Comune di
Montelupo
Fiorentino

MANUALE DI GESTIONE DOCUMENTALE

Il Servizio di protocollo informatico, i flussi documentali
e la conservazione

Approvato con Deliberazione di Giunta Comunale n. 126 del 16/12/2021

Sommario

1. PRINCIPI GENERALI

1.1. Premessa

Le nuove Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia Digitale per l'Italia pubblicate il 11/09/2020 obbligano le PP.AA. ad aggiornare il Manuale di gestione documentale adottato - ai sensi del DPCM 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", articolo 3, comma 1, lettera d) - per tutte le amministrazioni di cui all'articolo 2, commi 2 e 3, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale.

Lo scopo delle Linee Guida è duplice:

- aggiornare le attuali regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale (da ora in avanti CAD), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;
- incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

Le Linee Guida adottate da AGID, ai sensi dell'art.71 del CAD hanno carattere vincolante e assumono valenza *erga omnes*.

A partire dalla data di applicazione delle Linee Guida, sono abrogati:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".

  Per quanto concerne il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", a partire dalla data di applicazione delle Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:
- art. 2 comma 1, Oggetto e ambito di applicazione;
- art. 6, Funzionalità;
- art. 9, Formato della segnatura di protocollo;
- art. 18 commi 1 e 5, Modalità di registrazione dei documenti informatici;
- art. 20, Segnatura di protocollo dei documenti trasmessi;
- art. 21, Informazioni da includere nella segnatura.

- Sempre a far data dalla data di applicazione delle presenti Linee guida, la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni" è abrogata e sostituita dall'allegato 6 "Comunicazione tra AOO di documenti amministrativi protocollati" delle Linee Guida.

1.2. Il manuale di gestione

Il presente manuale di gestione del protocollo, dei documenti e degli archivi, adottato dal Comune di Montelupo Fiorentino con Deliberazione di Giunta Comunale n. 113 del 30/12/2015, viene aggiornato sulla base delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia Digitale per l'Italia.

Il manuale di gestione, che riunisce tutte le misure organizzative e tecniche per l'attuazione di un percorso di completa digitalizzazione dell'Ente, "*descrive il sistema di gestione anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi*" ed è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione e archiviazione dei documenti.

Il presente manuale è articolato in due parti:

- nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema,
- nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

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

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intendono le definizioni in "allegato 1"

Di seguito si riportano acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RPA** - Responsabile Procedimento Amministrativo- il dipendente che ha la responsabilità

dell'esecuzione degli adempimenti amministrativi relativi ad un affare;

- **RGD** - Responsabile della Gestione documentale;
- **SdP** – Servizio di protocollo informatico;
- **DPO** – Data Protection Officer
- **UOP** - Ufficio di registrazione di Protocollo;
- **UOR** - Ufficio di Gestione - ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le norme ed i regolamenti di riferimento vedasi l'elenco riportato in “allegato 2”.

1.4. Area Organizzativa Omogenea

Il Comune di Montelupo F.no ha individuato l’Area Organizzativa Omogenea, all'interno della quale, con Delibera di Giunta 19 del 19/03/2015, è nominato il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell’articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR n. 445 del 28 dicembre 2000).
L’AOO, denominata **AOOCMF,** è stata registrata all’IPA (Indice delle Pubbliche Amministrazioni).

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

All'interno della AOO il sistema di protocollazione è distribuito: la corrispondenza, in ingresso è gestita da alcune UOP, in uscita è gestita direttamente da tutti gli UOR dell’amministrazione.

La struttura organizzativa dell’Amministrazione, approvata e aggiornata con Delibera di Giunta Comunale, è consultabile sul sito del Comune.

1.5. Principi di gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali:

- formazione,
- gestione,
- conservazione.

Il sistema di gestione informatica dei documenti, viene presidiato dal sistema J-Iride di Maggioli, in grado di governare ogni singolo accadimento che coinvolge la vita del documento ed effettuato secondo i principi generali in materia di trattamento dei dati personali.

Una corretta gestione dei documenti sin dalla fase di formazione rappresenta la migliore garanzia per adempiere agli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.
Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione in ottemperanza a quanto disposto dal CAD e dalle Linee guida. In questo contesto l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati.
Nell'ambito della gestione documentale possono essere da prevedere attività di riversamento dei documenti in altro formato diverso da quello originale allo scopo di garantire finalità gestionali o conservative.

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale o comunque derivanti dalla normativa in materia di trasparenza devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione online possa generare un prodotto atto ad assolvere i predetti obblighi è necessario che esso garantisca la conformità di quanto pubblicato all'originale, la validità giuridica dei documenti, efficacia e perdurabilità nel tempo.

1.6. Servizio per la gestione informatica del protocollo

Nella AOO è costituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il responsabile della Gestione documentale (di seguito RGD), nominato con Delibera di Giunta 83 del 08/10/2015;
In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del servizio:

- lo sviluppo e la gestione del protocollo informatico e del sistema di gestione documentale;
- l'analisi e la gestione dei flussi documentali ;
- la conservazione a norma della documentazione amministrativa, in collaborazione con il responsabile della Conservazione;
- la gestione degli archivi.

Ciascuna delle attività sopra elencate sarà descritta nei capitoli successivi del presente manuale.

1.7. Il Responsabile della Gestione Documentale

È compito del Responsabile della Gestione Documentale, o di un suo incaricato, come previsto dal DPR 445/2000 e dalle Linee Guida Agid del Maggio 2021:

- sovrintendere e curare le funzionalità del sistema;
- attribuire il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni ;
- garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto delle disposizioni di legge;
- garantire la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53 del DPR 445/2000;
- conservare le copie di cui agli articoli 62 e 63,del DPR 445/2000;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 del DPR 445/2000 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69 del DPR 445/2000;
- Prevedere adeguati meccanismi di tracciabilità dei flussi documentali;
- Autorizzare le operazioni di annullamento;
- Vigilare sull'osservanza delle disposizioni del presente manuale di gestione da parte del personale autorizzato e degli incaricati.

Il Responsabile della Gestione Documentale, per aver un sistema di gestione documentale aderente alla normativa europea, deve definire i diritti di accesso ai documenti in base ai dati personali trattati. Per questo deve fornire delle regole a tutti coloro che vengono in possesso o trattino dati personali, che rispettino la normativa in vigore sulla privacy e il codice di comportamento per i dipendenti delle Pubbliche Amministrazioni (art. 54 c.5 del Dlgs n. 165 del 2001).
In particolare, rientra nei compiti del Responsabile della Gestione Documentale informare e formare i propri collaboratori sulle modalità di condotta operativa da adottare nelle procedure che prevedono il trattamento dei dati, trasferendo conoscenza della norma e consapevolezza delle situazioni a rischio reato;

1.8. Firma elettronica, firma elettronica avanzata e qualificata, firma digitale

La normativa prevede le seguenti tipologie di firma, sebbene la firma digitale risulti la più diffusa:

- **la firma elettronica** è "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica". La cosiddetta "firma debole". Esiste un PIN abbinato a una carta magnetica o credenziali di accesso costituite da nome utente e password.

- **la firma elettronica avanzata** è “l’insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l’identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati”. È una Firma Elettronica con alcune caratteristiche di sicurezza aggiuntive: consente di identificare in maniera certa il firmatario e se il documento è stato modificato a seguito della firma; dispositivo di firma sicuro (pc, smartphone, etc.).
- **la firma elettronica qualificata** è definita come “l’insieme di dati basati su un certificato qualificato e un dispositivo sicuro per la creazione della firma”. Ai sensi dell’art. 25, c. 3, del Regolamento del Parlamento e del Consiglio dell’Unione europea 23 luglio 2014, n. 910 corrisponde alla firma digitale italiana; utilizzata per tutti i documenti per cui viene richiesto dalla normativa.
- **la firma digitale** è definita "un particolare tipo di Firma Elettronica Avanzata basata su un certificato qualificato e 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".

