COMUNE DI
SESTO FIORENTINO

sestofiorentino

piazza Vittorio Veneto, 1
50019 | tel. 055 055

www.comune.sesto-fiorentino.fi.it

TESTO UNICO DELLA GESTIONE DOCUMENTALE, FASCICOLAZIONE E CONSERVAZIONE DEL COMUNE DI SESTO FIORENTINO

approvato con Delibera della Giunta Comunale n. 197 del 03.07.2018

Sommario

SEZIONE 1

1. PRINCIPI GENERALI

1.1. Scopo del Testo Unico della gestione documentale, fascicolazione e conservazione del Comune di Sesto Fiorentino

Il Testo Unico della gestione documentale, fascicolazione e conservazione del Comune di Sesto Fiorentino raccoglie in un unico documento il Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi, approvato con delibera della Giunta Comunale n. 138 del 12.12:2016 , e il Manuale Operativo del sistema di fascicolazione e di conservazione, approvato con delibera della Giunta Comunale n. 354 del 28.12.2017, comprensivi degli allegati, con lo scopo di coordinarne le disposizioni e di eliminare le duplicazioni.

Esso descrive il sistema di protocollazione e gestione del flusso dei documenti, a partire dalla fase di protocollazione, fino ad arrivare alla loro fascicolazione e conservazione.

In particolare disciplina:

- la gestione dei documenti elettronici al fine di dematerializzare e automatizzare i procedimenti;
- le modalità operative per la gestione del protocollo, dei flussi documentali e procedimentali, degli archivi;
- le modalità operative per la gestione e digitalizzazione dei documenti analogici;
- l'uso del titolario di classificazione.

Descrive inoltre il sistema di fascicolazione e conservazione ai sensi della normativa vigente in materia di formazione, acquisizione e conservazione dei documenti digitali, definendo, in particolare:

- i soggetti coinvolti nel processo di fascicolazione e in quello di conservazione;
- l'oggetto della fascicolazione e della conservazione;
- gli obblighi e le responsabilità;

- il processo di fascicolazione e il processo di conservazione;
- le modalità da attuare per garantire la conservazione permanente dei documenti;
- le modalità per ottenere l'esibizione a norma di un documento conservato.

Il T.U. è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce indicazioni complete circa la corretta esecuzione delle operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti. Si rivolge, pertanto, non solo agli operatori di protocollo ma, in generale, a tutti i dipendenti nonché ai soggetti esterni che si relazionano con l'Amministrazione, in un'ottica di trasparenza amministrativa, buona gestione e collaborazione con la cittadinanza.

1.2. Ambito di applicazione del T.U.

Il presente T.U. è adottato ai sensi del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – *Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47 e 71 del C.A.D. di cui D.L. 82/2005* e del Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

1.3. Responsabili del T.U.

Responsabili del presente T.U. sono il Responsabile del Protocollo e della Gestione dei Flussi Documentali e il Responsabile della Conservazione del Comune di Sesto Fiorentino.

1.4. Definizioni ed acronimi

- **Archiviazione elettronica**: processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, così come individuati nella normativa vigente, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione;

- **Blocco di conservazione**: raggruppamento di pacchetti informativi presi in carico per la conservazione dal sistema di conservazione.
- **Conservazione**: processo che assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, di documenti informatici, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità nel tempo.
- **Delegato per l'attività di conservazione**: la persona fisica o giuridica tenuta a svolgere le attività di conservazione dei documenti in forza di apposita delega conferita dal Responsabile della Conservazione.
- **Documento**: rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.
- **Documento informatico**: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art 1, lett. p, del D.Lgs. n. 82/2005).
- **Documento statico non modificabile**: documento informatico redatto adottando modalità che ne garantiscono l'integrità e l'immodificabilità durante le fasi di accesso e di conservazione; a tal fine il documento informatico non deve contenere macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.
- **Esibizione**: la richiesta con la quale il produttore richiede al conservatore di recuperare ed esibire un documento precedentemente affidatogli per la conservazione**.**
- **Esibizione a norma**: l'esibizione completa del pacchetto di distribuzione ottenuto tramite interrogazione al sistema di conservazione, legalmente valida ai sensi del secondo comma dell'articolo 10 del DPCM 03/12/13 e dell'articolo 5 del DMEF 17/06/14
- **Evidenza informatica**: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art.1, lett. f, del D.P.C.M. 22 febbraio 2013).
- **Firma digitale**: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 lett. s del D. Lgs. n. 82/05).
- **Funzione di hash**: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (art. 1, lett. g, D.P.C.M. 22 febbraio 2013).

- **Impronta di una sequenza di simboli binari (bit)**: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di un'opportuna funzione di hash (art. 1, lett. h, D.P.C.M. 22 febbraio 2013).
- **Marca temporale**: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, lett. i, D.P.C.M. 22 febbraio 2013).
- **Pacchetto di archiviazione**: pacchetto informativo composto dalla trasformazione di uno più pacchetti di versamento secondo le modalità riportate nel presente T.U.
- **Pacchetto di distribuzione**: pacchetto informativo inviato dal sistema di conservazione all'utente in risposta a una sua richiesta di esibizione.
- **Pacchetto informativo**: contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche).
- **Pacchetto di versamento**: pacchetto informativo inviato dall'utente al sistema di conservazione secondo un formato predefinito e concordato, descritto nel T.U. di conservazione del sistema di conservazione.
- **Posta elettronica**: un sistema elettronico di trasmissione di documenti informatici (art. 1, lett. h, D.P.R. n. 68/2005).
- **Posta elettronica certificata**: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi (art. 1 lett. v bis del D. Lgs. n. 82/05).
- **Produttore:** ogni persona che produce documenti o fascicoli gestiti attraverso il sistema di conservazione.
- **Responsabile della Conservazione**: il soggetto che svolge le attività di conservazione, in conformità a quanto disposto dal presente T.U. e dalle disposizioni normative vigenti in materia.
- **Responsabile del Protocollo e della Gestione dei Flussi Documentali:** il soggetto che coordina e sovrintende alle operazioni di protocollazione e di gestione del relativo flusso documentale, in conformità a quanto disposto dall'art. 61 del D.P.R. n. 445/2000, dall'art. 4 del Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – *Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71 del C.A.D. di cui D.L. 82/2005* e dal presente T.U., nel rispetto della normativa in materia di protezione dei dati personali.
- **Responsabile dei servizi informatici:** il soggetto che coordina e sovrintende alla gestione dei servizi informatici dell'ente, comprensivi di hardware, software e banche dati, compresi gli aspetti di sicurezza informatica, data breach e disaster recovery.

- **Riferimento temporale**: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, lett. m, D.P.C.M. D.P.C.M. 22 febbraio 2013).
- **Riversamento diretto**: processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità.
- **Riversamento sostitutivo**: processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione a un altro, modificando la loro rappresentazione informatica.
- **Sistema di conservazione a norma**: l'unione dei sistemi di conservazione di cui sono responsabili i delegati su un'infrastruttura tecnologica qualificata.
- **Sistema di protocollazione e di gestione dei flussi documentali**: l'infrastruttura tecnologica che consente di ricevere da varie fonti documenti, istanze, segnalazioni e documenti in genere, di protocollarli in modo elettronico e di indirizzarli in modo quanto più possibile automatico verso il corretto flusso documentale, nonché di monitorare le fasi di assegnazione e di presa di carico dei documenti.
- **Utente**: ogni persona abilitata ad operare nel sistema di protocollazione e di gestione dei flussi documentali del Comune e ogni persona abilitata ad accedere al sistema di conservazione o a fruire dei suoi servizi.
- **Validazione temporale**: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data e un orario opponibili ai terzi.
- **Vicario**: la persona fisica deputata a sostituire il Responsabile della Gestione dei Flussi Documentali in caso di assenza o impedimento.

Per ogni altra definizione si fa riferimento al D. Lgs. 82/2005, al DPCM 3 dicembre 2013 e al DPCM 13 novembre 2014.

Nel presente T.U. si possono utilizzare i seguenti acronimi ed espressioni sintetiche:

- **CAD** - Decreto Legislativo 7 marzo 2005 n. 82 – Codice dell'Amministrazione digitale, nel testo vigente;
- **Regole tecniche** - Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 – Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui D.Lgs. 82/2005;
- **T.U.** – Testo unico della gestione documentale, fascicolazione e conservazione del Comune di Sesto Fiorentino

- **Testo Unico sulla documentazione amministrativa** approvato con D.P.R. 445/2000;
- **AOO** - Area Organizzativa Omogenea.
- **IPA –** Indice delle Pubbliche Amministrazioni - Sito WEB che raccoglie gli indirizzi PEC ufficiali di tutte le PA.
- **PdP** - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'Amministrazione/AOO per implementare il servizio di protocollo informatico.
- **UO –** Unità Organizzativa – unità organizzativa interna (settore, servizio, ufficio).
- **UCP** - Unità Organizzativa Centrale di registrazione di Protocollo – rappresenta l'ufficio centrale di protocollo.
- **UOP –** Unità Organizzativa di registrazione di Protocollo – unità organizzativa abilitata alla protocollazione, diversa dall'ufficio centrale di protocollo.
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.
- **RPA**- Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare.
- **RC –** Responsabile della Conservazione
- **RF –** Responsabile della fascicolazione
- **RPF** - Responsabile del Protocollo e della Gestione dei Flussi Documentali.
- **ADS –** Amministratori di sistema.

1.5. Riferimenti normativi principali

- **Regolamento UE n. 679/2016** in materia di trattamento dei dati personali
- **Decreto del Presidente della Repubblica 11 febbraio 2005 n. 68** - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata.
- **Decreto Legislativo 5 marzo 2005 n. 82 e successive modifiche e integrazioni** - Codice dell'Amministrazione digitale.
- **D.M. 2 novembre 2005** - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.
- **Circolare dell'Agenzia delle Entrate 45/E del 19 ottobre 2005,** relativa al flusso e alla conservazione della fatturazione elettronica

- **Circolare dell'Agenzia delle Entrate 36/E del 6 dicembre 2006 –** Oggetto: Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.
- **D.L. 25 giugno 2008, n. 112** - Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria.
- **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 –** Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del C.A.D. di cui al D.Lgs. 82/2005.
- **Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013** - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 *-bis* , 23 *-ter* , comma 4, 43, commi 1 e 3, 44 , 44 *-bis* e 71, comma 1, del CAD di cui al D.Lgs. 82/2005.
- **Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto
- **Circolare 10 aprile 2014, n. 65** - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all' articolo 44-bis, comma 1, del Decreto legislativo 7 marzo 2005, n. 82
- **Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014** - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

2. SOGGETTI

2.1. Responsabile del Protocollo e della Gestione dei Flussi Documentali

Al fine di coordinare e gestire opportunamente il servizio di protocollazione, è nominato il Responsabile del Protocollo e della Gestione dei Flussi Documentali (RPF). In caso di assenza del Responsabile, le sue funzioni sono demandate al vicario formalmente delegato.
Il RPF normalmente coincide con il Responsabile del servizio nel quale è incardinato l'Ufficio protocollo dell'Ente, in relazione alla struttura organizzativa vigente. Egli risponde della fase di produzione del documento informatico.

Il RPF:

a) propone le modifiche al titolario di classificazione;
b) verifica la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dall'Ente attraverso l'adozione dei formati standard ammessi dalla normativa vigente, in collaborazione con il Responsabile dei Servizi Informatici;
c) cura, di concerto con il Servizio "Servizi Informatici", le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile, come da documentazione operativa depositata presso il Servizio "Servizi Informatici";
d) conserva le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il sistema principale o procede al loro versamento presso il sistema di conservazione a norma;
e) supervisiona il buon funzionamento degli strumenti e cura il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
f) propone i tempi, le modalità e le misure organizzative e tecniche finalizzate all'eliminazione dei protocolli di settore, di reparto, dei protocolli multipli, dei protocolli di fax, e, più in generale, dei protocolli diversi dal protocollo informatico;
g) provvede alla formazione del personale;
h) abilita gli operatori dell'Ente all'utilizzo del sistema software di gestione documentale e definisce per ciascuno di essi il livello di accesso e l'ambito di azione consentito;
i) verifica il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
j) supervisiona la corretta produzione del registro giornaliero di protocollo a cura dell'ufficio protocollo;

k) autorizza l'annullamento e/o la modifica delle registrazioni di protocollo richieste dai servizi/uffici dell'Ente;

l) autorizza l'utilizzo del registro di emergenza alle condizioni previste dal presente T.U.;

m) può modificare le assegnazioni di protocollo, derivanti da errori, e può effettuare interventi diretti sul software di gestione del protocollo informatico, sempre al fine di eliminare errori e inesattezze, ferma restando la tracciatura completa delle attività svolte.

In ragione del ruolo e dei compiti sopra indicati spetta al RPF la completa visibilità dell'intero protocollo dell'Ente e delle caselle di posta elettronica certificata istituzionali.

2.2. Responsabile della Conservazione

Il Responsabile della Conservazione viene nominato con atto deliberativo della Giunta Comunale tra i dirigenti o i funzionari con specifica competenza ed esperienza ed è designato per garantire la conservazione e l'affidabilità nel tempo dei documenti informatici prodotti o detenuti dall'Ente.

Il ruolo di RC può essere svolto dal RPF.

Il RC definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione, agendo d'intesa con il RPF, se diverso, e con il Responsabile dei Servizi Informatici, in relazione al modello organizzativo adottato dall'Ente.

In particolare, svolge i seguenti compiti attribuiti dall'art. 7 del DPCM 3 dicembre 2013:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
c) genera il rapporto di versamento, secondo le modalità previste dal presente T.U.;
d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal presente T.U.;
e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
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 ripristinarne la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati, avvalendosi in entrambi i casi del supporto tecnico del Servizio "Servizi informatici" dell'Ente;
h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal presente T.U., attraverso il supporto tecnico del Servizio "Servizi informatici" dell'Ente;
i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013, sempre attraverso il supporto tecnico del Servizi "Servizi informatici" dell'Ente;
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;

Il RC può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività a essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa e in particolare le specifiche funzioni e competenze affidate al delegato, come stabilito dalla successiva Sezione 4.

2.3. Delegato per l'attività di conservazione

Il delegato per l'attività di conservazione è il soggetto pubblico o privato, nominato dal RC, al quale viene affidata in modo totale o parziale la conservazione dei documenti digitali mediante contratto o convenzione di servizio che preveda il rispetto degli obblighi di cui alla Sezione 4 del presente T.U.

Esso viene nominato in base alle esigenze di conservazione e al modello organizzativo adottato dal Comune di Sesto Fiorentino, con apposito atto amministrativo.

Il delegato deve offrire idonee garanzie organizzative e tecnologiche per lo svolgimento delle funzioni affidategli.

Il delegato per l'attività di conservazione può svolgere i suoi compiti per il tramite di una o più persone o imprese incaricate che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ed il rispetto della normativa vigente.

Il delegato, a cui è affidata la conservazione, sottoscrive un contratto o convenzione di servizio con il Comune di Sesto Fiorentino che deve prevedere l'obbligo del rispetto del presente T.U.

Il sistema di conservazione può essere costituito, per esigenze tecniche-operative, da più sotto-sistemi di conservazione.

I soggetti, persone fisiche o giuridiche, che svolgono il servizio di conservazione come delegati devono essere accreditati presso l'Agenzia per l'Italia Digitale, secondo la Circolare 29 dicembre 2011, n. 59.

La sottoscrizione digitale, necessaria per la corretta esecuzione del processo di conservazione, sarà apposta dai rappresentanti legali del delegato per la conservazione, ovvero da altri soggetti espressamente individuati dal delegato stesso.

I soggetti, cui è delegato il processo di conservazione, assumono il ruolo di responsabili del trattamento dei dati, come previsto dal Regolamento Europeo 679/2016, a seguito di esplicito atto di nomina adottato dal titolare dei dati; la trasmissione dei pacchetti di conservazione non può iniziare prima che detto atto venga formalizzato.

Nel caso di delega dell'attività di conservazione, l'Amministrazione provvede ad incaricare formalmente il delegato delle attività di conservazione e riversamento e nel contempo lo diffida dal comunicare o diffondere anche accidentalmente, gli eventuali dati personali comuni, sensibili e/o giudiziari presenti nei supporti oggetto di copia e di riversamento.

2.4. Produttori e utenti del sistema di conservazione

I ruoli di produttore e utente sono svolti indifferentemente da persone fisiche o giuridiche interne o esterne al sistema di conservazione, secondo il modello organizzativo scelto dal Comune di Sesto Fiorentino.

