FINALI

46. 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 Gestione Documentale.

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

47. 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, nell'Area Amministrazione trasparente" sezione Regolamenti".

Inoltre, copia del presente Manuale è trasmessa a tutto il personale dell'Amministrazione;

48. Entrata in vigore

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