La firma digitale può avere i seguenti formati

- CAdES è un file con estensione “.p7m”, il cui contenuto è visualizzabile solo attraverso idonei software in grado di aprire la busta virtuale per visualizzare il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un’applicazione specifica.
- PAdES è un file con estensione “.pdf”, leggibile con i comuni reader disponibili per questo formato.
- XAdES è un file con estensione “.XML”, è possibile accedere ai metadati contenuti all’interno del documento stesso e c’è la possibilità di firmare singole parti del documento (ad esempio i documenti sottoscritti da più persone) ma necessita di un editor di lettura perché poco leggibile.

Per l'espletamento delle attività istituzionali il Comune di Montelupo F.no fornisce la firma digitale/ elettronica qualificata ai soggetti da essa delegati a rappresentarla.

1.9. Casella di Posta Elettronica Certificata

L'AOO è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita.

La casella ha il seguente indirizzo: ***comune.montelupo-fiorentino@postacert.toscana.it***
Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici dell'Amministrazione.

Il presidio della casella di posta elettronica certificata istituzionale è svolto dall'UOP SEGRETERIA GENERALE.

1.10. Sistema di classificazione dei documenti

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'Amministrazione. Esso si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze (microfunzioni) che rientrano concettualmente nella macrofunzione descritta dal titolo.
Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice dell'amministrazione.

Il **titolario** è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'amministrazione, soggette a modifiche in forza delle leggi e dei regolamenti statali. L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RGD.
Dopo ogni modifica del titolario, il RGD provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolario non è retroattivo: non si applica, cioè, ai documenti protocollati prima della sua introduzione.
Il sistema di protocollazione deve garantire la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi. Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.
Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di

approvazione del nuovo titolario e hanno durata almeno per l'intero anno.
Il titolario di classificazione adottato dall'Amministrazione è quello riportato in **"allegato 3"**

1.11. Accreditamento dell'AOO all' IPA

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA), fornendo le informazioni che individuano l'AOO e la sua struttura organizzativa.

Il codice identificativo dell'amministrazione è stato generato e attribuito autonomamente dall'amministrazione. L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.

L'amministrazione comunica tempestivamente all'IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.12. Conservazione

Nell'ambito del servizio di gestione informatica documentale si individuano due componenti:

- la prima è il backup della banca dati e dei log, assicurato dal piano della sicurezza di cui al capitolo 2;
- la seconda è la conservazione a norma presso il Conservatore accreditato AGID dei documenti informatici:
  - il registro informatico giornaliero di protocollo. Al fine di garantire la non modificabilità delle operazioni di registrazione, al termine della giornata lavorativa il registro viene generato automaticamente dal sistema in formato pdf, e entro il giorno successivo, inviato in conservazione;
  - le classi documentarie corredate dei metadati specifici, indicate al punto 10, mediante procedure batch periodiche.

1.13. Il Responsabile della Conservazione

Il Responsabile della Conservazione opera d'intesa con il Responsabile della Gestione documentale, con i Responsabili del trattamento dei dati personali. e con il Responsabile della sicurezza informatica.

Il Responsabile della Conservazione in particolare:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- avvalendosi del Conservatore accreditato AGID, definisce il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Manuale della conservazione costituisce "**Allegato 4"** al presente MdG.

1.14. Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione stabilisce percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

2. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate nell'ambito della gestione e della conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

2.1. Obiettivi

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO siano disponibili, integre e riservate;
- i dati personali, particolari e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, 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.

2.2. Politiche di sicurezza adottate dalla AOO

"Componente fisica della sicurezza". Questa componente indica la sicurezza delle apparecchiature hardware. Tutti i dispositivi classificati "di sistema" (server, apparati attivi di rete, firewall.) sono coperti da un servizio di manutenzione che garantisce tempi di intervento adeguati per il ripristino degli apparati.

"Componente organizzativa della sicurezza". La componente organizzativa della sicurezza, legata alla gestione del protocollo e della documentazione, si riferisce alle attività svolte per l'erogazione del SdP.

Le qualifiche funzionali coinvolte sono le seguenti:

- responsabile dei sistemi informativi;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali (DPO);

"Componente infrastrutturale della sicurezza". La componente infrastrutturale si riferisce alla sicurezza dei locali e dell'infrastruttura hardware dedicata.

È compito del responsabile della sicurezza e dei responsabili della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della

sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

"Componente logica della sicurezza". Per componente logica della sicurezza si intende il sottosistema di sicurezza finalizzato alla implementazione dei requisiti di sicurezza all'interno del SdP:

a) Meccanismi per il controllo degli accessi. Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico documentale avvengano secondo le modalità prestabilite (login, password). Il sistema di database traccia un file di registrazione degli accessi (file di log).
b) Funzioni per la realizzazione dell'integrità logica. Ogni utente, superata la fase di autenticazione, ha accesso solo ai dati residenti nella propria area di lavoro (scrivania virtuale) e non può accedere ad altre aree di lavoro.

I dati personali registrati nel log del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

2.3. Formazione dei documenti - Aspetti attinenti alla sicurezza

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

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura (text editor) che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, PDF/A, XML e i formati utilizzati dall'amministrazione sono redatti in conformità a quanto previsto dall'allegato 2 alle Linee Guida e sono quelli indicati nell'allegato 5.

I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, 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.

2.3.1. Gestione dei documenti informatici

Il sistema che eroga il SdP è conforme alle specifiche previste dalla normativa vigente.
I file documenti risiedono sul server che è configurato in maniera 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.
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- 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 personali particolari e/o giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato

2.3.2. Gestione della sicurezza nelle registrazioni di protocollo

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul SdP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul SdP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log dei dispositivi;
- dai log delle registrazioni dell'applicativo J-IRIDE del SdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza

addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;

- le registrazioni del modulo J-IRIDE sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione
- i supporti con le registrazioni di sicurezza sono conservati all'interno di un armadio ignifugo in un locale con controllo biometrico per l'accesso
- i log di sistema sono accessibili al personale incaricato in sola lettura;
- l'operazione di scrittura delle registrazioni del SdP, modulo J-IRIDE è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera di backup;

2.4. Trasmissione dei documenti informatici

Nella AOO 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.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il sistema di posta certificata del fornitore esterno (*provider*) di cui si avvale l'AOO, 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.

Lo scambio per via telematica di messaggi protocollati tra AOO presenta esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, particolari e/o giudiziari come previsto dal Regolamento europeo - GDPR.

Per garantire l'autenticità della provenienza e l'integrità del messaggio viene utilizzata la sottoscrizione del documento con firma digitale.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta

elettronica certificata è regolata dal Codice dell'Amministrazione Digitale.

2.5. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali, pubblica *(UserID)* e privata *(Password)* ed un sistema di autorizzazione basato sulla profilazione degli utenti.

La profilazione consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.
Queste, in sintesi, sono:

- *consultazione,* per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;
- *inserimento,* per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- *modifica,* per modificare i dati opzionali di una registrazione di protocollo;
- *annullamento,* per annullare una registrazione di protocollo autorizzata dal RSP.

Il SdP:

- 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 da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è possibile associare una *Access Control List* (ACL) che consente di stabilire quali utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere alla visualizzazione completa dei documenti protocollati.
Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

2.5.1. Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RGD dell'AOO.
Gli utenti creati non sono mai cancellati ma, eventualmente, storicizzati.