Il produttore, responsabile del contenuto del pacchetto di versamento, trasmette tale pacchetto al sistema di conservazione secondo le modalità operative di versamento condivise con il delegato per la conservazione.

L'utente richiede al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti del livello di autorizzazione attribuito dal RC. Tali informazioni vengono fornite dal sistema di conservazione secondo le modalità previste alla Sezione 4.

2.5. Responsabile della fascicolazione

Il Responsabile della fascicolazione, processo che va dall'apertura alla chiusura del fascicolo e al conseguente trasferimento del medesimo nell'archivio di deposito o al sistema di conservazione a norma, è il responsabile del procedimento amministrativo (RPA), o, se non nominato, il responsabile del Servizio cui sia conferito incarico di Posizione Organizzativa. In mancanza, il Dirigente del Settore o Responsabile di Unità Organizzativa Autonoma competente per materia.

Tutti i soggetti individuati al comma precedente operano tenendo conto dei principi e delle direttive di cui alla sezione 3 del presente T.U.

2.6. Struttura organizzativa dell'Ente

La struttura organizzativa, alla quale si collegano le funzioni, le responsabilità e gli obblighi dei diversi soggetti che intervengono nel processo di protocollazione, gestione dei flussi documentali e conservazione di cui al presente T.U. è pubblicata sul sito istituzionale dell'Amministrazione nella Sezione Amministrazione Trasparente – Organizzazione - Articolazione degli uffici (http://www.comune.sesto-fiorentino.fi.it/rete-civica/articolazione-degli-uffici), così come integrata dagli incarichi di funzioni dirigenziali e di posizione organizzativa pubblicati pubblicata sul sito istituzionale dell'Amministrazione nella Sezione Amministrazione Trasparente – Personale (http://www.comune.sesto-fiorentino.fi.it/rete-civica/personale).

SEZIONE 2

1. DOCUMENTI E MODALITA' DI GESTIONE

1.1. Documenti e modalità di gestione

Ai fini del processo di gestione documentale, il documento amministrativo è classificabile, in termini tecnologici, in:

- informatico ("rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti");
- analogico ("rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti").

Da un punto di vista operativo, il documento amministrativo è invece classificabile come:

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

Per quanto riguarda invece le modalità di gestione, la gestione informatica dei documenti è l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti.

1.2. Il documento amministrativo informatico

Il CAD definisce il documento informatico come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".
Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria e originale da cui è possibile effettuare, indifferentemente su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo, sottoscritti con firma digitale, hanno l'efficacia prevista dall'art. 2702 del codice civile.

Secondo quanto previsto dall'art. 40 del CAD "*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71*".

1.3. Il documento amministrativo analogico

Per documento analogico si intende "*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*", cioè un documento "*formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta, le immagini su film, le magnetizzazioni su nastro su supporto non digitale*". Può essere considerato analogico un documento amministrativo cartaceo predisposto con strumenti informatici (ad esempio, una lettera prodotta tramite un software di elaborazione testi) e poi stampato.
In quest'ultimo caso si definisce "originale" il documento cartaceo nella sua redazione definitiva, perfetta e autentica negli elementi sostanziali e formali, comprendente tutti gli elementi di garanzia e di informazione del mittente e del destinatario, stampato su carta intestata e dotato di timbro e firma olografa.

1.4. Documento ricevuto

La corrispondenza in ingresso può essere acquisita dall'Ente con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato:

- a mezzo posta elettronica, convenzionale o certificata;
- su supporti magnetico - ottici quale, ad esempio, CD ROM, DVD, floppy disk, pen drive, hard disk esterni, etc., consegnati direttamente con lettera d'accompagnamento cartacea o inviati per posta o corriere;
- tramite portale, spazio web dedicato, sistemi di condivisione dei file, social network, servizi VoIP.

Un documento analogico può essere recapitato:

- a mezzo posta ordinaria o corriere;
- a mezzo posta raccomandata;
- per telefax o telegramma;

• con consegna diretta all' UCP o a una delle UOP da parte dell'interessato o di persona delegata. In caso di consegna o ricezione a uffici diversi dal protocollo, il ricevente dovrà assicurare la protocollazione.

L'Ente opera conformemente al disposto dall'art. 45, c. 1, del CAD, in base al quale "*I documenti trasmessi da chiunque a una pubblica Amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale*".

L'Ente dà altresì attuazione all'art. 5 bis c. 1 del D.Lgs 82/2005, che prevede che "*la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese*".

Pertanto se un'impresa dovesse inviare documenti cartacei occorrerà respingerli con un diniego semplificato ai sensi dell'art. 2 c. 1 L. 241/90.

1.5. Documento inviato

I documenti informatici, con gli eventuali allegati, anch'essi informatici, sono inviati di norma per mezzo della posta elettronica certificata.

Il documento informatico può inoltre essere riversato su supporto digitale rimovibile in formato non modificabile, per l'invio al destinatario con altri mezzi di trasmissione.

Lo scambio di documenti ufficiali con altre Pubbliche Amministrazioni avviene esclusivamente, tranne dimostrata impossibilità tecnica, mediante l'utilizzo della posta elettronica certificata alle caselle censite da IPA o tramite il sistema INTERPRO della Regione Toscana o in cooperazione applicativa.

Per l'invio di documenti ufficiali ad altre Pubbliche Amministrazioni possono essere utilizzate caselle di posta elettronica certificate ulteriori rispetto a quelle censite in IPA fino al completamento e all'implementazione dell'indice stesso.

I documenti informali possono essere trasmessi anche a mezzo di posta elettronica ordinaria.

Al cittadino, fino all'entrata in vigore del "domicilio digitale", vengono inviati documenti analogici, a meno che non abbia accettato l'invio di documenti tramite posta elettronica certificata.

In ogni caso la dichiarazione da parte del cittadino del proprio indirizzo di posta elettronica certificata costituisce espressa accettazione dell'invio, tramite questo canale, degli atti e dei provvedimenti amministrativi ad esso relativi.

1.6. Documento interno formale

I documenti interni sono formati con tecnologie informatiche avvalendosi del sistema di gestione documentale o di altri strumenti in dotazione agli uffici dell'Ente.
Il documento informatico di rilevanza amministrativa giuridico-probatoria deve essere sottoscritto con firma digitale e viene scambiato tra diverse unità organizzative mediante il sistema di gestione documentale.
Il sistema di gestione documentale adottato è in grado di tracciare in modo immodificabile tutte le operazioni relative a una registrazione, con un meccanismo di attribuzione alla singola persona di documenti o annotazioni, fornendo i requisiti per l'identificazione informatica.

1.7. Documento interno informale

Il documento interno informale può essere trasmesso o mediante il sistema di gestione documentale o mediante posta elettronica ordinaria. Può non essere firmato digitalmente.

1.8. Copia informatica di documento analogico

La copia informatica di documento analogico viene formata mediante scansione, o, più raramente, attraverso foto digitale, generando un documento informatico con contenuto e forma identici a quelli dell'originale analogico.
La copia ha la stessa efficacia probatoria dell'originale, tranne nel caso cui la conformità all'originale non venga espressamente disconosciuta.
La dichiarazione di conformità all'originale:

1.1. certifica il processo di formazione della copia che garantisce la corrispondenza di forma e contenuto di originale e copia;

1.2. è attestata dal funzionario delegato dal Sindaco ad autenticare le copie o dal funzionario depositario dell'originale;

1.3. è sottoscritta con firma digitale;

1.4. viene inserita nel documento informatico contenente la copia informatica oppure può essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta (hash) di ogni copia.

Esempio

Il sottoscritto ___, nella sua qualità di_____, attesta che la presente copia analogica composta da n. ……. fogli è conforme all'originale informatico, sottoscritto con firma digitale, il cui certificato è intestato al Sig. ..... rilasciato da ..... n..... valido fino al ..... e non revocato, la cui verifica ha avuto esito positivo.

Il Funzionario incaricato

Firmato digitalmente

1.9. Copia analogica di documento informatico

Si tratta dell'attestazione di conformità di un documento cartaceo al documento informatico da cui proviene.

La confomizzazione consiste nell'attestazione di conformità di tutte le sue componenti:

1. software di creazione
    1. tipologia di firma elettronica utilizzata con indicazione del certificato e del titolare
    2. indicazione degli strumenti di verifica
    3. eventuale marcatura temporale e strumento di verifica della stessa

Le copie e gli estratti su supporto analogico del documento informatico, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta.

Esempio:

Il sottoscritto ___, nella sua qualità di_____, attesta che la presente copia analogica del documento informatico sopra riportato è stata prodotta mediante l'utilizzo di un sistema di gestione documentale conforme alla normativa vigente alla data odierna e garantisce la corrispondenza di forma e contenuto all'originale.

Il Funzionario incaricato

1.10. Copie ed estratti informatici di documenti informatici

Le copie e gli estratti informatici dei documenti informatici sono normalmente prodotti attraverso il sistema di gestione documentale, che utilizza i formati descritti nel presente T.U., nonché mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico d'origine. Copie ed estratti hanno dunque la stessa efficacia probatoria dell'originale se la conformità non è espressamente disconosciuta. La copia e l'estratto riportano la seguente formula:

Copia/estratto di documento informatico prodotto con sistema di gestione documentale del Comune di Sesto Fiorentino, conforme alle regole tecniche vigenti (D.P.C.M. 14 novembre 2014)

Se la copia e gli estratti informatici dei documenti informatici non possono essere prodotti attraverso il sistema di gestione documentale, in calce alle copie ed estratti informatici viene inserita l'attestazione di conformità all'originale delle copie o dell'estratto informatico sottoscritta con firma digitale dal funzionario delegato dal Sindaco.

Esempio:

Il sottoscritto, nella sua qualità di_____, attesta che la copia / l'estratto informatico sopra riportato è conforme all'originale informatico.

Il Funzionario Incaricato
Firmato digitalmente

1.11. Duplicati di documenti informatici

Il duplicato un documento informatico è un documento informatico risultante dall'utilizzo di un software specifico composto dalla stessa sequenza di bit del documento di origine, cioè un nuovo esemplare dello stesso documento. Il duplicato viene prodotto:

- sullo stesso sistema di memorizzazione: stesso PC o dispositivo mobile;
- su altro sistema di memorizzazione: ad esempio da PC a dispositivo mobile (CD ROM, chiavetta USB, …).

I duplicati prodotti dal presente sistema di gestione documentale, conforme alle regole tecniche vigenti in materia di formazione, copia, duplicazione, riproduzione e validazione, conservazione dei documenti informatici amministrativi (D.P.C.M. 14 novembre 2014), sono costituiti dalla la stessa sequenza di bit del documento informatico di origine e pertanto hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti.

Se i duplicati non sono prodotti dal sistema di gestione documentale (eventualmente attraverso il sistema di conservazione sostituiva, se dovesse essere necessario ricorrervi), ai duplicati viene allegata un'attestazione di conformità relativa al processo di formazione del duplicato che assicura l'identità della sequenza di bit del duplicato rispetto all'originale.

Esempio:

Il sottoscritto, nella sua qualità di_____, attesta che l'allegato duplicato informatico è conforme all'originale.

Il Funzionario Incaricato
Firmato digitalmente

1.12. Formazione del documento informatico

I documenti dell'Amministrazione sono prodotti con sistemi informatici, ai sensi dalla normativa vigente.

E' necessario che ogni documento formato per essere destinato sia all'esterno che all'interno in modo formale sia completo, ovvero tratti un unico argomento, indicato in maniera sintetica ma esaustiva, in un campo "oggetto" e faccia riferimento ad un solo fascicolo, almeno in via principale. In caso di riutilizzazione per altri fascicoli, si dovrà comunque citare il fascicolo per il quale è stato originariamente creato.
Le firme devono essere apposte prima della protocollazione del documento; è sempre consentito generare e spedire una copia di cortesia non firmata, chiaramente senza valore giuridico probatorio.

Per ciò che concerne la formazione, le caratteristiche di immodificabilità, integrità, ecc., si fa riferimento all'art. 3 del DPCM del 13 novembre 2014, con particolare attenzione all'insieme minimo di metadati.

1.13. La firma

Nell'ambito del sistema di gestione documentale, il Comune di Sesto Fiorentino utilizza le seguenti tipologie di firma:

Firma semplice: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica in forma di Username e Password.
La firma semplice viene utilizzata per l'autenticazione a fini di consultazione e accesso all'erogazione di servizi:

- interni dell'Ente per l'utilizzo delle procedure documentali dei software applicativi secondo i diversi livelli di autorizzazione (amministratore, operatore, limitato alla consultazione);
- di download di documentazione dal sito dell'Ente.

Non ha valore di sottoscrizione.
La firma semplice viene rilasciata a tutti gli operatori del sistema di gestione documentale.

Firma digitale: costituita da un certificato qualificato e da sistema di chiavi crittografiche, una pubblica e una privata, consente di rendere manifesta e di verificare la provenienza e l'integrità di uno o più documenti informatici. Si utilizza con dispositivi quali token, smart card, firma remota e firma automatica.
In relazione al valore legale di firma autografa e sottoscrizione, garantisce, oltre alla provenienza, anche l'integrità e l'autenticità del documento sottoscritto; inoltre sostituisce l'apposizione di timbri e sigilli.
Viene utilizzata per la firma di provvedimenti con effetto costitutivo, modificativo o estintivo di rapporti giuridici, sia di natura pubblicistica (delibere, decreti, determinazioni, ordinanze, buoni di ordinazione, ordinativi di incasso e pagamento, documenti finanziari e contabili,

pareri, etc) che privatistica e contrattuale (contratti, ordini, contabilizzazioni di lavori pubblici), che verranno versati nel sistema di conservazione.
La firma digitale viene rilasciata a tutti i RPA anche con delega all'adozione di provvedimenti, ai Responsabili di Servizio e a tutti gli operatori legittimati alla sottoscrizione di documenti aventi rilevanza esterna.

Firma autografa e timbro: su documenti analogici e copie analogiche di documenti informatici.

1.14. Autenticazione della firma

L'autenticazione delle firme è prevista per la firma autografa e viene effettuata da un pubblico ufficiale (Segretario Comunale o funzionario incaricato dal Sindaco) che attesta, con la propria firma, che la firma sia stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale.
Se al documento informatico autenticato deve essere allegato un altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata.

1.15. Immodificabilità ed integrità del documento informatico, copie, duplicati ed estratti

L'immodificabilità e l'integrità di documento informatici, copie, duplicati ed estratti viene assicurata mediante:
a) conversione in formato privo di contenuti dinamici quali PDF/A o altri formati aventi pari caratteristiche ed elencati nel presente T.U.;
b) sottoscrizione con firma digitale;
c) apposizione di una marca temporale;
d) trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
e) memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
f) versamento ad un sistema di conservazione.

Al documento, una volta reso immodificabile, deve essere associato l'insieme minimo dei metadati previsto dal presente T.U.

1.16. Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- la certificazione dell'avvenuto inoltro e ricezione;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno dell'Ente;
- l'interconnessione tra le unità organizzative dell'Ente nel caso di documenti interni.

1.17. Uso della Posta Elettronica Certificata

L'Ente dispone di caselle di Posta Elettronica Certificata istituzionali per la corrispondenza, sia in ingresso che in uscita.
Le caselle PEC del Comune di Sesto Fiorentino sono pubblicate sull'Indice delle Pubbliche Amministrazioni (IPA).
La casella del Protocollo costituisce l'indirizzo virtuale dell'Ente e di tutti gli uffici che lo formano ad ogni fine di legge.
Tutte le PEC che pervengono agli indirizzi dell'Ente devono comunque essere immediatamente protocollate, esclusi i casi di cui all'allegato B del presente T.U..

L'utilizzo della Posta Elettronica Certificata (PEC), o di altro sistema analogo che dovesse rendersi disponibile, consente di:

- garantire l'avvenuta consegna;
- certificare in modo inequivocabile la data e l'ora di trasmissione;
- interoperare con altre PA.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato, in maniera esplicita o

attraverso siti ufficiali quali Indice PA, Consigli di ordini professionali, Camere di Commercio, Ministero degli esteri e simili.
La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale all'invio di posta raccomandata con avviso di ricevimento, salvo diversa disposizione di legge.

Le comunicazioni provenienti dai cittadini possono anche essere trasmesse all'indirizzo di posta elettronica ordinaria. Le istanze e le dichiarazioni presentate all'Ente che abbiano contenuto giuridico probatorio tuttavia producono i loro effetti soltanto dopo la loro protocollazione.