2.5.2. Accesso al registro di protocollo per utenti della AOO

La visibilità del registro di protocollo è consentita a tutti i ruoli.

Nel caso in cui sia effettuata una protocollazione riservata, la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza ed eventualmente conoscenza, il RGD e gli appartenenti a quel ruolo (permesso applicativo di protocollazione riservata associato al ruolo)

2.5.3. Accesso utenti esterni alla AOO

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

2.6. Tutela dei dati personali: GDPR e D.Lgs. 196/2003

Il Comune di Montelupo F.no all'atto della produzione di documentazione amministrativa che contiene dati personali particolari deve ottemperare al Regolamento Generale per la Protezione dei Dati Personali - GDPR, all'atto della protocollazione. In particolare gli operatoti autorizzati ad accedere al sistema di protocollo informatico, incaricati dal Responsabile della Gestione Documentale, devono attenersi alle norme: riservatezza, credenziali strettamente personali e segrete, all'atto della protocollazione se si è costretti a muoversi bisogna bloccare il pc e non divulgare informazioni riservate.

In relazione alla protezione dei dati personali trattati al proprio interno l'Ente dichiara di aver ottemperato a quanto previsto dal GDPR e dal D.L gs. 196/2003:

- nominare un Responsabile della Protezione dei Dati, figura indicata come Data Protection Officer, con l'incarico di agevolare l'attuazione del regolamento da parte del titolare del trattamento dei dati personali;
- tutelare la riservatezza dei dati, impedendone la fruizione da parte di soggetti non autorizzati;
- rispettare le procedure standard di protezione e verificare le misure tecniche adottate per garantire la piena integrità dei sistemi e dei servizi di trattamento;
- ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico, dando avviso immediato al Garante Privacy in caso di fuga di dati o attacco esterno (data breach);
- la valutazione d'impatto da violazioni (Data Protection Impact Assessment) ;
- redigere un registro delle attività di trattamento .

Secondo quanto definito nell'art. 5 del GDPR e considerato il fatto che le Pubbliche Amministrazioni devono avere un sistema documentale in grado di sostenere quanto definito nel Regolamento

Europeo stesso e rispettare il principio di tracciabilità dell'azione amministrativa, bisogna:

- identificare in modo univoco ogni documento creato o acquisito mediante la registrazione di informazioni descrittive e la sua classificazione, utili per facilitare il recupero e comprovare l'esistenza del documento (elementi contenuti nel sistema di protocollo informatico)
- definire i diritti di accesso ai documenti in base ai dati personali trattati, attribuendo a ciascun utente di protocollo precisi permessi
- stabilire i tempi di conservazione a partire dalla creazione della documentazione elaborando un piano di conservazione
- prevedere sistemi di tracciabilità dei dati e dei documenti attraverso una infrastruttura informatica avanzata

Le condizionidi cui sopra devono essere applicate anche ai sistemi di conservazione, in modo da garantire rintracciabilità, integrità e riservatezza dei documenti nel rispetto dei principi definiti dalla normativa sulla privacy.

2.7. Conservazione dei documenti informatici

Il responsabile della conservazione, si avvale del Manuale della Conservazione del conservatore accreditato AGID, per definire le regole per la conservazione dei documenti informatici.

3. IL DOCUMENTO

3.1. Il Documento analogico

Il documento analogico è definito, nell' art. 1 lettera p -bis del CAD, come la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti su supporto cartaceo. Può essere prodotto con strumenti analogici o digitali.

3.2. Il Documento informatico

Il documento informatico è definito, nell' art. 1 lettera p del CAD, come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti completamente equiparato alla forma scritta, prodotto con strumenti digitali (art. 20 del CAD).

Può essere sottoscritto con firma elettronica, avanzata, qualificata o digitale (cfr. par 3.5) Il tipo di firma utilizzata differenzia il valore giuridico del documento, secondo le norme previste dalla legge. Il documento informatico privo di sottoscrizione è solo una copia informatica, e come tale descrive la prova dei fatti e delle cose rappresentate se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime (2712 cc, 23 quater CAD, 2713 cc). L'associazione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione.

3.3. Documento amministrativo informatico

Il Comune di Montelupo Fiorentino forma gli originali dei propri documenti attraverso gli strumenti informatici secondo le modalità definite nel presente manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis, 40 -bis e 65 del CAD.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori e negli albi.

Il documento amministrativo informatico, secondo quanto stabilito dalle Linee Guida, può essere:

- redatto tramite l'utilizzo di appositi strumenti software;
- acquisito da un documento informatico per via telematica o su supporto informatico;
- acquisito da una copia per immagine su supporto informatico di un documento analogico, acquisito da una copia informatica di un documento analogico;
- registrato elettronicamente dalle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generato o raggruppato anche in via automatica da un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

I formati utilizzati devono essere quelli indicati nell'allegato 2 alle Linee Guida.

Il documento assume la caratteristica di immodificabilità se formato in maniera tale che la forma e il contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

3.4. Copie per immagine su supporto informatico di documenti analogici

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

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

3.5. Duplicati, copie ed estratti informatici di documenti informatici

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

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione ".doc" in un documento ".pdf". L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta.

3.6. Formazione del documento

I documenti dell'Amministrazione sono prodotti come documenti informatici in base a quanto previsto dalla vigente normativa.
Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

- deve trattare un unico argomento, indicato in maniera sintetica ma esaustiva dell'autore nello

spazio riservato all'oggetto;
- deve essere identificato univocamente da un solo numero di protocollo;

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai RPA.

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

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

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- il numero di protocollo;
- la data;
- l'oggetto;
- il numero degli allegati, se presenti;

La firma digitale deve essere apposta in fase di protocollazione a cura del RPA. Prima della sottoscrizione digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità come previsto dalle Linee Guida.

La sottoscrizione digitale e la contestuale protocollazione assegnano al documento amministrativo informatico la valenza giuridico-probatoria.

Il software applicativo J-Iride consente la verifica in modalità integrata della firma digitale apposta sui documenti.
La verifica visualizza i dati del soggetto firmatario, della Certification authority, della validità del certificato e la chiave pubblica.

3.7. I Metadati del documento

Secondo la definizione dell' ISO i metadati sono “dati che descrivono e definiscono altri dati in un determinato contesto".

In ambito informatico il metadato descrive il contenuto, la struttura e l'ambito in cui s'inquadra un documento informatico, per la sua gestione, conservazione e archiviazione.
Gli obiettivi dei metadati sono:

- garantire l'identificazione permanente dei singoli oggetti informativi;
- garantire l' identificativo univoco (numero di protocollo, data, autore, ecc.);
- garantire l'identificazione permanente delle relazioni tra gli oggetti informativi (ad es. indici di classificazione e fascicolatura);
- conservare le informazioni che supportano l'intellegibilità degli oggetti informativi (ad es. procedimento amministrativo cui il documento è connesso) .

Le specifiche dei metadati, indicate nel Manuale di Conservazione, soddisfano quanto definito nell'allegato 5 alle Linee Guida.

4. IL FASCICOLO

Il fascicolo è l'insieme organico e ordinato di documenti che si forma nel corso dell'attività amministrativa della AOO allo scopo di riunire, a fini decisionali o informativi, i documenti utili allo svolgimento di tale attività.

Può essere suddiviso in due tipologie:

1. Il fascicolo relativo ad un procedimento amministrativo: i documenti appartengono ad uno ed un solo procedimento;
2. Il fascicolo raggruppato per attività: fatture elettroniche, contratti, collaborazioni esterne etc.

4.1. Il fascicolo: definizione e funzione

Si possono distinguere varie tipologie di fascicolo, relative a:

- ***procedimento amministrativo*:** conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un atto finale;
- ***persona fisica*:** conserva i documenti relativi a diversi procedimenti amministrativi, distinti per affari o per attività, ma legati da un vincolo archivistico interno, relativo a una persona fisica determinata. La chiusura del fascicolo dipende dalla conclusione del rapporto giuridico con l'ente;
- ***persona giuridica*:** conserva i documenti relativi a una persona giuridica con modalità simili a quelle del fascicolo di persona fisica;
- ***attività*:** conserva i documenti relativi a una competenza proceduralizzata, per la quale esistono documenti vincolati o attività di aggiornamento procedurale e per la quale non è comunque previsto l'adozione di un provvedimento finale;
- ***affare/dossier*:** conserva i documenti relativi a una competenza non proceduralizzata né procedimentalizzata. Per gli affari non esiste un termine per la conclusione previsto da norme.

Il fascicolo può essere ulteriormente suddiviso in sottofascicoli.

Il sottofascicolo può essere chiuso prima del fascicolo, ma non viceversa, in quanto di norma trattasi di un subprocedimento o di un endoprocedimento stesso.

4.2. Il fascicolo informatico: formazione e gestione

Per i procedimenti ogni AOO ha l'obbligo di conservare in un fascicolo informatico gli atti, i documenti e i dati da chiunque formati su supporto informatico.

Un fascicolo informatico può contenere anche copie di qualunque tipo di documenti nativi cartacei

autenticati (come definito dall’art. 22 del D.lgs. n.82 del 7/03/2005 e successive modificazioni).
Il fascicolo informatico è creato dall’ufficio responsabile del procedimento.

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

- indice di classificazione (cioè titolo, classe, sottoclasse);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'AOO;
- data di apertura del fascicolo;
- AOO e UOR;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare
I fascicoli, sono annotati nel repertorio dei fascicoli.
Il repertorio dei fascicoli, ripartito per ciascuna classe di ogni titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del titolario di classificazione 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.
Il repertorio dei fascicoli è costantemente aggiornato.

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

5. FASE CORRENTE DELLA GESTIONE DEI DOCUMENTI

L'organizzazione della gestione documentale deve rispondere a criteri di efficienza ed efficacia, al fine di garantire il corretto svolgimento dell'attività giuridico-amministrativa dell'AOO e la conservazione stabile della documentazione amministrativa dell'Ente.
Tutti i documenti generati nel corso di procedimenti amministrativi e necessari al loro espletamento, costituiscono la fase corrente della gestione documentale, la quale assume un'importanza strategica per un corretto funzionamento dell'attività amministrativa e una garanzia per le esigenze di trasparenza e integrità.
Ogni struttura provvede alla corretta gestione e conservazione dei documenti e dei fascicoli di propria competenza, siano essi di natura informatica o analogica, relativi ai procedimenti in corso, attuando le disposizioni contenute nel presente manuale e ottemperando a quanto previsto dalla normativa vigente.

5.1. Gli strumenti della fase corrente

Gli Strumenti della fase corrente sono rappresentati dal registro di protocollo e dai repertori.

5.1.1. Il Registro di protocollo

Il registro di protocollo è un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso ed è idoneo a produrre effetti giuridici a favore o a danno delle parti.
Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

5.1.2. I Repertori

Per repertori si intendono quei registri in cui sono annotati documenti per i quali è prevista una registrazione particolare. Il complesso dei documenti registrati a repertorio per forma omogenea costituisce una serie.
La numerazione di repertorio si rinnova ogni anno solare: inizia il 1° gennaio e termina il 31 dicembre di ogni anno.

I repertori attivi, afferenti al sistema gestione documentale, sono i seguenti:

- registro delle delibere del consiglio comunale,
- registro delle delibere della giunta comunale;
- registro dei decreti sindacali;
- registro delle determinazioni dirigenziali;

- registro delle ordinanze.

Il software J-Iride consente la formazione di queste tipologie di documentazione in originale informatico, la gestione e l'esecuzione di tutte le operazioni previste dai diversi workflow nell'ambito del sistema di gestione documentale.

6. IL PROTOCOLLO INFORMATICO

La protocollazione rappresenta una delle fasi determinanti nella gestione documentale. Il protocollo è uno strumento tecnico necessario per gestire la documentazione organizzando la fase corrente e quelle successive, ma è anche lo strumento con cui si da evidenza amministrativa ad un atto.
La valenza amministrativa di un documento, infatti, viene definita al momento della registrazione di protocollo.

Il registro di protocollo è esso stesso un atto pubblico di fede privilegiata. Come tale, fa fede fino a querela di falso e, in particolare, circa la data e l'effettivo ricevimento o spedizione di un documento determinato, di qualsiasi forma e contenuto. Esso, dunque, è idoneo a produrre effetti giuridici tra le parti.

Il registro di protocollo ha cadenza annuale, dal 1° gennaio al 31 dicembre di ogni anno ed è unico per l'AOO dell'Ente.
Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo. Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro. Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata nel SdP viene considerata giuridicamente inesistente presso l'amministrazione.
Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici.

6.1. La registrazione di protocollo

All'atto della protocollazione vanno attribuiti i seguenti elementi obbligatori immodificabili, come definito nell'art.53 del DPR 445/2000:

- numero di protocollo;
- data di registrazione;
- corrispondente: mittente per il documento in arrivo/destinatario per il documento in partenza;

- oggetto: deve contenere in forma chiara e sintetica gli elementi identificativi dell'atto amministrativo;
- impronta : se i documenti vengono scambiati per via telematica.

Gli elementi obbligatori immodificabili servono ad attribuire al documento data e provenienza certa segnando determinate informazioni, rilevanti sul piano giuridico.

Si distinguono, inoltre:

- **Elementi obbligatori modificabili**: unità organizzativa del UOR, responsabile del procedimento amministrativo;
- **Elementi non obbligatori e modificabili:** recapiti del mittente, collegamento ad altri documenti o a fascicoli diversi da quello d'inserimento, tipologia di documento, durata della conservazione, altri tipi di annotazioni (ad es. si può annotare l'arrivo in data successiva di un secondo esemplare dello stesso documento precedentemente ricevuto e protocollato, previa verifica della sua conformità al primo)

Il sistema di protocollo informatico deve garantire il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

6.2. La segnatura di protocollo

Secondo l'art. 55 del DPR 445/2000, la " segnatura di protocollo è l'associazione o l'apposizione al documento informatico originale di informazioni riguardanti il documento stesso in forma permanente e non modificabile."

Il suo scopo è di individuare in modo inequivocabile e univoco ciascun documento soggetto a procedura di registrazione di protocollo. I dati della segnatura di protocollo di un documento informatico sono contenuti in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) .

Il Testo Unico sulla documentazione amministrativa individua alcuni elementi informativi minimi di segnatura:

- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del messaggio ricevuto o inviato (art.18 c.1)
- l'oggetto
- il mittente
- il destinatario o i destinatari.

Nel caso di documenti informatici è facoltativo riportare ulteriori informazioni:

- denominazione dell'amministrazione;
- codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo

Nel caso di documenti cartacei la segnatura di protocollo di un documento cartaceo in arrivo, avviene attraverso l'apposizione di un timbro che riporta le seguenti informazioni relative alla registrazione di protocollo:

- denominazione dell'amministrazione;
- codice identificativo dell'AOO;
- data e numero di protocollo del documento.