1.18. Interoperabilità dei sistemi di protocollo informatico

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattare in modalità automatica, da parte di un sistema di protocollo ricevente, le informazioni trasmesse da un sistema di protocollo mittente, allo scopo di rendere automatiche le attività di registrazione e i processi amministrativi che ne conseguono (ad esempio il sistema INTERPRO della Regione Toscana).
Per realizzare l'interoperabilità dei sistemi di protocollo informatico all'interno delle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

2. ORGANIZZAZIONE DELL'ENTE E DEL PROTOCOLLO

2.1. Aree organizzative omogenee

Ai fini della gestione del protocollo e relativo flusso documentale, l'Amministrazione individua un'unica Area amministrativa Omogenea, denominata "Comune di Sesto Fiorentino".

2.2. Accreditamento dell'Ente all'IPA

Nell'ambito degli adempimenti previsti dalla normativa vigente, l'Ente si è accreditato presso l'Indice delle Pubbliche Amministrazioni (IPA) fornendo le seguenti informazioni che individuano l'Amministrazione stessa e le AOO in cui è articolata:

- la denominazione della Amministrazione;
- il codice identificativo proposto per l'Amministrazione;
- l'indirizzo della sede principale dell'Amministrazione;
- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:
  - della denominazione;
  - del codice identificativo;
  - della casella di posta elettronica;
  - del nominativo del RPF;
  - della data di istituzione;
  - dell'eventuale data di soppressione;
- l'elenco degli UOR dell'AOO;
- i dati relativi alla fatturazione elettronica.

Ogni variazione è comunicata tempestivamente all'IPA dal Responsabile dei Servizi Informatici.

2.3. Il protocollo informatico

Il protocollo fa fede, con effetto giuridico di fede privilegiata, dell'effettivo ricevimento o spedizione di un documento. I documenti elettronici e/o informatici inviati all'Amministrazione tramite posta elettronica certificata si considerano ricevuti dall'Ente, a ogni effetto giuridico, nel caso in cui il mittente riceva nella propria casella di PEC le ricevute di avvenuta accettazione e consegna inviate dai gestori della PEC.

L'Ente gestisce un unico protocollo informatico per tutti i documenti in arrivo e in partenza nell'ambito di un sistema di gestione documentale conforme alle previsioni di cui:

- alle Regole Tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57 bis e 71 del CAD di cui al D.Lgs n. 82/, approvate con D.P.C.M. 3 dicembre 2013;
- al Testo Unico sulla documentazione amministrativa approvato con D.P.R. 445/2000.

Il registro di protocollo è generato automaticamente dal sistema, che assegna a ciascun documento registrato un numero progressivo e la data di protocollazione, e provvede a salvare tutte le informazioni relative.
Al sistema di protocollazione corrisponde un unico titolario di classificazione, allegato quale parte integrante al presente T.U. (allegato A).
L'Ente produce un unico archivio elettronico. La ripartizione in archivio corrente, archivio di deposito e archivio storico corrisponde a diversi contrassegni elettronici del sistema.
I RPA provvedono all'implementazione della fascicolazione della corrispondenza in arrivo e alla protocollazione e fascicolazione della corrispondenza in partenza. Gestiscono e custodiscono i documenti dell'archivio corrente.

Nell'ambito della gestione dei flussi documentali, il sistema di protocollo si compone di:

- risorse archivistiche: piano di classificazione o titolario (allegato A);
- risorse informatiche: software applicativo e piattaforma documentale gestita dalla suite Sicraweb, PEC e posta elettronica ordinaria, piattaforme di interscambio;
- risorse umane: a) operatori dell'Unità Organizzativa Centrale di registrazione di Protocollo e RPF, che opera con la collaborazione del Responsabile dei Servizi Informatici e con il RC; b) operatori dell'Ente, appartenenti a Unità Organizzative di registrazione di Protocollo, cui sono attribuiti compiti di protocollazione in entrata e in uscita, secondo la logica del "protocollo distribuito" descritto di seguito.

2.4. Classificazione dei documenti

Tutti i documenti spediti, ricevuti, interni devono essere classificati, in base all'argomento trattato, secondo uno schema che identifica attività e materie specifiche come definito nel titolario di classificazione.
Lo scopo del titolario di classificazione è quello di ripartire i documenti a seconda delle competenze istituzionali dell'Ente e non a seconda della struttura organizzativa vigente.

2.5. Tutela dei dati

Il titolare dei dati di protocollo e dei dati personali in esso contenuti è l'Ente quale persona giuridica ed organo istituzionale.

Relativamente agli adempimenti esterni, il Comune di Sesto Fiorentino si è organizzato per garantire che i certificati rilasciati, nonché le informative ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

Le registrazioni di protocollo non sono accessibili da parte di soggetti esterni, pubblici o privati, ad eccezione dei fornitori dei software Sicraweb e degli altri software che si interfacciano con il sistema di protocollo informatico e di gestione documentale dell'Ente.

Tali soggetti sono nominati responsabili del trattamento dal titolare.

2.6. Diffusione dei dati personali

Fatto salvo quanto previsto dal D. Lgs. 33/2013 e successive modifiche e integrazioni, per quanto concerne la diffusione dei dati personali l'Ente applica quanto previsto dal Regolamento UE 679/2016, dal D. Lgs. 196/2003 e successive modifiche e integrazioni e dai provvedimenti del Garante della privacy.

Il Comune di Sesto Fiorentino diffonde i dati personali, esclusivamente ove consentito dal Regolamento UE 679/2016 o da altra specifica norma di legge o di regolamento.

Per quanto riguarda i documenti a pubblicazione obbligatoria che non contengano dati sensibili, è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti sia realmente necessaria e proporzionata al raggiungimento delle finalità perseguite dall'atto (c.d. "principio di pertinenza e non eccedenza").

I dati sensibili e giudiziari possono essere diffusi solo nel caso in cui la diffusione sia prevista da una espressa disposizione di legge e possono essere trattati solo qualora siano in concreto "indispensabili" per svolgere l'attività istituzionale, non potendo questa essere adempiuta mediante l'utilizzo di dati anonimi o di dati personali di natura diversa.

E' del tutto vietata la diffusione di "dati idonei a rivelare lo stato di salute".

2.7. Pubblicazione dei documenti all'Albo Pretorio e sul sito web istituzionale e tecniche di anonimizzazione dei dati

Le informazioni relative a dati sensibili e/o giudiziari e le informazioni che, pur non contenendo dati sensibili, sono tali da rivelare la situazione di disagio economico-sociale degli interessati sono pubblicate ricorrendo alle tecniche di anonimizzazione sotto elencate.

Per procedere alla anomizzazione è possibile alternativamente, in relazione a quanto previsto dalla normativa di settore e alle esigenze di tutela che si riscontrano nel caso specifico:

a) oscurare i dati su originale cartaceo e pubblicare la relativa scansione (tecnica unica da seguire per la pubblicazione on line di ordinanze contenenti TSO);
b) menzionare i dati solo in documenti allegati quale parte integrante non pubblicati, a disposizione degli uffici e consultabili, sussistendone le condizioni di cui alla normativa vigente, solo da interessati e controinteressati;
c) fare riferimento ai dati solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici.

In generale è necessario fare ricorso a procedure in virtù delle quali *i dati personali non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile* (art. 4 Reg.UE 679/2016).

La responsabilità del rispetto di quanto sopra indicato fa carico al RPA o, se non nominato, il responsabile del Servizio cui sia conferito incarico di Posizione Organizzativa. In mancanza, il Dirigente del Settore o Responsabile di Unità Organizzativa Autonoma competente per materia.

La necessità di non pubblicare i dati deve essere indicata ex ante nel software di gestione degli atti o in quello di gestione dell'Albo pretorio on line.

2.8. Requisiti minimi di sicurezza

Il sistema di gestione documentale e di protocollo informatico assicura:

a) l'univoca identificazione ed autenticazione degli utenti;
b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;

d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione;
e) l'univoca identificazione dei documenti;
f) il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
g) il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Le registrazioni di cui sopra protette da modifiche non autorizzate.

Viene in ogni caso garantito, secondo la normativa vigente, il diritto dei cittadini e delle imprese a ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conforme al rispetto dei diritti, delle libertà fondamentali, della dignità dell'interessato e della riservatezza.

2.9. Formazione del personale

Stante la quantità di dati trattati, anche di natura sensibile e ultra sensibile, è indispensabile che il personale addetto specificamente al protocollo e tutti gli operatori che possono accedere a esso e ai relativi flussi documentali siano resi consapevoli della delicatezza dell'incarico, dei vincoli di segretezza, della normativa vigente e della sua evoluzione. Vengono pertanto organizzati periodicamente corsi di formazione al fine di istruire il personale e consentirgli di operare in modo autonomo, consapevole e conforme alle direttive e normative.

3. FLUSSI DOCUMENTALI

3.1. Introduzione

I documenti possono essere ricevuti e inviati secondo diverse modalità. In ogni caso devono essere protocollati, in ingresso e in uscita, dagli addetti all'UCP o dall'addetto all'UOP, che si occupa della protocollazione.

In linea di principio, tranne le eccezioni di cui all'art. 53 c. 5 D.P.R. 445/2000 e i documenti riportati nell'allegato B) parte integrante del presente T.U., devono essere protocollati tutti i documenti che arrivano, incluse le istanze palesemente infondate. Solo nel caso in cui il destinatario sia chiaramente un altro Ente, si potrà respingere il documento al mittente senza procedere alla protocollazione.

3.2. Formati dei documenti digitali in entrata e in uscita

In particolare, i formati accettabili sono i seguenti:

- Documenti di testo: Pdf/A, docx/OOXM, ODT
- Calcolo: xls, xslx, ods
- Immagini raster: BMP TIFF, JPEG, PNG
- Immagini vettoriali: DXF, Shapefile, SVG, DWG
- File audio: MP3
- File video: MPEG4
- File archivio: .zip e .rar
- File non binari "in chiaro": XML e i suoi derivati
- TXT con specifica della codifica del carattere adottata (Character Encoding)
- Messaggi di posta elettronica Eml e tutti i formati conformi allo standard RFC 2822/MIME

I formati non indicati, ma che rispettino i requisiti di "apertura", sicurezza, "portabilità", etc, sono consentiti se concordati in un contratto o accordo di servizio.
I documenti sottoscritti digitalmente e la marcatura temporale sono rispettivamente accettati nei formati P7M (CAdES), PAdES, XAdES e TSR, TSD.
Per quanto concerne le dimensioni dei documenti da inviare tramite PEC la dimensione complessiva dei file da trasmettere con un unico invio non possono essere superiori a 100 Megabyte (MB).

3.3. Documenti in entrata

I documenti possono pervenire attraverso:

a) le caselle di posta elettronica certificata;
b) le caselle di posta elettronica ordinaria;
c) il portale web dell'Ente;
d) i servizi on line;
e) il servizio postale;
f) con consegna diretta all' UCP o agli UOP da parte degli utenti;
g) tramite telefax, ove non vi siano espresse esclusioni.

3.4. Ricezione, protocollazione e smistamento

La corrispondenza in arrivo genericamente indirizzata al Comune è ricevuta di norma dall'UCP, a eccezione di quella pervenuta tramite posta elettronica ordinaria, consegna a mano o telefax ad altri UOP dell'Ente, disciplinata nel dettaglio nei paragrafi seguenti.
Ricevuto un documento, l'UCP procede a protocollarlo con la massima celerità e comunque non oltre il giorno successivo alla ricezione, avendo cura comunque di indicare la data di arrivo corretta.
Nel caso in cui la protocollazione avvenga successivamente alle 24 ore rispetto alla data di ricezione del documento, l'UCP o gli UOP devono specificare nella sezione NOTE del software di gestione il motivo del ritardo. E' comunque ammessa la registrazione differita, alle sole condizioni indicate nel presente T.U.
Se il documento ricevuto è di tipo cartaceo, l'UCP procede alla sua scansione.

Il documento deve essere assegnato al Settore o al Servizio o all'Ufficio che ha competenza sull'oggetto specificato nel documento.
L'assegnazione del documento ad un singolo dipendente di norma non deve essere effettuata, salvo il caso di documenti riservati. In questo caso l'UCP avvisa il destinatario telefonicamente o tramite mail.
Nel caso di un unico documento indirizzato a più soggetti o più Servizi, l'UCP lo invia a tutti i destinatari indicati.
Nel caso in cui il documento sia stato inviato al Comune di Sesto Fiorentino, esclusivamente per conoscenza, non avendo l'Ente alcun obbligo di provvedere al riguardo, il documento è comunque assegnato per competenza all'ufficio cui afferisce la materia oggetto della comunicazione.

Il Settore, il Servizio o l'Ufficio competente ha notizia dell'arrivo del documento tramite il sistema di gestione del protocollo e dei flussi documentali; la notifica è generata automaticamente dal sistema.
Il documento viene preso in carico da un operatore autorizzato appartenente al Settore, al Servizio o all'Ufficio e viene gestito all'interno del suo fascicolo digitale.
Gli appartenenti al Settore o al Servizio possono smistare il documento alle unità organizzative di livello inferiore (il Settore può smistare ai servizi che ne fanno parte, il Servizio agli uffici sottostanti).

Al fine di evitare disguidi e ritardi nella gestione della corrispondenza, ciascun Settore, Servizio o Ufficio deve segnalare con la massima tempestività all'UCP eventuali documenti pervenuti erroneamente, in modo tale che sia possibile procedere alla riassegnazione a un Settore, Servizio o Ufficio diverso entro il minor tempo possibile.
Allo stesso modo ciascun Settore o Servizio deve segnalare con la massima tempestività al RPF e all'UCP eventuali variazioni nelle proprie competenze, al fine di evitare errori nell'assegnazione dei documenti pervenuti.

3.5. Ricezione di documenti sulle caselle di posta elettronica certificata

Le comunicazioni di documenti tra le Pubbliche Amministrazioni, professionisti e imprese avvengono mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza, come previsto dall'art. 47 del CAD.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le AOO e associate ai documenti protocollati.

L'unica modalità tramite la quale far pervenire quei documenti per i quali è richiesta la pubblicazione all'Albo Pretorio on line dell'Ente è la posta elettronica certificata. Nel caso di documenti inviati a mezzo PEC per la pubblicazione all'Albo Pretorio Comunale, la

conferma di pubblicazione viene trasmessa al mittente attraverso lo stesso canale, successivamente alla scadenza della pubblicazione richiesta.

Ogni messaggio deve riferirsi a una sola questione. Anche nel caso in cui vengano inviati contestualmente più documenti, deve essere possibile attribuire all'invio un'unica protocollazione e un'unica classificazione.
Quando i documenti informatici pervengono all'UCP, esso verifica la provenienza della PEC, la validità di eventuali firme e la leggibilità del messaggio e di eventuali allegati, quindi - se l'esito dei controlli è positivo - procede alla protocollazione e al successivo smistamento. Quando la PEC arriva direttamente al Settore, Servizio o Ufficio di destinazione, esso procede autonomamente alle operazioni di cui sopra.

Resta fermo quanto riportato nell'allegato B) relativamente ai documenti esclusi dalla registrazione di protocollo.
Il sistema di gestione del protocollo e dei flussi documentali adottato dall'Ente rende disponibili i documenti ricevuti per via telematica appena completata l'operazione di classificazione e smistamento.
La ricezione di documenti attraverso la casella di posta certificata comporta automaticamente la notifica al mittente dell'avvenuto recapito al destinatario, assicurata dallo stesso servizio di posta certificata.
Nel caso di invio di documenti tramite PEC, l'UOP invia al destinatario la comunicazione, generata automaticamente dal sistema, del numero di protocollo attribuito.

Le caselle PEC sono controllate al momento dell'ingresso al lavoro e poi successivamente più volte nel corso della giornata lavorativa dal personale assegnato all'UCP e almeno giornalmente dal personale assegnato ai singoli UOP dell'Ente, ognuno nell'ambito delle proprie competenze.

3.6. Ricezione di documenti sulla casella di posta elettronica ordinaria

Le comunicazioni pervenute attraverso posta elettronica ordinaria non sono considerate valide ai fini del procedimento amministrativo fino al momento del loro inserimento nel

sistema di gestione dei flussi documentali e alla loro protocollazione e sempre che ne sia verificata la provenienza, secondo quanto previsto dall'art. 47 del CAD.