L'operazione di acquisizione dell'immagine dei documenti cartacei viene effettuata solo dopo che l'operazione di segnatura è stata eseguita, tramite il "segno" della segnatura di protocollo apposto sulla prima pagina dell'originale, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

L'operazione di segnatura dei documenti in partenza viene integralmente eseguita dalla UOR tramite l'apposizione del timbro o riportando il numero di protocollo e la data sul documento.

La segnatura di protocollo deve avvenire contestualmente all'operazione di registrazione di protocollo.
Le modalità operative dettagliate sono riportate nell'"**allegato 6**"

6.3. La classificazione dei documenti

La classificazione è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.
Tutti i documenti ricevuti e prodotti dalle UOR dell'Amministrazione, indipendentemente dal supporto sul quale vengono formati, sono classificati.

La *classificazione* garantisce:

- l'omogeneità tematica dei documenti dell'AOO;
- la reperibilità dei documenti rispetto all'argomento ed alla struttura;

Questa attività ha l'obiettivo principale di ordinare i documenti in modo logico, di consentire il loro inserimento in un sistema di gestione documentale in grado di governare i processi/procedimenti

amministrativi nel corso dei quali i documenti sono prodotti o acquisiti.
Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse), il numero del fascicolo ed eventualmente del sottofascicolo.

Le operazioni di classificazione vengono svolte dalle UOR.
Attraverso l'attività di classificazione da parte di ciascun ufficio responsabile del procedimento, dovrà essere attribuito a ciascun documento un indice desunto da una struttura di voci (il titolario di classificazione - "**Allegato 3**") per poi essere associato ad un fascicolo.

6.4. La fascicolazione dei documenti

I documenti vengono inseriti in fascicoli tramite aggregazione.
L'inserimento dei documenti nei fascicoli del sistema di gestione documentale permette la costituzione di un archivio organizzato. Oltre al recupero di efficienza questa prassi consente una corretta organizzazione e reperimento dei documenti di ogni procedimento, permettendo il pieno rispetto del principio di trasparenza e dell'istituto del diritto di accesso.

6.5. Modalità di produzione e di conservazione delle registrazioni

Ogni operazione di inserimento e modifica viene registrata su un file di log corredato da codici di controllo in grado di evidenziare eventuali tentativi di manipolazione. Tramite il file di log è possibile ottenere l'elenco delle modifiche effettuate su una data registrazione, permettendo quindi una completa ricostruzione cronologica di ogni registrazione e successiva lavorazione (smistamento, invio per conoscenza, restituzione, fascicolazione).

6.6. Casi particolari di registrazioni di protocollo

Tutta la corrispondenza diversa da quella di seguito descritta viene regolarmente aperta, protocollata e assegnata con le modalità e le funzionalità proprie del SdP.

6.6.1. Protocollo riservato

Sono previste e regolamentate particolari forme di riservatezza e di accesso controllato al protocollo unico per:

1. Documenti legati a vicende di persone o a fatti privati o particolari;
2. Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa (di carattere politico o gestionale).

Tali documenti sono specificatamente individuati dalla normativa vigente in particolare dall'art. 24

della legge 7 agosto 1990 n. 241 e successive modificazioni, dall'art. 8 del DPR 27 giugno 1992 n. 352 e dalla serie di norme collegate alla legge 31 dicembre 1996, n. 675 e successive modificazioni con particolare riferimento al Decreto Legislativo 30 giugno 2003 n. 196, al Codice in materia di protezione di dati personali, al Regolamento generale per la protezione dei dati personali n. 679/2016 (General Data Protection Regulation o GDPR - normativa europea in materia di protezione dei dati del 24/05/2016).
L'accesso alla documentazione riservata potrà essere effettuata dal personale avente titolo e a seguito di motivata richiesta.

IL SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.
L'UOP se trattasi di documento in arrivo, o la UOR se trattasi di documento in partenza decide se il documento da protocollare è un documento riservato, Il documento riservato è un documento visibile solo al destinatario.

6.6.2. Registrazione di protocollo differita

Se per un temporaneo ed eccezionale carico di lavoro non fosse possibile protocollare la corrispondenza cartacea ricevuta nella medesima giornata lavorativa, e solo se la mancata registrazione di protocollo potesse far venire meno il diritto di terzi (ad es. bandi di concorso, bandi di gara,), il responsabile della gestione documentale può autorizzare, con provvedimento motivato, la protocollazione differita che consiste nel differimento dei termini di registrazione.
Al provvedimento motivato deve essere allegato e protocollato un elenco contenente gli elementi identificativi dei documenti non protocollati
I documenti protocollati in data successiva alla data di ricezione devono riportare la data di ricevimento all'interno della registrazione di protocollo.

6.6.3. Domande di partecipazione a concorsi

L'UOR competente informa con congruo anticipo Il RSP dell'AOO in merito alla scadenza dei bandi di concorso al fine di organizzare la gestione delle domande in ingresso.

La corrispondenza ricevuta:

- con rimessa diretta dall'interessato, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.
- per via telematica, viene protocollata al momento del ricevimento, dando ricevuta di consegna per email o pec con i riferimenti del protocollo (numero e data)
- per posta, viene protocollata al momento della ricezione e gli estremi della protocollazione sono comunicati via email o telefonicamente al mittente.

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, per via telematica e per posta. gli stessi saranno accantonati e protocollati successivamente entro le 24 h, o 48 h. se di sabato, riportando nella registrazione di protocollo data e ora di ricevimento del documento.
In caso di rimessa diretta, al mittente viene rilasciata ugualmente ricevuta con data e ora di consegna, ma senza gli estremi del numero di protocollo, che saranno comunicati successivamente.

6.6.4. Protocollazione di documenti inerenti gare di appalto (cartacei)

Per motivi organizzativi tutti gli UOR sono tenuti ad informare con congruo anticipo il RSP dell'AOO in merito alle scadenze di gare e bandi di ogni genere.
La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo", o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede ad inoltrarla alla UOR competente che provvede ai necessari adempimenti.
Dopo l'apertura delle buste, l'UOR che gestisce la gara riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

6.6.5. Integrazioni documentarie

L'operatore di protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento e gli eventuali allegati.
Tale verifica spetta al RPA.
La mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.
I documenti pervenuti ad integrazione di quelli già disponibili, sono protocollati con una nuova registrazione dalla UOP sul protocollo generale e, a cura del RPA, vengono classificati ed inseriti nel relativo fascicolo.

6.6.6. Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati all'UOP Segreteria, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

6.6.7. Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RGD attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, sono protocollate su richiesta del RGD e identificate con la dicitura "mittente sconosciuto o anonimo" e "documento non sottoscritto".
Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.
È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

6.6.8. Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica convenzionale non consente una sicura individuazione del mittente, è l'UOR che riceve la comunicazione a valutare i contenuti, l'attendibilità del mittente e decidere se trasmetterla all'UOP per la protocollazione.

6.6.9. Fatture

Le fatture provenienti dal SDI pervengono al SdP.
Esse sono protocollate sul registro ufficiale di protocollo in modalità automatica e inviate quotidianamente, in originale, alla UOR competente.
Il registro delle fatture è costituito sull'apposito software dedicato.

6.6.10. Istanze web

Le istanze presentate tramite portali web sono ricevute dal sistema J-Iride che le protocolla automaticamente e ne restituisce gli estremi di protocollazione direttamente al portale web.

Le istanze presentate tramite il sito istituzionale dell'Ente, al quale il cittadino si accredita mediante identità digitale, pervengono al sistema J-Iride tramite mail e vengono protocollate tramite le UOP. Gli estremi di protocollazione vengono inviati via email al richiedente la protocollazione.