Spetta al ricevente valutarne l'attendibilità, con particolare attenzione a messaggi che possono contenere virus o altri malaware, che dovranno essere immediatamente cancellati ed eliminati anche dal cestino virtuale.

Non sono normalmente previste ricevute, ma si darà conferma di lettura, se richiesta, o si comunicheranno gli estremi del protocollo, se richiesti.

3.7. Ricezione di documenti informatici dal portale web istituzionale o dai servizi on line

I documenti digitali possono anche essere ricevuti o formati direttamente tramite il sito internet istituzionale o i servizi on line. In questo caso il servizio dovrà essere configurato per rilasciare una ricevuta elettronica di presa in carico, oppure un messaggio di errore, nel caso in cui l'operazione non vada a buon fine.

3.8. Ricezione di documenti cartacei a mezzo posta, corriere o per consegna a mano

I documenti pervenuti a mezzo servizio postale o tramite corriere sono consegnati all'UCP.
La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta, e contestualmente protocollata.
Qualora non fosse possibile procedere alla protocollazione nel giorno stesso della ricezione, ad esempio perché la posta viene consegnata in corrispondenza del termine dell'orario lavorativo, si procederà il giorno seguente, avendo cura comunque di indicare la data di arrivo corretta.
Nelle raccomandate A/R compilate a cura degli UOP deve essere indicato il numero di protocollo in uscita.
Le ricevute di ritorno della posta raccomandata sono scansionate e inserite nel sistema di gestione documentale.

I documenti consegnati a mano o inviati tramite telefax agli UOP sono protocollati direttamente dal personale assegnato all'UOP, cui fa carico anche la scansione e l'inserimento nel sistema di gestione documentale.

Quando il documento è consegnato a mano ed è richiesto il rilascio di una ricevuta, l'UCP o l'UOP rilasciano la ricevuta generata automaticamente dal sistema di protocollo.
Qualora non sia possibile il rilascio della ricevuta, l'UCP o l'UOP appongono un timbro o un'etichetta sulla copia della prima pagina del documento (o sulla fotocopia della busta chiusa), con gli estremi della registrazione di protocollo.

Possono essere esclusi dalla registrazione di protocollo i documenti indicati nell'allegato B) al presente T.U.

Al di fuori di queste categorie, non sono consentite eccezioni all'obbligo di protocollazione, segnatura e corretta gestione dei documenti.

Il ritiro della corrispondenza cartacea pervenuta deve essere effettuato a cura del personale dei Servizi dell'Ente presso l'UCP entro le ore 11.00 di ogni giorno lavorativo.

3.9. Ricezione di documenti informatici su supporti rimovibili

In analogia con quanto disposto ai paragrafi precedenti, i contenuti dei supporti rimovibili vengono protocollati e inseriti nel flusso documentale se provenienti da fonti attendibili. Se ritenuti spam o comunque pericolosi, non vengono protocollati e della mancata protocollazione l'UCP o l'UOP danno comunicazione al mittente.

3.10. Smistamento dei documenti interni

Lo smistamento dei documenti interni non soggetti a protocollazione avviene a cura di ogni Servizio, utilizzando:

- nel caso di documenti cartacei, gli appositi spazi fisici dedicati all'interno dell'UCP.;

- nel caso dei documenti elettronici o informatici, il sistema di gestione documentale o la posta elettronica ordinaria.

3.11. Casi particolari

3.11.1. Documenti relativi a gare o bandi

I Servizi che curano la gestione dei procedimenti relativi alle gare e ai bandi devono tempestivamente, di norma almeno 3 giorni prima del presunto arrivo delle offerte e/o domande, comunicare all'UCP l'oggetto della gara/bando, la relativa scadenza e l'Ufficio competente a ricevere la documentazione.

Per quanto riguarda le procedure di gara, la corrispondenza riportante l'indicazione "offerta" - "gara d'appalto" o simili, o comunque dal cui aspetto si evince la partecipazione ad una gara, non deve essere aperta al momento dell'arrivo. Questo tipo di corrispondenza viene protocollata con l'apposizione del numero di protocollo e della data di registrazione (eventualmente integrata con l'orario di arrivo) direttamente sulla busta, plico o simili, ed è inviata al RPA, che successivamente dovrà riportare gli estremi di protocollo contenuti sulla busta, plico o simili, mantenendo comunque la busta come allegato.

3.11.2. Corrispondenza personale

La corrispondenza personale cartacea non deve essere aperta né protocollata, ma consegnata integra al destinatario. Qualora questi riscontri che si tratta di una questione istituzionale, provvede a protocollarla e a inserirla nel sistema di gestione dei flussi documentali. In alternativa può consegnarla all'UCP per la registrazione e l'inserimento nel sistema.

3.11.3. Documenti di assegnazione complessa

Quando non sia chiaro l'oggetto del documento e quindi non sia possibile effettuare correttamente l'assegnazione, l'UCP effettua una verifica con il RPF e con i vari RPA prima

di procedere alla protocollazione. Se non è possibile ottenere un chiarimento entro il giorno lavorativo successivo alla ricezione, procede comunque alla protocollazione, indicando la data di effettivo ricevimento, sotto la categoria "oggetti diversi". L'UCP comunica a tutti gli uffici attraverso posta interna l'oggetto del documento e il numero di protocollo, in modo tale da poter procedere alla corretta assegnazione.

3.11.4. Documenti privi di firma o anonimi

I documenti privi di sottoscrizione, ma di cui sia indicato l'autore sono soggetti a registrazione di protocollo.

I documenti dei quali non è possibile identificare l'autore sono soggetti a registrazione di protocollo per testimoniarne l'arrivo, indicando "ANONIMO" nel campo del mittente.

3.11.5. Documenti di competenza di altre amministrazioni o di altri soggetti

Qualora pervenga all'UCP un documento di competenza di un altro Ente o altra persona fisica o giuridica, questo è restituito al mittente a cura dell'UCP.

Nel caso in cui un documento della fattispecie sia stato erroneamente protocollato, la registrazione di protocollo viene annullata con la dicitura "pervenuto erroneamente".

3.12. Protocollazione in uscita

L'Ente non produce, salvo casi di comprovata necessità approvati dal RPF, originali cartacei, ma forma tutti i documenti in modalità elettronica, utilizzando il formato e il software più opportuno per la tipologia del documento da generare.

Tutti i documenti in uscita vengono protocollati, direttamente dall'UOP competente, sia che restino in forma elettronica, sia che vengano resi cartacei. Il documento elettronico viene inserito nel fascicolo, insieme agli altri documenti che lo formano.

Ogni UOP è autorizzato dal RPF a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita, provvedendo quindi ad eseguire direttamente le verifiche di conformità della documentazione da inviare.

3.13. Gestione della corrispondenza in partenza attraverso il "Protocollo Distribuito"

Ogni UOP provvede alla registrazione di protocollo della corrispondenza da inviare, nonché alla predisposizione e consegna all'UCP dei documenti cartacei da postalizzare.

3.13.1. Documenti informatici

La trasmissione telematica a Pubbliche Amministrazioni di comunicazioni avviene mediante l'utilizzo della posta elettronica certificata alle caselle censite da IPA o tramite il sistema INTERPRO di Regione Toscana o in cooperazione applicativa.

La PEC è strumento ordinario di trasmissione anche verso i cittadini che hanno dichiarato il proprio domicilio digitale, nonché verso imprese e professionisti iscritti ad ordini professionali.
Qualora un documento protocollato sia inviato a più destinatari, è possibile, se non ci sono ragioni per le quali i destinatari non debbano conoscere chi sono gli altri riceventi, inviare un'unica PEC a tutti gli indirizzi. In questo caso la ricevuta di accettazione sarà unica, mentre le ricevute di consegna saranno tante quanti sono i destinatari. Diversamente, si genereranno tante PEC distinte, una per ogni destinatario.
In alternativa alla PEC si possono considerare altri mezzi (condivisione, social network, VoIP, upload su siti web, …), purché siano in grado di fornire una ricevuta, se richiesta, oppure vengano utilizzati per comunicazioni informali, o per anticipare comunicazioni formali recapitate con altri mezzi.

Nel caso di trasmissione di allegati al documento che eccedano la capienza della casella di posta elettronica, è possibile utilizzare supporti rimovibili, o avvalersi di strumenti informatici diversi.

3.13.2. Documenti cartacei

La corrispondenza cartacea in partenza, già protocollata dall'UOP, deve essere consegnata all'UCP in busta chiusa completa dell'indirizzo del destinatario con l'indicazione della modalità di invio (posta prioritaria o raccomandata) e con la "distinta" accompagnatoria della corrispondenza da inviare. Nel caso di raccomandata con avviso di ricevimento sulla busta deve anche essere indicato il fascicolo cui si riferisce il documento e l'ufficio mittente.

La corrispondenza in partenza deve in ogni caso essere consegnata all'Ufficio Protocollo entro le ore 11.30 al fine di assicurare la spedizione nella stessa giornata di consegna. La corrispondenza consegnata dopo l'orario indicato viene postalizzata il primo giorno lavorativo successivo.

In caso di invii massivi di corrispondenza, è opportuno avvertire l'UCP almeno due giorni lavorativi prima della data di spedizione prevista.

In casi particolari può essere effettuata la spedizione a mezzo corriere, a cura dei singoli UOP.

3.13.3. Documenti informali

Si considerano informali quei documenti che non hanno valore giuridico o amministrativo all'interno dei procedimenti (informazioni, suggerimenti, richieste preliminari informali intese come propedeutiche all'avvio di procedimenti, pubblicità, ecc).
Gli scambi di documenti informali, all'interno dell'Ente o verso l'esterno, non danno luogo a protocollazione, ma possono essere registrati nel programma informatico di gestione dei flussi documentali.

4. REGISTRAZIONI DI PROTOCOLLO

4.1. Unicità del protocollo

Il registro di protocollo è un atto pubblico di fede privilegiata - ovvero si considera valido fino a querela di falso - che attesta l'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.
Il registro di protocollo è unico ed è solamente informatico, fatta salva la procedura per la registrazione di emergenza. Unica è anche la numerazione progressiva delle registrazioni; si chiude al 31 dicembre di ogni anno e ricomincia dal 1° gennaio dell'anno successivo.
Il numero di protocollo individua un unico documento; pertanto ogni documento riporta un unico numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche; se sono riportate manualmente cifre più brevi si intendono implicitamente anteposti tanti zeri quanti ne occorrono per arrivare a sette.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo. 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 avvenga per errore, la seconda protocollazione deve essere annullata.

Qualora si rinvenga un documento ricevuto, ma erroneamente non protocollato, l'UCP o gli UOP procedono immediatamente alla sua protocollazione, indicando, se nota, la data di effettivo ricevimento. Il Responsabile del Servizio, che non ha effettuato la protocollazione, è tenuto ad adottare le misure più opportune per evitare il ripetersi dell'errore.

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

4.2. Registrazione di protocollo

Le regole di registrazione del protocollo sono valide per tutti i tipi di documenti trattati dall'Ente che siano ricevuti, inviati o interni formali, tanto digitali quanto analogici.
Su ogni documento ricevuto o spedito dall'Ente, ad esclusione dei documenti indicati nell'allegato B), è effettuata una registrazione di protocollo mediante il sistema informatico, consistente almeno nella memorizzazione dei dati obbligatori.
Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive.

4.3. Elementi obbligatori delle registrazioni di protocollo

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori ai sensi dell'art. 53 del D.P.R. n. 445/2000:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

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

4.4. Elementi facoltativi delle registrazioni di protocollo

Gli elementi obbligatori indicati dal punto precedente sono integrati dall'ufficio di assegnazione.

Il RPF, con proprio provvedimento motivato, al fine di migliorare la gestione, la ricerca e la conservazione dei documenti, può modificare ed integrare gli elementi facoltativi del protocollo, anche per singole categorie o tipologie di documenti, in accordo con i Responsabili dei Servizi.

La registrazione degli elementi facoltativi del protocollo, previa autorizzazione del RPF, può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOP o dell'UCP. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

4.5. Segnatura di protocollo dei documenti

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

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile.

Le informazioni previste sono:

- l'identificazione in forma sintetica o estesa dell'Amministrazione;
- l'anno solare di riferimento del protocollo;
- titolo e classe di riferimento;
- il numero progressivo di protocollo, costituito da almeno sette cifre numeriche;
- la data di protocollo.

Per i documenti analogici, le informazioni sopra riportate vengono riportate sul documento attraverso il timbro di registrazione di protocollo o attraverso l'apposizione di un'etichetta generata dal sistema di gestione del protocollo.

Per i documenti informatici, tutte le informazioni sopra riportate sono generate automaticamente dal sistema e sono incluse nella segnatura informatica di ciascun messaggio protocollato.

4.6. Annullamento delle registrazioni di protocollo

La necessità di modificare anche un solo campo tra quelli obbligatori e immodificabili della registrazione di protocollo per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare la registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, insieme a data, ora ed autore dell'annullamento e agli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RPF.

La procedura riporta infatti l'annotazione di annullamento, la data e il soggetto che è intervenuto.

Solo il RPF è autorizzato ad annullare, direttamente o delegando al vicario o ai dipendenti assegnati all'UCP, una registrazione di protocollo; qualora provveda un delegato, il RPF deve essere comunque avvisato, a mezzo di un documento interno o di un report automatico generato dal sistema

L'annullamento di una registrazione di protocollo deve essere richiesto in modo specifico, adeguatamente motivato, al RPF, utilizzando a tal fine le funzionalità della procedura di gestione del protocollo informatico.

4.7. Protocollazione documenti interni formali

I documenti formali interni all'Ente sono soggetti a protocollazione e indicati come protocolli interni. Vengono inseriti nel sistema di gestione documentale con opportuna classificazione, assegnazione di visibilità, collegamento ai documenti o procedimenti correlati, fascicolazione e archiviazione, esattamente come avviene per documenti esterni.

4.8. Pratiche ricorrenti

Poiché molte pratiche sono ricorrenti, ciascun Servizio può individuare le tipologie di documenti aventi tali caratteristiche e concordare con l'UCP l'indicazione esatta dell'oggetto, la titolazione, la tipologia e l'assegnazione a predeterminati soggetti o ambiti organizzativi.

E' compito di ciascun Servizio provvedere a verificare ed eventualmente comunicare al RPF gli aggiornamenti relativi ai propri documenti ricorrenti.

4.9. Registrazione differita

Per registrazione differita si intende la registrazione di un documento in arrivo che riporta una data di arrivo diversa da quella di protocollazione e la causa che ne ha determinato il differimento.
Normalmente non si considera "differito" il protocollo assegnato il giorno lavorativo seguente alla ricezione, se questa è avvenuta allo scadere dell'orario di servizio o comunque non in tempo utile per la protocollazione immediata, tranne nel caso che dalla mancata registrazione immediata possa venire meno un diritto di terzi (ad esempio una gara d'appalto), nel qual caso si dà atto in modo formale di quanto avvenuto.
Eccezionalmente il RPF può differire ulteriormente la registrazione del protocollo dei documenti ricevuti, determinando comunque il periodo di differimento e conferendo valore al timbro datario di arrivo.

4.10. Documenti riservati

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni è disponibile all'interno del sistema di protocollo informatico dell'Autorità una specifica funzionalità che consente la gestione di un protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.

I documenti soggetti a questa particolare procedura sono i seguenti:

- atti dei procedimenti amministrativi in relazione ai quali sussistano particolari esigenze di protezione della riservatezza di terzi, persone, gruppi, imprese ed associazioni e dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- atti contenenti informazioni classificate, o coperte da segreto di Stato;
- documenti relativi a vicende di persone o a fatti privati o particolari;

- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obiettivi prefissati;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241;
- documenti che contengano dati sensibili, giudiziari o personali, come definiti dal Codice in materia di protezione dei dati personali;
- documenti afferenti a segnalazioni di cui all'art. 54 bis d.lgs. 165/2001 (*whistleblowers*).

La selezione della casella "riservato" rende la protocollazione riservata e visibile ai soli utenti abilitati.

In particolare, su indicazione del Segretario Generale, gli operatore dell'UCP - all'atto della registrazione- devono selezionare l'apposita casella "*riservato*" e il nominativo dell'assegnatario. In tal modo il documento rimane visibile esclusivamente dal protocollatore, dal RPF e dal destinatario.

Va evidenziato che la procedura di cui sopra consente di eseguire sul documento c.d. riservato tutte le operazioni quali: la registrazione, la segnatura, la classificazione e la fascicolazione, adottate per gli altri documenti e procedimenti amministrativi. In caso di documento analogico va eseguita la scansione ai fini della conservazione dello stesso in formato pdf.

Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

4.11. Utilizzo del registro di emergenza

Il RPF o il suo vicario autorizza la registrazione di protocollo sul registro di emergenza ogniqualvolta non sia possibile utilizzare il sistema informatico a causa di impedimenti tecnici.

Il registro di emergenza è unico ed è gestito dall'UCP. Tutti gli UOP, in caso di necessità, fanno quindi riferimento all'UCP 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 primo gennaio e termina il 31 dicembre di ogni anno.

Per le specifiche procedure relative al protocollo di emergenza si rimanda all'allegato C al presente T.U.

4.12. Registro giornaliero di protocollo

Il RPF o il suo vicario, direttamente o delegando gli addetti, provvede alla produzione del registro giornaliero di protocollo in formato elettronico, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

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

5. SISTEMA DI CLASSIFICAZIONE

5.1. Titolario o piano di classificazione

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), cioè di quello che viene definito un "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Ente, al quale viene ricondotta la molteplicità dei documenti gestiti".
Il piano di classificazione è sempre stato, storicamente, lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'Ente; col sistema di protocollazione e gestione del flusso documentale si riproduce lo stesso schema logico, attribuendo ad ogni documento e fascicolo un attributo d'archivio.
Il Titolario o Piano di classificazione, allegato A) al presente T.U., è lo schema logico utilizzato per organizzare i documenti in base alle funzioni e alle materie di competenza del Comune. Esso si divide in categorie, classi e sottoclassi. La categoria individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni). Le successive partizioni (classi, sottoclassi) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo.
Questi livelli di classificazione vengono attribuiti nella fase di protocollazione.
Livelli ulteriori (macro-fascicolo, fascicolo, sotto-fascicolo digitale) possono essere attribuiti anche in momenti successivi alla fase di protocollazione da parte del RPA.
Tutti i documenti ricevuti e prodotti dall'Ente, indipendentemente dalla forma analogica o digitale, sono classificati in base al sopra citato Titolario.

5.2. Variazioni del Titolario e loro efficacia

Poiché il Titolario è uno strumento preposto a descrivere le funzioni e le competenze dell'Ente, che sono soggette a modifiche in forza di leggi o regolamenti, nonché all'evoluzione culturale della società, le categorie e sottocategorie dello stesso possono essere soggette a variazioni, esaminate dal RPF su proposta dei responsabili dei Servizi.

Le modifiche e integrazioni entrano in vigore il 1° gennaio dell'anno successivo alla loro approvazione. Il Titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Deve comunque essere garantita la possibilità di risalire al Titolario utilizzato al momento di protocollazione, mantenendo stabili i legami dei fascicoli digitali e dei documenti con la struttura del Titolario vigente al momento della produzione degli stessi.

Il RPF deve conservare il Titolario attuale ed i titolari precedenti, indicando in modo chiaro il periodo di utilizzazione.

5.3. Classificazione

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

SEZIONE 3

1. FASCICOLAZIONE

1.1. Il sistema di fascicolazione

La fascicolazione è un'attività strategica per la gestione documentale e per la corretta archiviazione dei documenti all'interno del sistema di gestione documentale.

Essa consiste nel riunire in un'unica entità (il fascicolo) i documenti riguardanti uno stesso procedimento amministrativo/affare o riferiti a una stessa attività o persona fisica o giuridica, nel completare le operazioni di registrazione e classificazione dei documenti e nell'organizzare i documenti prodotti e ricevuti dal Comune.

La formazione dei fascicoli e delle altre aggregazioni di documenti è strettamente legata allo svolgimento quotidiano dell'attività amministrativa, in quanto esiste un rapporto di causa-effetto tra la gestione del procedimento amministrativo e il fascicolo, il quale a sua volta è strumento della concreta azione amministrativa.

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

I fascicoli possono essere:

- **cartacei:** laddove tutta la documentazione originale della pratica è prodotta in formato cartaceo;
- **informatici:** laddove tutta la documentazione originale della pratica è prodotta in formato elettronico;
- **misti (o ibridi):** nel caso in cui la documentazione riguardante la pratica sia stata formata da documenti prodotti, in originale, sia in formato cartaceo che in formato elettronico; in questi casi vengono prodotti due fascicoli distinti, ma funzionalmente collegati e ben individuabili, e i riferimenti al fascicolo collegato sono riportati sia nella copertina del fascicolo cartaceo che nei dati di identificazione del fascicolo informatico.

I fascicoli possono anche essere distinti in annuali e non annuali, a seconda della durata e tipologia delle pratiche.

La creazione di un fascicolo deve essere effettuata dai soggetti di cui alla Sezione 1 par. 2.5, direttamente o tramite i propri collaboratori, di norma nel momento in cui perviene un primo documento che ne richiede la creazione.

Ogni documento, dopo la sua protocollazione e la conseguente classificazione, viene inserito nel fascicolo di riferimento dai soggetti di cui alla Sezione 1 par. 2.5, direttamente o tramite i propri collaboratori.

I documenti sono archiviati secondo l'ordine cronologico di registrazione

I fascicoli dell'archivio corrente gestiti a cura dei Servizi/Uffici competenti fino alla loro chiusura nel sistema informatico.

I fascicoli e i sottofascicoli sono consultabili da tutti gli utenti, fermo restando quanto previsto dal dalla Sezione 5 par. 1.7, mentre possono essere modificati soltanto dagli appartenenti al Settore/U.O.A. competente.

Restano esclusi i fascicoli ed i documenti che, in ragione del loro contenuto, debbano essere riservati, in base a quanto previsto dalla normativa di settore relativa alla tutela dei dati personali.

I soggetti di cui alla Sezione 1 par. 2.5 sono responsabili della corretta gestione dei fascicoli di propria competenza e forniscono al proprio personale le indicazioni operative per la gestione dei fascicoli e assicurano, mediante opportuna vigilanza, che la formazione dei fascicoli avvenga in modo uniforme, sia con riferimento ai criteri da adottare per la classificazione, sia nei confronti della denominazione della pratica, al fine di agevolarne la ricerca successiva.

1.2. Tipologie di fascicoli

Il sistema di gestione documentale del Comune consente la gestione informatica dei fascicoli e delle aggregazioni documentali, così come previsto dalla normativa in materia.

Nel sistema di gestione documentale sono aperti fascicoli archivistici.

Per l'individuazione delle tipologie di fascicolo all'interno del Comune si è scelto di utilizzano le seguenti definizioni tradizionali di fascicolo archivistico:

- il **fascicolo per procedimento** comprende i documenti, recanti tutti la medesima classifica, prodotti da uno o più uffici per la trattazione di un procedimento. Ogni fascicolo si riferisce ad un procedimento amministrativo specifico e concreto e si chiude con la conclusione del procedimento stesso. Ha quindi una data di apertura, una durata circoscritta ed una data di chiusura.
- il **fascicolo per affare** comprende i documenti, recanti tutti la medesima classifica, prodotti da uno o più uffici per la trattazione di un affare (ad esempio il fascicolo relativo alla realizzazione di un'opera pubblica). Ha le medesime caratteristiche del fascicolo per procedimento, ma essendo relativo ad un affare può non chiudersi con un atto finale né in tempi pre-determinati.
- il **fascicolo per attività** comprende i documenti prodotti nello svolgimento di un'attività amministrativa non discrezionale, che si esaurisce in risposte obbligatorie per legge (quali ad esempio il fascicolo relativo alle richieste accesso ai documenti, il fascicolo relativo alle

richieste di verifica da parte di altri enti, il fascicolo delle fatture, ecc). La sua chiusura è periodica, tendenzialmente annuale, salvo diverse esigenze gestionali.

- il **fascicolo nominativo**, ossia per persona fisica o giuridica comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica o giuridica (quali ad esempio i fascicoli del personale). Si tratta di fascicolo permanente, attivo fino quando è 'attiva' la persona a cui è intestato.

I fascicoli gestiti nel sistema informatico sono costituiti da file, che possono costituire originali digitali, e copie immagine di documenti analogici.

Qualora un procedimento/affare/attività sia costituito anche da documenti analogici, i Servizi/Uffici creino anche il fascicolo cartaceo di riferimento, che dovrà contenere i documenti originali analogici anche se di essi vi sia copia immagine nel sistema informatico.

La copertina di tale fascicolo dovrà riportare i medesimi dati del fascicolo informatico compreso il codice.

Nei fascicoli possono essere inseriti anche documenti soggetti a registrazione particolare/repertorio.

1.3. I fascicoli elettronici

Al fascicolo digitale corrisponde una "aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento".
Qualora un documento porti ad avviare un nuovo procedimento amministrativo, i soggetti di cui alla Sezione 1 par. 2.5, direttamente o tramite i propri collaboratori, provvedono all'apertura di un nuovo fascicolo/sottofascicolo, eventualmente collegato a un macro-fascicolo digitale già esistente.

I Servizi/Uffici comunali sono tenuti ad individuare quali fascicoli debbano essere aperti nel sistema di gestione documentale sulla base delle proprie esigenze pratiche ed operative, quindi attivare la procedura di apertura del fascicolo nel sistema informatico.

Nel momento di apertura del fascicolo devono essere compilati almeno i campi obbligatori, ovviamente ad eccezione della data di chiusura che diventa obbligatoria in fase di chiusura del fascicolo.

L'oggetto del fascicolo o sottofascicolo, che ne identifica il contenuto, deve essere espresso in forma sintetica, ma nello stesso tempo chiara ed univoca, in modo tale da renderne agevole la ricerca anche a distanza di molti anni o da parte di utenti non assegnati al Servizio/Ufficio competente.

I fascicoli annuali sono aperti ogni anno automaticamente dal sistema; gli altri fascicoli devono essere aperti dai Servizi/Uffici competenti.

1.4. Metadati da associare

I metadati costituiscono gli insiemi di dati da associare a un documento informatico o a un fascicolo informatico o a un'aggregazione documentale informatica, per identificarlo e descriverne il contesto, il contenuto, la struttura, nonché per permetterne la gestione e la ricerca nel tempo nel sistema di conservazione.

I metadati generali o oggettivi da associare a tutte le tipologie di documenti da conservare devono fornire le informazioni base relative al pacchetto di archiviazione, al suo contenuto e al processo di produzione dello stesso.

I metadati specifici o soggettivi da associare alle diverse tipologie di documenti e di fascicoli da conservare sono indicati dai soggetti di cui al Sezione 1 – par. 2.5 al RC, che a sua volta li comunica al delegato per la conservazione all'atto della stipula del contratto o convenzione di servizio e delle successive modifiche o integrazioni.

Tale contratto dovrà prevedere l'aggiornamento dell'insieme minimo dei metadati in funzione di eventuali aggiornamenti normativi.

I metadati devono essere inclusi nel pacchetto di archiviazione ottenuto dalla trasformazione del pacchetto di versamento all'atto della messa in conservazione.

I metadati minimi sono quelli indicati nell'allegato 5 al DPCM 3 dicembre 2013 e sono riportati nell'allegato D per ciò che riguarda i documenti informatici, all'allegato E per i fascicoli informatici.

1.5. La gestione dei fascicoli elettronici

La formazione di un nuovo fascicolo/sotto-fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali (metadati), cosi come previsto nell'allegato 5 del D.P.C.M del 3 dicembre 2013 (regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis, 23 -ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del CAD di cui al D.Lgs. 82/2005).

I documenti contenuti in un fascicolo hanno solitamente identica classificazione e devono essere facilmente individuabili e reperibili, anche attraverso i metadati.
Criteri di reperibilità ed archiviazione più dettagliati possono essere definiti dai soggetti indicati nella Sezione 1 – par. 2.5.

I documenti in ingresso, dopo la classificazione e la protocollazione, vengono rimessi dall'UCP (o da altre postazioni abilitate alla protocollazione in ingresso) ai Servizi/Uffici di competenza che avranno cura di fascicolarli attraverso la compilazione del "campo fascicolo" sulla scheda di protocollo.

Una volta ricevuto il documento, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati prendono in carico il documento all'interno del sistema informatico e stabiliscono, eventualmente con l'ausilio delle funzioni di ricerca di Sicr@web, se il documento:

- si riferisce ad attività annuali di cui esiste già un fascicolo "annuale e ripetitivo";
- deve essere collegato ad un affare o procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente;
- dà avvio ad un nuovo procedimento/affare per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

In caso di **nuovo procedimento** indicati nella Sezione 1 – par. 2.5. i soggetti indicati Sezione 1 – par. 2.5 o i loro delegati:

1. verificano la correttezza dell'assegnazione;
2. verificano la correttezza della classificazione;

3. eseguono l'operazione di apertura del fascicolo/sottofascicolo;
4. collegano il documento al nuovo fascicolo aperto;
5. si occupano della gestione del documento o assegnano il documento all'impiegato che dovrà istruire la pratica;
6. se necessario, e se già non automaticamente notificato dal sistema di gestione del flusso documentale, avvisano altri uffici eventualmente coinvolti.

Se il documento si riferisce ad un **procedimento in corso**, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati:

1. verificano la correttezza dell'assegnazione;
2. verificano la correttezza della classificazione;
3. selezionano il relativo fascicolo;
4. collegano la registrazione di protocollo del documento al fascicolo selezionato;
5. gestiscono direttamente il documento o lo assegnano all'ufficio o al dipendente che dovranno istruire la pratica;
6. se necessario, e se già non automaticamente notificato dal sistema di gestione del flusso documentale, avvisano gli altri uffici eventualmente coinvolti.

I documenti in partenza, invece, devono essere fascicolati nel sistema di gestione dei flussi documentali dai Servizi/Uffici contestualmente alla classificazione e protocollazione.

1.6. Modifica delle assegnazioni dei documenti ai fascicoli elettronici

Quando si verifica un errore nell'assegnazione di un documento a un fascicolo, il soggetto preposto all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico, a partire dalla classificazione del documento, se il documento e il relativo fascicolo sono comunque di competenza del proprio ufficio.

Se il documento protocollato invece è di competenza di un ufficio diverso, lo rifiuta entro tre giorni lavorativi, in modo tale che l'Ufficio Protocollo possa modificare la classificazione e

assegnare il documento a un Ufficio diverso, che provvede a sua volta alle operazioni di fascicolazione.

Ogni Servizio/Ufficio è responsabile dello svolgimento tempestivo dell'attività di cui al capoverso precedente.

Il sistema di gestione dei flussi documentali tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che comunica la necessità di procedere alla modifica dell'assegnazione, nonché dell'operatore che la effettua con la data e l'ora dell'operazione.

1.7. Sottofascicoli elettronici

Il sistema di protocollo informatico consente l'apertura all'interno dei diversi fascicoli di "sottofascicoli". I sottofascicoli sono creati e gestiti dai Servizi/Uffici in base alle proprie esigenze organizzative, tra cui:

- gestire fasi di procedimento diverse;
- gestire tempi di conservazione diversi dei documenti che costituiscono i procedimenti/affari;
- gestire eventuali riservatezze.

Gli uffici competenti per la gestione dei diversi fascicoli possono in ogni momento aprire e gestire all'interno degli stessi i sottofascicoli che ritengono necessari per la gestione delle pratiche.

Le regole di apertura, gestione e chiusura sono le medesime di quelle stabilite per i fascicoli.

1.8. Chiusura dei fascicoli e dei sottofascicoli elettronici

I fascicoli per attività, per i quali in apertura è stata attivata nel sistema di gestione dei flussi documentali la funzione di "annuali", vengono chiusi annualmente dal sistema e riaperti automaticamente per l'anno successivo.

i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati ogni anno devono controllare che i fascicoli "annuali" di loro competenza debbano essere aperti anche l'anno successivo e in caso contrario segnalare prima del 15 dicembre di ciascun anno l'eventuale modifica al RC.

Tutti gli altri fascicoli devono essere chiusi alla loro conclusione.

Qualora dovesse essere necessario riaprire i fascicoli (ad esempio in caso di contestazioni o ricorsi) il sistema consente di riportarli ad uno stato attivo, tenendo traccia di questi passaggi.

1.9. Repertorio dei fascicoli

I fascicoli sono annotati nel repertorio dei fascicoli.

Il repertorio dei fascicoli, ripartito per ciascun titolo del Titolario di classificazione, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del Titolario e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il Titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe, sottoclasse);
- il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sottofascicoli);
- l'annotazione sullo status relativo al fascicolo, se cioè sia ancora una "pratica" corrente, o se abbia esaurito la valenza amministrativa immediata e sia quindi da mandare in deposito, oppure, infine, se sia da scartare o da passare all'archivio storico.