6.7. Annullamento di una registrazione di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile - 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 l'intera registrazione di protocollo.
Nel record di protocollo devono apparire, in forma ben visibile, oltre agli elementi già indicati, anche data e ora dell'annullamento, nonché il codice identificativo dell'operatore che ha effettuato l'annullamento.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la

lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.
Se viene effettuata una richiesta di annullamento per un mero errore materiale, si potrà effettuare una nuova protocollazione del medesimo documento solo successivamente ad annullamento completato.
Solo il RGD, o il vicario, sono autorizzati ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RGD o il vicario.

6.8. Documenti pervenuti erroneamente

6.8.1. Documenti digitali pervenuti erroneamente

L'addetto al protocollo, in caso di documenti digitali pervenuti erroneamente per via telematica (PEC, INTERPRO, APACI):

- se protocollati, previa autorizzazione del RSP, provvede o ad annullare il protocollo stesso o a protocollare il documento in uscita collegandolo al protocollo in entrata, indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente;
- se non protocollati, ripudia il messaggio con indicazione al mittente dell'errata destinazione.

6.8.2. Documenti cartacei pervenuti erroneamente

La busta, ricevuta per errore, se è indirizzata ad altra amministrazione non deve essere aperta e deve essere restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

Nel caso in cui la busta ricevuta per errore venga aperta e il documento cartaceo protocollatoto, l'addetto al protocollo, previa autorizzazione del RSP, può:

- annullare il protocollo stesso;
- provvedere a protocollare il documento in uscita, indicando nell'oggetto "protocollato per errore";

In entrambi i casi il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

6.9. Il registro giornaliero di protocollo

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione

documentale J-Iride, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, immodificabile e integra.

6.10. Valore giuridico del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente attribuendo valore giuridico-probatorio alla registrazione.

Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale della rete.

6.11. Il registro di emergenza

Il Responsabile della gestione documentale dell'AOO, o un suo incaricato, ha la facoltà di attivare il registro di emergenza ogni qualvolta, per cause tecniche, non sia possibile utilizzare la normale procedura informatica per un periodo che si prolunghi oltre le **3 ore lavorative**.
Sul registro di emergenza sono riportate:

a) Causa, data ed ora d'inizio dell'interruzione,
b) Data ed ora del ripristino della funzionalità del sistema
c) Estremi dell'autorizzazione all'uso del **Registro di Emergenza**

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le 24 ore, per cause di eccezionale gravità, il responsabile della gestione documentale autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.
Alla chiusura del registro di emergenza, non appena sia tornata disponibile la normale procedura informatica, tutti i documenti di cui sia stata eseguita la registrazione di emergenza devono essere acquisiti nel protocollo informatico e sulla corrispondente registrazione deve essere annotato l'estremo della registrazione di emergenza.
In questo caso il documento sarà registrato con due numeri diversi:

- l'efficacia giuridico-probatoria è garantita dal numero del registro di emergenza;
- il numero di Protocollo Generale garantirà l'unicità delle registrazioni.

Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Causa dell'interruzione: _____
Data inizio evento: __/__/____ ___:___ Data fine evento: __/__/____ ___:___
Annotazioni: _____
Numero protocollo: Iniziale _____ finale _____ Pagina n. _____

DATA REGISTR.	Numero	DIR. (E/U)	TITOLARIO	MITTENTE/DESTINATARIO	OGGETTO

Questa attività è coordinata dal RGD.

6.12. L'utilizzo della Posta Elettronica Certificata

La casella di Posta Elettronica Certificata è presidiata, per la ricezione di documenti, dall'UOP Segreteria e segue le regole di assegnazione previste.

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

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente, ovvero non siano dotati di firma elettronica e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio, con il formato di origine, è protocollato, smistato, assegnato e inserito nel sistema di gestione documentale. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

La UOP previa verifica della validità e della leggibilità del documento, procede alla registrazione di protocollo e alla assegnazione agli UOR di competenza.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è trattato come previsto al punto 6.8.1

La trasmissione di un documento tramite PEC è consentito a tutte le UOR dell'Amministrazione e

avviene in base alle seguenti modalità:

- redazione del documento con un sistema di videoscrittura;
- firma digitale del documento da parte del RPA;
- registrazione di protocollo in uscita nel SdP, allegando il documento firmato digitalmente;
- inviare il documento al destinatario dotato di casella di posta elettronica certificata tramite apposita funzione del software applicativo;

L'utilizzo della posta elettronica certificata (PEC) garantisce:

- la conoscenza in modo inequivocabile della data e dell'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;

Le ricevute di ritorno dal gestore di PEC dell'Amministrazione, sono classificati in:

- conferma di ricezione;
- notifica di eccezione;
- avvenuta consegna;
- mancata consegna;

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica amministrazione (IPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata delle Pubbliche amministrazioni.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa, vigente e alle relative regole tecniche sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notifica per mezzo della posta nei casi consentiti dalla legge.

L'Amministrazione, in base a quanto previsto dalla vigente normativa, deve comunicare con i soggetti dotati di PEC in modalità digitale.

6.13. Il sistema interoperabile InterPro

L'interoperabilità di protocollo permette a due sistemi di protocollo informatico di trattare in maniera automatica l'uno le informazioni trasmesse dall'altro. Il sistema consente quindi lo scambio di documenti digitali tra amministrazioni e ne permette il trattamento automatico al protocollo.

Il software applicativo J-Iride è conforme alle RFC di Regione Toscana relativamente al sistema InterPRO e consente l'interscambio dei documenti di protocollo e le relative informazioni accessorie con sistemi di altre PP.AA.

Il sistema di protocollo interoperabile InterPRO è presidiato, per la ricezione di documenti, dall'UOP Segreteria e segue le regole di assegnazione previste.

La trasmissione di un documento tramite InterPro è consentito a tutte le UOR dell'Amministrazione e avviene in base alle seguenti modalità:

- redazione del documento con un sistema di videoscrittura;
- firma digitale del documento da parte del RPA;
- registrazione di protocollo in uscita nel SdP, allegando il documento firmato digitalmente;
- inviare il documento al destinatario registrato all'IPAR di Regione Toscana tramite apposita funzione del software applicativo;

L'utilizzo del sistema InterPro garantisce:

- di conoscere in modo inequivocabile la data e l'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna all'AOO dichiarata dal destinatario;
- la ricezione del file XML contenente il numero di protocollo dell'Amministrazione destinataria.

6.14. Il sistema telematico Ap@ci

Ap@ci è il sistema di Regione Toscana con cui privati cittadini, imprese e associazioni possono usare per inviare documenti all'amministrazione.

Sono accettati documenti con formati adatti alla conservazione. E' possibile inviare anche più allegati alla stessa comunicazione. Il sistema è presidiato da parte dell'UOP Segreteria che provvede alla registrazione nel SdP ed invia al mittente ricevuta nella casella di mail.

L'utilizzo del sistema Ap@ci garantisce:

- di conoscere in modo inequivocabile la data e l'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna alla casella mail del mittente;

Il soggetto che scrive all'amministrazione tramite Ap@ci elegge il proprio domicilio elettronico.

L’Amministrazione, in base a quanto previsto dalla vigente normativa, ha l’obbligo di comunicare con tale soggetto in modalità digitale.

7. FLUSSO DI LAVORAZIONE DEI DOCUMENTI

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

I documenti, siano essi analogici o informatici, in base allo stato di trasmissione si distinguono in:

- **Documenti in arrivo:** si intendono tutti i documenti di rilevanza giuridica e amministrativa acquisiti dall'Amministrazione indirizzati sia da persone fisiche che da persone giuridiche (soggetto pubblico o privato);
- **Documenti in uscita:** si intendono i documenti di rilevanza giuridica e amministrativa prodotti dall'Amministrazione pubblica nell'esercizio delle proprie funzioni e indirizzati ad un diverso soggetto pubblico o privato, a persone fisiche ed anche ai propri dipendenti nell'esercizio delle loro funzioni;
- **Documenti interni:** si definiscono documenti interni quei documenti scambiati tra i diversi uffici appartenenti alla medesima AOO

  I documenti interni possono essere formali o informali
  - **Documenti formali**: hanno una qualche rilevanza amministrativa verso terzi
  - **Documenti informali**: sono comunicazioni scambiate tra gli uffici tramite la posta elettronica e non interessano il sistema di protocollo

Le UOP non effettuano fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

7.1. Flusso dei documenti in ingresso alla AOO

Per "documento in ingresso" s'intende quel documento amministrativo inviato da un soggetto esterno all'AOO e assume rilevanza giuridico-probatoria.

7.1.1. Ricezione dei documenti cartacei

I documenti che arrivano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente all'UOP Segreteria.

La consegna "brevi manu" direttamente dall'utenza viene effettuata presso l'Ufficio Unico Amministrativo.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti, e successivamente aperti per gli ulteriori controlli preliminari alla registrazione; la busta o contenitore si allega al documento per la parte relativa ai timbri postali.

La corrispondenza relativa a procedure negoziali aperte o ristrette è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.
La corrispondenza recante la dicitura "RISERVATA" , "SPM" o "PERSONALE" viene trattata con le modalità descritte;

La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, viene trattata con le modalità descritte nei successivi capitoli.

Nel caso di documenti pervenuti direttamente ad una UOR, questa deve consegnarli alle UOP per la protocollazione.

La documentazione cartacea ricevuta, a seguito delle operazioni di registrazione e segnatura di protocollo previste dal presente MdG a cura delle UOP competenti, viene assegnata alle UOR in originale a seguito della scansione e la conseguente assegnazione telematica.
Il personale preposto all'apertura e alla registrazione della corrispondenza è regolarmente autorizzato al trattamento dei dati personali in qualità di "incaricato al trattamento".
Qualora la corrispondenza riservata o personale sia smistata per errore ad un ufficio diverso, quest'ultimo, a tutela dei dati personali eventualmente contenuti, non apre le buste o i contenitori e li rinvia, entro la giornata lavorativa successiva, all'UOP che ha effettuato la registrazione.

7.1.2. Rilascio di ricevute attestanti la ricezione di documenti cartacei

Quando il documento cartaceo è consegnato "brevi manu" dal mittente, o da altra persona incaricata, all'Ufficio Unico Amministrativo, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'Ufficio Unico Amministrativo che lo riceve, a seguito delle operazioni di segnatura e di protocollazione, provvede alla stampa della relativa ricevuta tramite specifica funzione del software applicativo.

Nel caso non sia possibile stampare la ricevuta, le UOP possono consegnare al mittente copia del documento con apposizione del timbro, contenente numero del protocollo, data e indicazione della denominazione dell'Ente.

La semplice apposizione del timbro datario da parte dell'Ufficio Unico Amministrativo per la tenuta del protocollo, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale in merito alla ricezione ed all'assegnazione del documento.

Nel caso di corrispondenza pervenuta direttamente ad una UOR, questa deve consegnarla ad una

UOP preposta allo scopo di ottenere una ricevuta valida.

7.1.3. Ricezione dei documenti informatici

I documenti informatici possono pervenire secondo i canali descritti nei precedenti capitoli:

1. PEC istituzionale
2. InterPRO
3. Ap@ci

I documenti informatici che pervengono tramite questi canali vengono protocollati dall'UOP Segreteria.

I documenti informatici possono essere recapitati anche per altri canali.

Nei casi in cui con un documento cartaceo siano trasmessi gli allegati su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione. Superata questa fase il documento viene inserito nel flusso di lavorazione.

I documenti digitali che pervengono alle caselle di posta elettronica ordinaria sono trattati come al punto 6.6.8. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

I documenti digitali che pervengono all'Amministrazione tramite altri sistemi (es. moduli web, flussi dati, etc) vengono trattati come al punto 6.6.10.

7.1.4. Rilascio di ricevute attestanti la ricezione di documenti informatici

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

L'Amministrazione provvede inoltre all'invio di un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso del documento ricevuto e della sua presa in carico.

7.1.5. Attività di protocollazione dei documenti in ingresso

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli standard e le modalità indicate nel capitolo 6.

7.1.6. Archiviazione delle copie per immagine dei documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono

acquisiti in formato immagine *(copia per immagine di documento analogico)* attraverso un processo di scansione che avviene secondo le fasi di seguito indicate:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico *file;*
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento del file delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;

Tale attività, come indicato nell'allegato 3 alle Linee Guida, deve soddisfare quanto indicato dal CAD all'art. 22 comma 1bis del CAD:
«la copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia»

Nel modello di certificazione di processo devono concorrere due elementi fondamentali:

- la presenza di una procedura tecnologica in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia;
- la previa descrizione e certificazione di questo processo, al fine di conferire ai documenti risultanti dal processo di scansione l'efficacia probatoria prevista:
  *«Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le regole tecniche stabilite ai sensi dell'articolo 71». (*art. 22 comma 2 del CAD)

Le copie per immagine dei documenti cartacei sono archiviate nel sistema informatico J-Iride, secondo le regole vigenti, in modo non modificabile al termine del processo di scansione. La validazione delle copie avviene secondo le modalità descritte nel presente paragrafo..

Gli originali dei documenti cartacei ricevuti di norma vengono ricevuti dalle UOR contestualmente all'assegnazione telematica.

7.1.7. Archiviazione dei documenti informatici

I documenti informatici ricevuti dall'Amministrazione sono archiviati nel sistema informatico J-Iride, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

7.1.8. Assegnazione, presa in carico dei documenti, classificazione e fascicolazione

Gli addetti alla UOP provvedono ad inviare il documento alla/e UOR responsabile/i.

L'UOR provvede alle seguenti operazioni:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP assegnataria;
- in caso di verifica positiva, esegue l'operazione di presa in carico ed il RPA procede con la corretta fascicolazione e classificazione sulla base delle procedure in essere presso l'AOO.

7.1.9. Casi di rifiuto

Per rifiuto si intende la restituzione da parte di un ufficio di un protocollo erroneamente assegnato per competenza. Il rifiuto deve essere accompagnato da un'annotazione che ne motivi la restituzione e che indichi l'ufficio competente, se conosciuto. Il documento informatico ritorna così in carico alla UOP assegnataria che provvederà ad inoltrarlo all'ufficio competente.
Detto rifiuto deve avvenire entro 48 h dall'assegnazione.
Non devono restare documenti in carico alle UOP e tutti i documenti devono avere un assegnatario per competenza.

7.1.10. Conservazione dei documenti e dei fascicoli nella fase corrente

Ciascuna UOR è responsabile della organizzazione e della tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e all'archiviazione dei documenti al loro interno.
Il RPA della UOR stabilisce se il documento assegnatogli dalla UOP debba essere ricollegato ad un affare o procedimento in corso e pertanto debba essere inserito in un fascicolo già esistente oppure se il documento si riferisce a un nuovo affare, o procedimento, per cui è necessario aprire un nuovo fascicolo.