Il repertorio dei fascicoli è automaticamente aggiornato dal sistema di gestione dei flussi documentali.

Il repertorio dei fascicoli viene creato automaticamente dal sistema di gestione dei flussi documentali stesso, a seguito dell'attività quotidiana di fascicolazione.

2. ARCHIVIAZIONE

2.1. Archivio dei documenti cartacei dell'Amministrazione

All'organizzazione e alla tenuta dei documenti cartacei dell'Amministrazione è preposto il RC.

La Giunta comunale individua le sedi dell'archivio cartaceo dell'Amministrazione.

A cura del RC sono regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il RC deve essere portato a conoscenza, in ogni momento, della collocazione del materiale archivistico; lo stesso cura la corretta predisposizione degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e del registro sul quale sono annotati i movimenti delle singole unità archivistiche collocate nell'archivio di deposito.

2.2. Archiviazione sostitutiva dei documenti analogici

Il RC, valutati i costi ed i benefici, può proporre l'operazione di conservazione sostitutiva dei documenti analogici su supporti di memorizzazione sostitutivi del cartaceo in conformità alle disposizioni vigenti.

2.3. Archiviazione sostitutiva dei documenti digitali

Il processo di archiviazione sostitutiva viene effettuato mediante flussi crittati di riversamento verso il sistema adottato DAX di Regione Toscana, accreditato presso AGID. e verificabile all'indirizzo http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi dove è possibile anche scaricare il Manuale di conservazione aggiornato.

2.4. Serie archivistiche e repertori

2.4.1. Serie archivistiche

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti (es. le autorizzazioni a costruire, i contratti).

Le serie documentarie sono formate dai registri e dai relativi fascicoli compresi in un arco d'anni variabile.

I fascicoli subiscono il processo di selezione e scarto dei documenti.

Le serie archivistiche formate a seguito del processo di scarto di cui al paragrafo 2.5 della presente Sezione, fanno parte, dopo 40 anni dalla chiusura del fascicolo, della sezione storica dell'archivio.

2.4.2. Repertori e serie archivistiche

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'Amministrazione, le ordinanze ed i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati in uno specifico registro di repertorio integrato nel sistema di gestione documentale.

Con riguardo alla gestione dei documenti, è previsto che per ogni documento che costituisce serie archivistica soggetta a registrazione particolare dell'Ente sia, di norma, disponibile nella serie archivistica di appartenenza e nel fascicolo di riferimento.

Pertanto i soggetti di cui alla Sezione 1 – par. 2.5 devono chiedere al RC la creazione dei repertori generali già indicati a titolo esemplificativo nell'allegato F e l'integrazione dell'elenco in occasione della modifica e revisione del presente T.U.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.

Il repertorio è costantemente aggiornato.

2.4.3. Versamento dei fascicoli nell'archivio di deposito

La formazione dei fascicoli elettronici o digitali, nonché delle serie e dei repertori è una funzione fondamentale della gestione archivistica.

Periodicamente, e comunque almeno una volta all'anno, viene effettuato a cura del RC, nell'ambito di rispettiva competenza, il versamento dei fascicoli e delle serie documentarie relativi ai procedimenti conclusi in un'apposita sezione di deposito dell'archivio generale.

Per una regolare e costante "alimentazione" dell'archivio di deposito, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati stabiliscono tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi uffici dell'Amministrazione/AOO all'archivio di deposito.

Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori generali.

La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.

Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

Prima di effettuare il conferimento di cui sopra, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati o loro incaricati procedono alla verifica:

- dell'effettiva conclusione della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel fascicolo e nel registro di repertorio dei fascicoli, a meno che la chiusura non avvenga automaticamente.

Nel caso si tratti di fascicoli analogici, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati o loro incaricati provvedono inoltre:

- allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli analogici e controllato l'aggiornamento del relativo repertorio, il RC predispone un elenco di "versamento" da conservare presso il Servizio stesso.

Copia di detto elenco viene conservata i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati che hanno versato la documentazione.

I fascicoli che riguardano il personale, di norma vengono trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio o dopo il perfezionamento della pratica pensionistica.

Tutti i fascicoli che andranno a creare l'archivio di deposito dell'ente dovranno essere gestiti nel rispetto del D.P.R. 28 dicembre 2000, n. 445, dei D.P.C.M. del 3 dicembre 2013 e 13 novembre 2014, rispettivamente in materia di protocollo informatico, conservazione e documento informatico, nonché nel rispetto della normativa archivistica.

2.4.4. Verifica della consistenza del materiale riversato nell'archivio di deposito

Gli incaricati della gestione dell'archivio di deposito eseguono il controllo del materiale riversato.

Devono essere riversati nell'archivio di deposito soltanto i fascicoli con materiale ordinato e completo.

Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito ai tenutari dell'archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie.

Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, i soggetti indicati nella Sezione 1 – par. 2.5 o i loro delegati depositano il fascicolo dichiarando ufficialmente che è incompleto e si assumono la responsabilità della trasmissione agli atti.

Ricevuti i fascicoli e controllato il relativo elenco, gli incaricati della gestione dell'archivio di deposito firmano per ricevuta l'elenco di consistenza.

I fascicoli digitali seguono la stessa disciplina normativa, sono essere gestiti mediante il software di gestionale documentale e vengono conservati attraverso il sistema di conservazione di cui alla Sezione 4.

2.5. Scarto, selezione e riordino dei documenti

2.5.1. Tempi minimi di archiviazione e conservazione dei documenti

I documenti amministrativi prodotti e detenuti dal Comune di Sesto Fiorentino sono oggetto di tutela ai sensi dell'art. 10 del Codice dei beni culturali di cui al Decreto Legislativo 42/2004; pertanto si considera che tutti i soggetti che agiscono nell'ambito del sistema di gestione documentale dell'Ente svolgano attività archivistica.

L'Ente, ai sensi dell'art. 30 del predetto Codice, assolve all'obbligo di conservazione e ordinamento degli archivi.

Ai fini di un corretto esercizio dell'azione amministrativa, i fascicoli prodotti dagli uffici dell'Ente sono raccolti in archivi che possono essere distinti in:

- **archivio corrente:** la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione; l'archiviazione corrente si identifica per i documenti e i fascicoli informatici con l'archiviazione all'interno del sistema di gestione documentale;
- **archivio di deposito:** la parte di documentazione di affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, che, per i documenti cartacei si trova localizzato in un immobile nella disponibilità dell'Ente all'interno del territorio comunale; i documenti elettronici invece sono conservati tanto nel sistema di gestione dei flussi documentali quanto nel sistema di conservazione, essendo automaticamente contrassegnati come archivio di deposito una volta chiuso il fascicolo elettronico;
- **archivio storico:** la parte di documentazione relativa agli affari esauriti destinata alla conservazione perenne, che per i documenti cartacei si trova localizzato in un

immobile nella disponibilità dell'Ente all'interno del territorio comunale; i documenti elettronici invece sono conservati tanto nel sistema di gestione documentale e nel sistema di conservazione.

La coesistenza, nell'ambito di uno stesso procedimento, di documenti di natura mista (digitali e cartacei) si definisce "**archivio ibrido**".

La gestione dei processi di selezione dei documenti dell'archivio di deposito, può condurre alla conservazione permanente dei documenti che rivestono significativo valore di testimonianza storica, oltre che rilevanza giuridico probatoria, oppure allo scarto, ossia l'eliminazione irreversibile dei documenti di valore transitorio e strumentale, da effettuarsi con l'autorizzazione del soprintendente archivistico competente per territorio.

A seconda delle diverse tipologie documentali gestite dall'Ente vengono definiti criteri e regole di selezione al fine di individuare i documenti da scartare e quelli da conservare, secondo quanto previsto dal Piano di conservazione del 2005 pubblicato sul sito istituzionale redatto della Soprintendenza Archivistica della Toscana, specificato per quanto riguarda il Comune di Sesto Fiorentino dal Massimario di selezione documentale, di cui all'allegato G.

2.5.2. Operazione di scarto

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che non devono essere conservati ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento sia che esso sia redatto su supporto analogico che digitale.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza giuridico-amministrativa e non ha assunto alcuna rilevanza storica.

Le operazioni di selezione e scarto dei documenti analogici sono effettuate, secondo la normativa vigente, sotto la vigilanza degli incaricati della gestione dell'archivio di deposito.

I documenti e gli atti sottoposti a procedura di scarto sono distrutti in modalità atte a garantire l'illeggibilità degli stessi.

2.5.3. Conservazione del materiale presso la sezione di deposito dell'archivio

L'operazione di riordino della sezione di deposito dell'archivio cartaceo viene effettuata con la periodicità stabilita dall'Amministrazione/AOO e consiste nella catalogazione dei materiali e nell'aggiornamento del data base dei documenti archiviati.

L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di confezionamento che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti o dati dai quali è possibile risalire alle stesse informazioni.

2.5.4. Versamento dei documenti nell'archivio storico

Gli incaricati della gestione dell'archivio di deposito provvedono a trasferire alla sezione separata dell'archivio storico i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.

I trasferimenti vengono effettuati dopo il completamento delle operazioni di scarto.

Presso l'archivio storico i documenti vengono organizzati al fine della conservazione, consultazione e valorizzazione.

2.6. Consultazione e movimentazione dell'archivio corrente, di deposito e storico

2.6.1. Principi generali

La richiesta di consultazione dei fascicoli e/o documenti analogici può provenire dall'interno dell'Amministrazione/AOO oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per ricerche storiche.

La consultazione dei fascicoli e /o documenti sia analogici che informatici viene effettuata garantendo l'osservanza delle disposizioni in materia di accesso e in materia di trattamento dei dati personali e, nel caso di richiesta da parte di soggetto esterno, concessa previa autorizzazione del responsabile del procedimento a cui essa afferisce.

2.6.2. Consultazione ai fini giuridico-amministrativi

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 e successive modifiche e integrazioni, dal D. Lgs. 33/2013 e successive modifiche e integrazioni e dal Regolamento in materia di accesso del Comune di Sesto Fiorentino.

2.6.3. Consultazione per scopi storici

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata da specifico regolamento emanato sulla base degli indirizzi generali stabiliti dal Ministero per i beni e le attività culturali (a norma dell'art. 124 del decreto legislativo 22 gennaio 2004, n. 42 s.m.i.).

La ricerca per scopi storici è:

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'interno (a norma dell'art. 125 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione/AOO. È possibile l'ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);
- condizionata all'accettazione integrale del "Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

2.6.4. Consultazione da parte di soggetti esterni all'Amministrazione

La domanda di accesso ai documenti viene presentata nel rispetto delle disposizioni richiamate al precedente paragrafo 2.6.2.

Le domande vengono evase con la massima tempestività nei termini previsti per l'accesso.

Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate e archiviate in formato digitale.

Il RC provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

L'ingresso all'archivio di deposito e storico è consentito solo agli incaricati della gestione dell'archivio comunale.

La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto presso la sede dell'archivio di deposito sotto la diretta sorveglianza del personale addetto.

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

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.

Le disposizioni dei commi precedenti si applicano anche alla consultazione dell'archivio storico.

2.6.5.Consultazione da parte di personale interno all'Amministrazione

Gli uffici interni, per motivi di consultazione, possono richiedere in ogni momento al Servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica.

Qualora non sia possibile l'invio telematico delle immagini del fascicolo o per specifici casi particolari, l'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico a un ufficio avviene solamente per il tempo strettamente necessario alla consultazione o estrazione di copia dei documenti in esso contenuti.

L'affidamento del fascicolo temporaneo avviene solamente mediante richiesta espressa redatta in duplice copia su un apposito modello predisposto dagli incaricati della gestione dell'archivio di deposito

Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura degli incaricati della gestione dell'archivio di deposito in un apposito registro e/o software di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.

Gli incaricati della gestione dell'archivio di deposito verificano che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

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

Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'AOO.

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

Per quanto riguarda i fascicoli digitali essi potranno, per un periodo transitorio, essere gestiti nel relativo software applicativo e successivamente versati al sistema di conservazione. Comunque anche la consultazione e gestione dei fascicoli digitali facenti parte dell'archivio di deposito è effettuata nel rispetto della normativa vigente in materia archivistica.

SEZIONE 4

1. CONSERVAZIONE

1.1. Il sistema di conservazione

Per conservazione digitale si intende un processo, indipendente dalla tecnologia utilizzata, che permette di conservare documenti di qualsiasi natura in formato digitale in modo che risultino disponibili nel tempo nella loro integrità e autenticità.

La conservazione viene attuata attraverso il sistema di conservazione previsto dall'art 3 del DPCM 3 dicembre 2013, in attuazione di quanto previsto dall'art. 44, comma 1, del Codice

dell'Amministrazione Digitale. Il sistema di conservazione assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, degli oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, dei seguenti oggetti:

- documenti informatici comprensivi dei metadati ad essi associati;
- fascicoli informatici ovvero aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

Il sistema di gestione informatica e conservazione dei documenti informatici assicura:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) la sicurezza e l'integrità del sistema e dei dati e documenti presenti;

c) la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;

d) la raccolta di informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati;

e) l'agevole reperimento delle informazioni riguardanti i documenti registrati;

f) l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle disposizioni in materia di tutela dei dati personali;

g) lo scambio di informazioni, ai sensi di quanto previsto dall'articolo 12, comma 2, del CAD, con sistemi di gestione documentale di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi;

h) la corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato;

i) l'accesso remoto, in condizioni di sicurezza, ai documenti e alle relative informazioni di registrazione tramite un identificativo univoco;

j) il rispetto delle regole tecniche di cui all'articolo 71 del CAD.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato indipendentemente dall'evolversi del contesto tecnologico, a tempo indeterminato o fino al momento dell'eventuale scarto o cessazione del contratto.

Ai fini della conservazione:

- il RC produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione;
- in qualità di utenti, i dipendenti e gli amministratori possono interagire con i servizi del sistema di gestione informatica dei documenti e di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.

1.2. Oggetti conservati

Sono conservati tutti i documenti informatici dichiarati ammissibili dal Comune di Sesto Fiorentino. La selezione conservativa dei documenti informatici deve riguardare tutti i documenti informatici prodotti dal Comune secondo le indicazioni previste dalla legge e dal presente T.U.

I documenti informatici devono essere statici, non modificabili e devono essere muniti di sottoscrizione elettronica e/o di marca temporale.

Sono accettati, per la conservazione, i formati che soddisfino caratteristiche di apertura, sicurezza, portabilità, funzionalità, diffusione, leggibilità nel tempo e supporto allo sviluppo.

Sono privilegiati i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche.

Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici.

I formati sono indicati nella Sezione 2 par. 3.2.

1.3. Conservazione elettronica dei documenti digitali

La conservazione dei documenti informatici deve avvenire nel rispetto delle specifiche contenute e richiamate nelle regole tecniche di cui al DPCM 3 dicembre 2013. La conservazione elettronica dei documenti è svolta sotto la responsabilità del RC, in collaborazione con il Servizio "Servizi Informatici", che cura la gestione delle varie piattaforme Server in cui sono memorizzati i dati dell'Ente, e del servizio di conservazione se affidato all'esterno.

Il Sistema informatico, implementato per la conservazione dei dati dell'ente, garantisce che le informazioni in esso memorizzate siano sempre consultabili ed estraibili.

È compito del Servizio "Servizi informatici" espletare le procedure atte ad assicurare la corretta archiviazione, la disponibilità e la leggibilità dei documenti informatici e delle registrazioni di protocollo.

La conservazione elettronica dei documenti riguarda:

- le registrazioni di protocollo;
- la gestione dei documenti prodotti o detenuti dall'Ente;
- la gestione dei fascicoli;
- la gestione dei repertori.

Devono essere trasmessi al sistema di conservazione da norma le informazioni relative:

- al registro giornaliero del protocollo informatico;
- ai fascicoli e ai documenti che fanno riferimento a procedimenti conclusi.

La conservazione svolta direttamente o tramite il delegato per la conservazione deve assicurare nel tempo la leggibilità dei documenti e dei fascicoli conservati.

L'archiviazione avviene mediante riversamento dei documenti tramite flusso dati crittato verso il conservatore Regione Toscana (applicativo DAX) accreditato presso AGID. Il manuale di conservazione è disponibile presso il sito dell'AGID al seguente indirizzo: http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi

1.3. Conservazione delle rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e classificazione, devono essere acquisiti in formato pdf attraverso un processo di scansione integrato nel sistema di gestione documentale.

Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che a ogni documento, anche se composto da più pagine, corrisponda un unico file, e conversione automatica in formato .pdf;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento del file generato alla rispettiva registrazione di protocollo in modo non modificabile.

Le rappresentazioni digitali di documenti analogici, dichiarate conformi all'originale cartaceo, sono inviate al sistema di conservazione a norma. A seguito di tale procedura gli originali cartacei potranno essere distrutti con procedura di scarto, previa autorizzazione della Soprintendenza archivistica.

L'operazione sopra descritta costituisce conservazione sostitutiva.

I documenti analogici, acquisiti al sistema di gestione documentale tramite scansione, sono inviati agli uffici destinatari, che comunque li fascicolano nel rispetto della normativa archivistica e del T.U.

2. AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE A UN SOGGETTO ESTERNO

2.1. Accesso al servizio di conservazione

Nel caso di affidamento ad un soggetto esterno, l'accesso al servizio di conservazione deve avvenire mediante un canale sicuro, attivato dagli applicativi di gestione documentale o via web.

2.2. Obblighi e responsabilità del delegato per l'attività di conservazione

Il delegato per l'attività di conservazione, in nome e per conto del RC:

- predispone un sistema atto alla conservazione dei documenti informatici per conto del Comune di Sesto Fiorentino, secondo le caratteristiche e i requisiti indicati nel presente T.U. e, comunque, nel rispetto della normativa vigente e della sua evoluzione;
- organizza il contenuto dei supporti e gestisce le procedure di sicurezza e di tracciabilità che garantiscano la corretta conservazione dei documenti, in particolare per quanto riguarda la autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti nel sistema;
- archivia e rende disponibili, relativamente ad ogni pacchetto di archiviazione, le informazioni minime seguenti: file di chiusura in formato xml firmato digitalmente contenente le impronte dei documenti conservati e i metadati ad essi associati, i documenti conservati medesimi, il file di marcatura temporale del pacchetto di archiviazione e tutte le informazioni relative alla tracciatura del pacchetto di archiviazione all'interno del sistema di conservazione;
- adotta, ai fini dell'interoperabilità dei sistemi di conservazione, le specifiche della struttura dati dei pacchetti di archiviazione previsti per legge;
- fornisce un rapporto di versamento a fronte di ogni pacchetto di versamento generato dagli utenti produttori del pacchetto attraverso le soluzioni di gestione documentale adottate per gli specifici tipi di documenti;
- mantiene e rende accessibile un archivio del software dei programmi di gestione e un archivio degli standard dei formati ammessi;
- verifica la corretta funzionalità del sistema e dei programmi in gestione, delle logiche di tracciatura e documentazione del sistema stesso;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
- documenta le procedure di sicurezza rispettate per l'apposizione della marca temporale;

- verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti;
- rende disponibili i documenti conservati ad ogni richiesta di esibizione da parte degli utenti, creando i pacchetti di distribuzione richiesti;
- prevede, ai fini dell'interoperabilità dei sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;
- rende disponibili al Comune i documenti conservati nel caso di scadenza e/o risoluzione e/o cessazione del contratto di gestione secondo le clausole indicate nella convenzione/contratto sottoscritto tra le parti;
- rende disponibili le procedure informatiche e operative volte allo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone previa informativa al produttore;
- fornisce al Comune, all'atto di stipula del contratto o della convenzione, un documento contenente almeno le seguenti informazioni: i dati generali delle imprese coinvolte nel processo di conservazione, il modello organizzativo interno, le modalità operative di formazione e trattamento dei documenti, il flusso di lavoro del procedimento di conservazione, il sistema di archiviazione e conservazione sostitutiva dal punto di vista delle risorse umane e tecnologiche impiegate, le misure di sicurezza fisica e logica del sistema preposto al processo di conservazione, la descrizione delle procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, la garanzia circa la conservazione dei dati e delle copie di sicurezza nell'ambito del territorio nazionale; tale documento può costituire parte del Manuale di conservazione del delegato;
- si impegna a rispettare tutte le clausole indicate nel contratto o convenzione di servizio stipulata tra le parti.

Il delegato per l'attività di conservazione deve verificare la completezza della trasmissione, ma non è tenuto a eseguire un controllo sul contenuto e sulla integrità dei documenti ricevuti per la conservazione, né a verificare le eventuali firme elettroniche o marche temporali apposte ai documenti oggetto di conservazione.

Il delegato per l'attività di conservazione verifica che il formato dei documenti trasmessi sia tra quelli ammessi, segnalando al RC e all'utente che prodotto il pacchetto di versamento formati diversi da quelli fissati dal presente T.U.

Nel caso in cui il file abbia un formato diverso rispetto a quelli ammessi, il RC stabilisce se occorre modificare l'elenco dei formati ammissibili oppure se occorre convertire il file.

Il delegato può effettuare verifiche strutturali sulla leggibilità dei documenti.

2.3. Obblighi degli utenti

Gli utenti sono tenuti a:

- inviare esclusivamente documenti leggibili e conformi a quanto dal presente T.U.;
- controllare che i certificati di firma digitale dei documenti non aventi un riferimento temporale certo (marca temporale o segnatura di protocollo o registrazione particolare) contenuti nel pacchetto di versamento siano validi almeno fino alla generazione del pacchetto di archiviazione, ovvero fino alla avvenuta memorizzazione e conservazione a norma;
- accettare o annullare il processo di conservazione avviato entro e non oltre 3 giorni lavorativi dal ricevimento della ricevuta di conservazione; in assenza di comunicazione entro l'indicato termine, il processo sarà considerato validamente concluso. In caso di esito negativo la procedura deve comunque essere ripetuta.

2.4. Formazione del personale

Al fine di consentire di adempiere agli obblighi ed alle prescrizioni del presente T.U., l'Ente organizza percorsi formativi sia specifici che generali che coinvolgono il personale.

3. PROCESSI OPERATIVI

3.1. Conservazione digitale

La conservazione digitale è l'insieme delle attività e dei processi che, tramite l'adozione di regole, procedure e tecnologie, garantiscono l'accessibilità, l'utilizzabilità (leggibilità e

intelligibilità), l'autenticità (identificabilità univoca e integrità) e la reperibilità dei documenti e dei fascicoli informatici con i metadati a essi associati nel medio e nel lungo periodo.

Il valore legale dell'attività di conservazione è subordinato all'organizzazione del servizio e allo svolgimento dell'attività secondo le regole tecniche vigenti.

Ogni servizio di conservazione deve essere composto dai seguenti processi:

- conservazione;
- esibizione;
- riversamento diretto;
- riversamento sostitutivo;
- rinnovo delle marche temporali;
- verifica del sistema;
- gestione del giornale di controllo;
- procedura di scarto.

Il sistema di conservazione opera trattando dei Pacchetti informativi, contenitori che racchiudono uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche) o anche i soli metadati riferiti agli oggetti da conservare.

I pacchetti informativi possono essere di diverse tipologie:

- **di versamento**: pacchetto inviato dal produttore del documento al sistema di conservazione secondo il formato predefinito e concordato, con il delegato per la conservazione; con il versamento il documento, il fascicolo informatico, la serie documentale e il repertorio vengono inviati dal sistema di gestione dei flussi documentali al sistema di conservazione, senza che vengano cancellati dal sistema di gestione;

- **di archiviazione:** pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento utilizzando le specifiche contenute nell'allegato 4 del D.P.C.M 3 dicembre 2013 e secondo le modalità riportate nel presente T.U.;

- **di distribuzione:** pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di esibizione, fermi restando le modalità ed i limiti definiti dal RC.

La conservazione di documenti informatici avviene mediante memorizzazione su supporti conformi alle normative vigenti e termina con l'apposizione, su una evidenza informatica contenente una o più impronte dei documenti, della marca temporale e della firma digitale da parte del delegato per l'attività di conservazione, che attesta il corretto svolgimento del processo.

Il processo di conservazione opera secondo le seguenti fasi:

- formazione e trasmissione del pacchetto di versamento da parte del produttore;
- presa in carico del pacchetto da parte del sistema di conservazione;
- indicizzazione e conservazione a norma dei documenti informatici.

3.2. Formazione e trasmissione del Pacchetto di Versamento

Il produttore invia al sistema di conservazione un pacchetto di versamento contenente l'insieme dei *file* relativi ai fascicoli e ai documenti da conservare e il pacchetto informativo.

3.3. Presa in carico del Pacchetto di Versamento

Ogni sistema di conservazione deve effettuare il controllo del pacchetto di versamento ricevuto, a partire dal pacchetto informativo ad esso associato. In particolare, il sistema deve verificare, in modo automatico, che:

- il pacchetto di versamento sia di struttura conforme allo schema di riferimento;
- i file contenuti nel pacchetto di versamento corrispondano a quelli indicati nel pacchetto informativo;
- i file ricevuti dal sistema siano integri;
- le estensioni dei file corrispondano a quelle relative ai formati ammissibili.

Nel caso in cui l'insieme dei controlli abbia avuto esito positivo, tutti i pacchetti presi in carico sono inviati al sistema di memorizzazione che ne garantisce l'integrità, anche nell'ipotesi di guasti agli apparati.

Per tali attività il sistema deve fare uso di un sistema di memorizzazione per la conservazione a lungo termine e una base dati, detta di conservazione, per la registrazione di tutte le

informazioni necessarie per recuperare i file contenuti nel sistema di memorizzazione ai fini dell'esibizione.

3.4. Indicizzazione e conservazione a norma dei documenti informatici

Il delegato per l'attività di conservazione, a intervalli di tempo stabiliti nel contratto o convenzione di servizio, avvia la procedura di firma e marcatura temporale dei pacchetti presi in carico, consistente in:

- raccolta di tutti i pacchetti informativi;
- generazione del pacchetto di archiviazione costruito a partire dall'unione di tutti i pacchetti informativi contenenti le impronte di tutti i documenti;
- apposizione della firma digitale al pacchetto informativo e apposizione di una marca temporale.

Avvenuta l'effettiva memorizzazione e conservazione a norma, il sistema di conservazione invia al RC e all'utente che ha formato il pacchetto di versamento una ricevuta contenente il pacchetto di versamento e l'informazione relativa all'identificativo del pacchetto informativo e del pacchetto di archiviazione di appartenenza.

Alla ricezione della ricevuta, il RC può controllare che il pacchetto informativo riportato nella ricevuta corrisponda a quello del pacchetto inviato e verificare che i documenti siano leggibili mediante l'operazione di esibizione.

Tali operazioni possono essere supportate da apposite funzionalità presenti sul sito del sistema di conservazione o attraverso specifici applicativi condivisi fra il Responsabile o il delegato.

3.5. Esibizione ed esibizione a norma

L'esibizione dei documenti conservati dal sistema può essere richiesta da ogni utente abilitato e si realizza attraverso la produzione del pacchetto di distribuzione.

L'esibizione a norma dei documenti conservati dal sistema, valida anche a fini legali, può essere richiesta esclusivamente dal RC e dai soggetti da lui espressamente autorizzati.

I soggetti autorizzati accedono al servizio mediante le credenziali di autenticazione e autorizzazione assegnate all'atto della stipula del contratto di servizio.

Il sistema, dopo il controllo della validità delle credenziali:

- consente la ricerca del documento nei pacchetti di archiviazione anche mediante funzioni avanzate di ricerca nei metadati memorizzati;
- recupera il pacchetto di archiviazione contenente il documento ricercato;
- effettua la verifica della firma digitale e della marca temporale apposta al pacchetto recuperato;
- consente la visualizzazione del documento ricercato;
- consente la produzione e lo scarico del pacchetto di distribuzione contenente il documento ricercato.

In caso di malfunzionamento del servizio del sistema di conservazione, garantisce comunque l'esibizione su supporto cartaceo del documento conservato, secondo le modalità indicate nel paragrafo successivo.

3.6. Esibizione cartacea

I soggetti autorizzati possono chiedere l'esibizione del documento su supporto cartaceo inviando al sistema di conservazione apposita richiesta.

Il delegato per la conservazione, dopo aver verificato con i Servizi/Uffici dell'Ente la sussistenza dei presupposti dell'accesso, consegna i documenti richiesti e la ricevuta che accerta il controllo sulla integrità dei documenti.

Se il documento è digitalmente sottoscritto e/o munito di validazione temporale, l'esibizione cartacea sarà effettuata dal RC o da altro pubblico ufficiale che ne attesta la conformità all'originale.

3.7. Riversamento diretto

Il riversamento diretto è il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione a un altro, non alterando la loro rappresentazione informatica.

Tale processo è applicato nei seguenti casi:

- obsolescenza del supporto;
- aggiornamenti periodici del sistema legati alla sicurezza e alla tenuta dei dati;
- richiesta motivata del RC.

3.8. Riversamento sostitutivo

Il riversamento sostitutivo è il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, solitamente per aggiornare il formato ad uno standard più moderno.

Tale processo avviene mediante memorizzazione dei documenti informatici su altro supporto e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del delegato per l'attività di conservazione, che attesta il corretto svolgimento del processo.

Qualora l'unico obiettivo del riversamento sia di aggiornare il formato, l'operazione può anche essere effettuata sullo stesso supporto, d'intesa col RC.

Per i documenti informatici sottoscritti è, inoltre, richiesta l'apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto riversato al documento d'origine.

La tecnica del riversamento sostitutivo può essere impiegata anche per l'esibizione di un singolo documento contenuto in un pacchetto di archiviazione a fronte di una ispezione.

3.9. Rinnovo marche temporali

Il sistema di conservazione effettua in modo automatico il rinnovo della marche temporali applicate alle firme che il delegato per l'attività di conservazione appone al termine del processo di conservazione.

Tale procedura automatica viene eseguita almeno una volta al mese ed è applicata a tutti i blocchi di conservazione la cui marca temporale è in scadenza.

Per ogni pacchetto informativo individuato viene applicata e memorizzata una nuova marca temporale.

3.10. Verifica del sistema

Il delegato per l'attività di conservazione, in nome e per conto del RC, verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

La verifica avviene controllando automaticamente l'integrità dei file contenuti in ogni pacchetto di versamento conservato e, ove tecnicamente possibile, appurando che la rappresentazione informatica del documento sia conforme alla struttura prevista dal suo formato (documento ben formato).

E' inoltre verificata periodicamente la corretta funzionalità del sistema, dei programmi di gestione e degli applicativi di visualizzazione dei formati adottati.

3.11. Gestione del giornale di controllo

Tutte le operazioni effettuate automaticamente dai dispositivi installati presso il sistema di conservazione sono archiviate e annotate nel giornale di controllo, rappresentato mediante documento elettronico protetto rispetto a confidenzialità e integrità e assoggettato a meccanismi di back up e disaster recovery.

3.12. Dati da archiviare

I dati da annotare e da archiviare, cui è associata la data e l'ora dell'effettuazione, riguardano l'inizio e la fine di ciascuna sessione di lavoro e sono inerenti a:

- registrazione di soggetti abilitati;
- conservazione a norma;
- esibizione di un documento;
- riversamento sostitutivo o diretto;

- aggiornamento delle marche temporali.

3.13. Conservazione dei dati

Le registrazioni riportano la data e l'ora in cui sono state effettuate e sono conservate per un periodo minimo di 30 anni.

3.14. Protezione dell'archivio

Il giornale di controllo deve garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

3.15. Gestione del giornale di controllo

Il delegato per l'attività di conservazione ha il compito di gestire il giornale di controllo attraverso l'effettuazione di operazioni di back-up, controlli e report periodici.

Il delegato per l'attività di conservazione deve verificare periodicamente la leggibilità dei supporti di backup del giornale di controllo.

3.16. Verifiche

L'integrità del giornale di controllo è verificata con frequenza almeno mensile dal delegato e, su richiesta, dal RC almeno una volta l'anno.

3.17. Procedura di scarto

Il delegato per l'attività di conservazione esegue la procedura di scarto dei documenti e dei fascicoli contenuti nei pacchetti di archiviazione alla scadenza dei termini di conservazione previsti per la tipologia di documenti, secondo quanto indicato dalla normativa vigente e dal

presente T.U., comunque sempre su autorizzazione del RC e del Ministero per i Beni e le Attività Culturali.

In ogni caso è necessario:

- predisporre la proposta di scarto, indicando in modo dettagliato la documentazione che si intende scartare;
- presentare apposita istanza di autorizzazione alla Soprintendenza archivistica competente per territorio;
- ottenere il rilascio dell'autorizzazione da parte della Soprintendenza con approvazione dell'elenco di scarto;
- distruggere la documentazione scartata con verbalizzazione delle operazioni.

Nel caso in cui un documento da scartare sia incluso in un pacchetto di archiviazione contenente altri documenti da conservare, il delegato per l'attività di conservazione esegue l'estrapolazione del documento e la ricostruzione del pacchetto di archiviazione a norma.

Il Comune di Sesto Fiorentino si riserva la possibilità di richiedere un certificato di avvenuta distruzione dei documenti soggetti a scarto o non più conservati.

4. GESTIONE DELLE COPIE DI SICUREZZA E DISASTER RECOVERY

4.1. Controlli periodici

Il sistema di conservazione deve prevede con frequenza giornaliera, l'esecuzione di copie di sicurezza del sistema di memorizzazione e della base dati di conservazione.

Le copie si appoggiano ad infrastrutture tecnologiche che assicurino assoluti livelli di sicurezza, stabilità e scalabilità.

A tal fine il sistema in modo automatizzato o il delegato manualmente deve provvedere a:

- verificare l'esito dell'operazione e comunicarlo al Responsabile dei Servizi Informatici con una mail in caso di esito negativo;

- registrare l'esito dell'operazione su apposito registro.

Le copie, come i dati originali, sono conservate sul territorio nazionale.

4.2. Gestione degli eventi catastrofici

Il sistema di conservazione garantisce la continuità del servizio, in caso di disastro, attraverso la predisposizione di opportune procedure che consentono il ripristino, in tempi certi, del servizio di esibizione.

Il servizio di esibizione è comunque sempre disponibile perché delocalizzato presso i sistemi informatici della Regione Toscana e rimane attivo anche in caso di malfunzionamento o temporanea perdita di dati all'interno dei sistemi del Comune.

SEZIONE 5

1.1. Obiettivi del piano di sicurezza

Il piano di sicurezza deve garantire che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, siano ridotte a probabilità minime in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

1.2. Generalità

Il RPF e il RC predispongono il piano di sicurezza in collaborazione con il Responsabile dei Servizi Informatici, nel rispetto di quanto previsto dal Regolamento UE 679/2016, dallae misure di sicurezza generali dall'Ente e dal presente T.U.

Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, 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 ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alla valutazione del rischio ed alla procedura da seguire in caso di data breach come previsto dal regolamento UE 679/2016;
- 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 del Servizi Informatici e tutti i soggetti autorizzati dal titolare al trattamento dei dati personali in possesso dell'Ente adottano 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 acceso 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), i medesimi del sistema LDAP di autenticazione al dominio, e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;

- conservazione, a cura del responsabile dei backup 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;
- nomina del RC;
- conservazione del registro di protocollo informatico presso conservatore accreditato Regione Toscana;
- conservazione di tutti i documenti a firma digitale e PEC presso conservatore accreditato Regione Toscana;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale.

I dati personali registrati nei log delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RPF e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

1.3. Formazione dei documenti – aspetti di sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF-A, XML) come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Nel caso si voglia attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

1.4. Gestione dei documenti informatici

II sistema operativo del PdP utilizzato dall'AOO è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;

- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

1.4.1. Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'AOO.

Nella conduzione del sistema informativo sono stati individuati i responsabili come previsto dal Reg. UE 679/2016. Tutte le nomine sono pubblicate all'indirizzo http://www.comune.sesto-fiorentino.fi.it/rete-civica/privacy.

Nella conduzione del sistema di sicurezza con riferimento alla gestione dei flussi documentali ed alla conservazione, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- Coordinamento e sviluppo del sistema di gestione documentale
- Coordinamento e sviluppo di sistemi per la conservazione sostitutiva dei documenti
- Formazione interna all'Ente in ambito tecnico-normativo legata all'uso delle tecnologie
- Stesura di regolamenti/manuali per l'utilizzo delle tecnologie nel modello organizzativo dell'ente
- Gestione tecnologica della Server Farm Comunale e della infrastruttura di rete;
- Gestione della sicurezza dei dati ai sensi del Regolamento UE 679/2016;
- Gestione tecnica del nodo Internet dell'Ente e del sito WEB istituzionale;
- Assistenza agli utenti nell'uso delle attrezzature informatiche e risoluzione problematiche hardware e software di base;
- Gestione dei sistemi "antivirus" informatici;
- Gestione backup dei dati;
- Gestione delle autorizzazioni utente e sistemi di posta elettronica.

1.4.2.Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- accesso ai locali tramite chiave a disposizione del solo personale addetto;
- gli altri utenti possono accedere solo in presenza del personale del Servizio;
- business continuity con ridondanza di UPS dedicati;
- sistema antintrusione notturno verificato nelle sue funzionalità ogni 6 mesi.

1.4.3.Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del PdP, è stata realizzata attraverso l'uso di:

- ACL (Access Control Listi) per la definizione degli accessi ai documenti (dati strutturati e file);
- Versioning per la gestione delle versioni dei documenti e conseguente tracciatura e storicizzazione delle diverse versioni succedute nel tempo;
- Gestione dei ruoli associati agli utenti
- Sistema di abilitazione all'uso multilivello
- Abilitazione di menu
- Abilitazione di funzione (all'interno del menu)
- Abilitazione di folder (all'interno della funzione)
- Abilitazione di bottone (all'interno del folder)
- Abilitazione di report (all'interno della funzione)
- Autenticazione degli utenti tramite LDAP
- Uso della firma digitale e dell'impronta informatica

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura basata su:

- server centralizzati con sistemi operativi aggiornati e protetti da sistemi antivirus
- sistema di backup giornaliero
- sistema di autenticazione per la connessione al dominio di rete.

1.4.4.Componente infrastrutturale della sicurezza

Il sistema informatico utilizza i seguenti impianti:

- server farm centralizzata con dispositivi server ridondati nei sistemi di calcolo, storage e connettività
- seconda server farm per la continuità operativa e il DR
- storage area network (due) connesse in FC attraverso switch ottici ridondati
- libreria di backup su nastri e server di backup dedicato
- sistema di firewalling e proxy clusterizzato
- virtualizzazione di server con (VMWARE)
- alimentazioni ridondate, doppio UPS

1.5. Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano a oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza. Le registrazioni di sicurezza sono costituite:

- dai log di sistema degli accessi eseguiti dagli amministratori;
- dalle registrazioni del PdP.

1.6. Trasmissione e interscambio dei documenti informatici

I componenti delle UOP e gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la comunicazione o diffusione, in applicazione del Regolamento UE 2016/679, e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse. Il server di posta certificata del fornitore esterno *(provider)* di cui si avvale l'amministrazione, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

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

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete. Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

1.6.2. All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nei paragrafi precedenti.

Gli uffici si scambiano documenti informatici giuridicamente rilevanti attraverso l'utilizzo del gestionale documentale e non attraverso i sistemi di posta elettronica. Questo garantisce completa tracciabilità dell'accesso e trattamento dei dati.

1.7. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) e un sistema di

autorizzazione basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale. Si intende ovviamente riferito al personale in organico allo specifico servizio che tratti normalmente procedimenti dell'ente.

Le regole per la composizione delle password e per il blocco delle utenze sono le seguenti:

1) la password non potrà essere uguale alle tre precedenti

2) la password dovrà avere una lunghezza di almeno 8 caratteri

3) la password non potrà contenere né il proprio nome utente né il nome né il cognome

4) la password dovrà contenere caratteri di almeno 3 delle seguenti 4 categorie

- lettere maiuscole (A-Z)

- lettere minuscole (a- z)

- numeri (0 - 9)

- caratteri speciali (ad esempio ? ! @ & % $ +)

5) blocco dell'account dopo il terzo tentativo errato di connessione.

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

Il PdP adottato dall'AOO:

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

Il Sindaco, i dipendenti assegnati al gabinetto del Sindaco, il Segretario Generale, il RPF e il Responsabile dei Servizi Informatici, in ragione della funzione esercitata, possono accedere a tutti i documenti dell'Ente compresi quelli riservati. Gli Assessori, i Dirigenti, i responsabili di U.O.A. e i titolari di posizione organizzativa possono accedere a tutti i documenti dell'Ente, esclusi quelli riservati.

I componenti dell'UCP, che possono accedere a tutti i documenti con esclusione di quelli riservati.

Ogni altro utente del PdP può accedere solamente ai documenti che sono stati assegnati al Settore/UOA di appartenenza e ai Servizi/Uffici che ne fanno parte, esclusi quelli riservati.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

1.7.1.Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RPF dell'AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla modifica delle informazioni e abilitazione alla cancellazione.

1.7.2.Utenti esterni alla AOO – Altre AOO

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO potrà avvenire, quando sarà possibile attivare tale caratteristica, nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.

Le AOO che accederanno ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzeranno funzioni di accesso per ottenere le seguenti informazioni: numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali; identificazione dell'Ufficio di appartenenza del RPA.

1.7.3.Utenti esterni alla AOO

L'esercizio del diritto di accesso ai documenti, così come previsto dalla L. 241/1990 e dal D. Lgs. 33/2013 e ss.mm.ii, avviene nelle forme e nelle modalità rese pubbliche attraverso il sito istituzionale e disciplinate dal Regolamento comunale in materia di accesso a documenti, dati e informazioni, approvato con deliberazione del Consiglio Comunale n. 25 del 23 febbraio 2017. Quando è consentito l'accesso diretto per via telematica, esso può avvenire con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO.

Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili agli utenti, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

1.8. Servizio di conservazione sostitutiva

Il Delegato della Conservazione fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RPF, per una corretta esecuzione delle operazioni di salvataggio dei dati tramite flussi dati crittati.

Il Delegato della Conservazione:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

1.9. Conservazione dei documenti informatici e delle registrazioni di protocollo

Le procedure di conservazione sono descritte nel disciplinare del servizio DAX utilizzato dall'Ente ed erogato da Regione Toscana

1.10. Conservazione delle registrazioni di sicurezza

I Log degli ADS sono conservati localmente e duplicati su un apposito data base.

1.11. Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici (data breach).

La sicurezza e l'integrità dei dati di protocollo e dei documenti elettronici archiviati sono garantiti dall'applicazione informatica adottata dall'Ente, secondo un piano di sicurezza informatica del sistema informativo dell'amministrazione e definito dall'organizzazione dell'Ente, che gestisce il sistema informatico generale.

La politica in merito alla sicurezza dell'Amministrazione è finalizzata a assicurare che:

- i documenti e le informazioni trattati dall'Ente siano resi disponibili all'occorrenza, restino integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari siano custoditi in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

A tale fine l'Ente definisce:

- le politiche generali di sicurezza da adottare;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;

- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure di sicurezza a protezione dei dati personali e alla procedura di data breach.

Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.

II riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza (data breach), di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dall'Agenzia per l'Italia Digitale o a seguito dei risultati delle attività di *audit.*

In ogni caso, tale attività è svolta almeno per verifica, con cadenza annuale.

Il RC adotta, di concerto con il Responsabile dei Servizi Informatici le misure tecniche e organizzative ritenute opportune, al fine di assicurare la sicurezza dell'impianto tecnologico dell'Ente, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni.

In particolare prevede:

- la protezione fisica ed informatica della rete dell'Ente;
- la protezione fisica ed informatica dei sistemi di accesso e conservazione delle informazioni;
- l'assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti di un'identificazione utente, una password ed un profilo di autorizzazione;
- il cambio delle password e la robustezza delle stesse con la frequenza prestabilita durante la fase di esercizio, in ogni caso non inferiore a sei mesi;
- il piano di continuità del servizio, con particolare riferimento sia alla esecuzione e alla gestione dei backup da effettuarsi con frequenza almeno giornaliera, sia alla capacità di ripristino del sistema informativo in caso di evento catastrofico;
- la conservazione delle copie di riserva dei dati e dei documenti, in locali diversi e, se possibile, lontani da quelli in cui è installato il server;

•la gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);

•l'impiego e la manutenzione di un adeguato sistema antivirus e di gestione degli aggiornamenti dei sistemi operativi e dei programmi;

•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 RPF, dal titolare dei dati e, ove previsto, dalle forze dell'ordine, oppure su ordine della magistratura.

1.12. Credenziali di accesso al sistema di conservazione

Il controllo degli accessi è il processo che garantisce l'impiego del sistema informatico nel rispetto di modalità prestabilite.

Il processo è caratterizzato da utenti che accedono a strumenti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, inserimento, cancellazione, 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 ed operazioni effettuabili alle sole funzioni necessarie.

Possono essere valutate soluzioni tecniche più avanzate, come impronte biometriche, anche limitatamente a determinate funzioni.

Ogni utente può accedere esclusivamente alla documentazione relativa ai servizi di propria competenza. L'accesso ad altri documenti può essere autorizzato dal responsabile della pratica o del procedimento.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RC, 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, normalmente 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 consentano il riutilizzo.

1.13. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le autorizzazioni che possono essere rilasciate ad un utente del sistema di conservazione sostitutiva. Ciascun utente può accedere solamente ai documenti di propria competenza.

Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione.

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

1.14. Dati personali contenuti nei documenti conservati

La protezione dei dati personali contenuti nei documenti conservati è sotto la responsabilità del RC; rispetto a tali dati il delegato per l'attività di conservazione agisce come responsabile

"esterno" del titolare secondo quanto previsto dal Regolamento UE 2016/679. I suoi compiti sono analiticamente specificati per iscritto nell'ambito del contratto o convenzione di servizio.

1.15. Archivi contenenti dati personali per l'accesso al servizio di conservazione

L'Amministrazione, tramite il RC, è titolare del trattamento dei dati personali degli utenti del servizio di conservazione contenuti nell'archivio logico contenente i dati degli utenti abilitati al servizio di conservazione.

In particolare, il database di registrazione contiene:

- le informazioni relative al profilo dei soggetti abilitati al servizio di conservazione;
- ulteriori informazioni associate al suddetto profilo, generate dal delegato per l'attività di conservazione, per l'accesso al sistema da parte del soggetto.

Al delegato per la conservazione, nell'ambito del contratto di servizio, è fornita l'informativa di cui agli artt. 13 e 14 del regolamento UE 2016/679 limitatamente ai dati necessari per l'attivazione del servizio stesso.

Il database di registrazione contiene dati personali inseriti dal RC in qualità di responsabile del trattamento dei dati dei propri incaricati.

Vengono trattati i soli dati obbligatori indispensabili per il rilascio delle credenziali di accesso al sistema e per la corretta gestione del sistema di autorizzazione.

Il RC fornisce ai propri incaricati, utenti del servizio, l'informativa di cui agli artt. 13 e 14 del regolamento UE 2016/679.

Il RC attribuisce al delegato per l'attività di conservazione in outsourcing le funzioni di ADS con riferimento al sistema di conservazione e al data base di registrazione, nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, in particolare dall'art. 2, lett. c) e d).

1.16. Modalità di protezione dei dati personali

Le misure di protezione adottate relativamente ai dati personali contenuti sia negli atti conservati che nell'archivio di registrazione del servizio di conservazione sono conformi alle misure minime di sicurezza per il trattamento dei dati personali prescritte dal Regolamento UE 2016/679.

SEZIONE 6

1. ALLEGATI

A. Piano di Classificazione
B. Elenco documenti esclusi dalla registrazione di protocollo
C. Registro di protocollo d'emergenza
D. Metadati documenti informatici
E. Metadati fascicoli informatici
F. Repertori generali dell'ente
G. Massimario di selezione documentale

SEZIONE 7

1. APPROVAZIONE E PUBBLICITÀ

1.1. Modalità di approvazione ed aggiornamento del T.U.

Il T.U. viene aggiornato almeno una volta l'anno e, in ogni caso, a seguito di:

- aggiornamenti normativi;
- introduzione di nuove procedure o strumenti intesi al miglioramento dell'azione amministrativa in termini di efficacia, efficienza e trasparenza.

Il T.U. viene approvato e modificato con deliberazione della Giunta comunale.
Gli allegati sono modificati di norma con provvedimento dirigenziale.

1.2. Pubblicità

Il T.U. è reso disponibile alla consultazione del pubblico attraverso il sito web dell'Ente.

Inoltre, copia del presente T.U. è:

- resa disponibile a tutto il personale dell'Ente tramite il sistema di gestione dei flussi documentali o altro strumento accessibile al personale;
- resa disponibile al pubblico in forma cartacea, su richiesta.

1.3. Entrata in vigore

Il presente documento entra in vigore nel momento in cui la delibera di approvazione diviene esecutiva.