A seconda delle ipotesi, si procede come segue:

- se il documento si ricollega ad un *procedimento in corso,* l'operatore:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato;
- se il documento dà avvio ad un *nuovo fascicolo,* il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo;
  - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;

7.2. Flusso dei documenti in uscita dalla AOO

Per "documento in uscita" s'intende quel documento amministrativo prodotto da ciascuna UOR

dell'Amministrazione nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinato ad essere trasmesso ad un soggetto esterno.
Per le modalità operative di protocollazione in uscita si rimanda all'allegato 6

7.2.1.Verifica del documento, registrazione di protocollo e segnatura

È a cura della UOR provvedere ad eseguire le seguenti verifiche di conformità del documento:

- lo standard formale del documento;
- la corretta indicazione del destinatario;
- la necessità dell'apposizione di firma digitale;
- eventuale presenza di allegati.

Superate le verifiche, l'UOR provvede:

- alla registrazione nel protocollo generale e all'apposizione del numero di protocollo sul documento principale;
- all'apposizione di firma digitale;
- alla fascicolazione come descritto dal paragrafo 7.1.12..
- all'inoltro del protocollo stesso.

7.2.2.Trasmissione di documenti informatici

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

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

La trasmissione avviene secondo quanto indicato ai precedenti capitoli e con le apposite funzioni del software applicativo J-Iride.

7.2.3. Inserimento delle ricevute di trasmissione nel repository del documento

Le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate automaticamente all'interno del relativo repository.
Le UOR curano l'archiviazione delle ricevute di ritorno delle proprie raccomandate inviate.

7.2.4. Trasmissione di documenti cartacei, invio alla Segreteria e affrancatura

I documenti devono essere prodotti come documenti informatici e sottoscritti con firma digitale.

Le UOR dell'Amministrazione, dopo la registrazione di protocollo, provvedono alla stampa in copia conforme del documento originale informatico e degli eventuali allegati. Dopodiché, imbustano i documenti così prodotti e li consegnano all'UOP Segreteria che ne cura l'invio tramite il servizio di pick-up postale.

La compilazione dei moduli contenenti i dati delle spedizioni è a cura della UOP Segreteria.

8. REGOLE PER L'ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

Il SdP per l'assegnazione della documentazione pervenuta all'Amministrazione si basa sulla struttura organizzativa indicata nell'allegato " 7 ", che riporta l'articolazione della AOO in UOR e UOP.

8.1. L'attività di assegnazione

Di seguito viene descritta con maggiore dettaglio l'operazione di assegnazione dei documenti ricevuti illustrata nel flusso di lavorazione del precedente capitolo.

L'attività di assegnazione consiste nell'operazione di inviare direttamente dalla UOP il documento protocollato e segnato all'UOR competente e la contestuale trasmissione del materiale documentario oggetto di trattazione.
Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel RPA designato.

Preso atto dell'assegnazione, il RPA verifica la competenza e, se esatta, provvede alla presa in carico del documento che gli è stato assegnato; se l'assegnazione risulta errata, provvede, entro 48 ore, al rifiuto e il documento torna all'UOP che lo ha protocollato, per la sua riassegnazione.

L'UOR competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.

Il SdP memorizza tutti i passaggi, tracciando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia individua i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.
L'assegnazione può essere effettuata: per conoscenza o per competenza.

Nel caso di documenti in formato digitale le UOR assegnatarie del documento per "competenza" e/o per "conoscenza" lo ricevono esclusivamente in formato digitale.

Nel caso di documenti in formato cartaceo la UOR che ha ricevuto l'assegnazione per "competenza" riceve sia il documento cartaceo che digitale, nel caso vi sia anche assegnazione per "conoscenza" la UOR assegnatarie del documento riceve unicamente copia digitale
Per le modalità operative di protocollazione si rimanda all'allegato 6.

9. DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

9.1. Elenco documenti esclusi

Sono, esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 come riportato nell'allegato “8 ”.

9.2. Elenco documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'allegato “9”. Tale tipo di registrazione consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti. Le funzioni sono coordinate con il RGD.

10. IL SISTEMA DI CONSERVAZIONE

Il servizio archivistico è competente a gestire l'intera documentazione archivistica - informatica e analogica, ovunque trattata, distribuita o conservata, ai fini della sua corretta collocazione, classificazione, e conservazione. Al servizio archivistico è preposto il responsabile della conservazione.

10.1. Principi generali

Come Archivio si intende il complesso dei documenti prodotti e acquisiti nello svolgimento della attività e l'esercizio delle funzioni dall'amministrazione comunale.
Fanno parte dell'archivio dell'Amministrazione anche gli archivi e i documenti acquisiti per dono, deposito, acquisto o qualsiasi altro titolo.

L'archivio è suddiviso funzionalmente nelle seguenti sezioni:

- ARCHIVIO CORRENTE: il complesso dei documenti relativi a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente;
- ARCHIVIO DI DEPOSITO: il complesso dei documenti relativi a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico;
- ARCHIVIO STORICO: il complesso dei documenti relativi a procedimenti conclusi da oltre 40 anni e destinati, previa operazione di scarto, alla conservazione perenne nella sezione separata d'archivio.

10.2. Misure di protezione e conservazione

Gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico sono beni culturali inalienabili.

I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'Amministrazione, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.
I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.
Il responsabile della gestione documentale in accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati

personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR).

L'archivio non può essere smembrato, e deve essere conservato nella sua organicità.
L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della Soprintendenza Archivistica regionale.
Anche lo scarto dei documenti dell'archivio è subordinato all'autorizzazione della Soprintendenza Archivistica regionale,

10.3. Movimentazione dei fascicoli cartacei

Il responsabile della gestione documentale, in accordo con il responsabile della conservazione e acquisito il parere del responsabile della protezione dei dati personali, cura la procedura di trasferimento dei fascicoli cartacei relativi a procedimenti conclusi e affari esauriti, nell'archivio di deposito dell'Amministrazione, stabilendo modi e tempi del versamento dall' archivio corrente a quello di deposito.
Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli ed i repertori avevano nell'archivio corrente.

10.4. Movimentazione dei fascicoli e dei documenti informatici

Il responsabile della gestione documentale, in accordo con il responsabile della conservazione, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, organizza il trasferimento dei fascicoli elettronici relativi a procedimenti conclusi e affari esauriti, nel sistema di conservazione a norma individuato dall'Amministrazione previa autorizzazione della Soprintendenza archivistica della Toscana.
Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.
Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato all'art. 44, comma 1-bis, del CAD;

10.5. Il processo di conservazione dei documenti informatici

Il trasferimento avviene sulla base di quanto indicato nel Manuale di Conservazione e comunque con procedure batch periodiche a corredo del software di gestione documentale.

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

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

Il processo di conservazione è descritto con il dettaglio delle specifiche funzionalità nel Manuale di Conservazione del conservatore accreditato AGID individuato dal Comune di Montelupo F.no.

Le classi documentali attivate dal ns. ente per la conservazione digitale sono le seguenti:

- Decreti-v2-072016
- Delibere-Consiglio-v2-072016
- Delibere-Giunta-v2-072016
- Determinazioni-v2-072016
- FatturazionePA-v2-072016
- Ordinanze-v2-072016
- Protocollo-Generale-v2-072016
- Registro-Protocollo-v2-072016
- Contratti-v2-072016
- Documenti-Generici-v2-072016
- OPI-v2-072016

10.6. Procedure di scarto

Sulla base del piano di conservazione di cui all'allegato "10", l'Amministrazione, periodicamente, effettua la procedura di scarto sempre nel rispetto della normativa sui beni culturali ed in particolare alle regole della Soprintendenza archivistica della Toscana.

10.7. Consultazione ai fini giuridico-amministrativi

La richiesta di consultazione dei documenti amministrativi, può pervenire dall'interno dell'amministrazione, oppure da utenti esterni per scopi giuridico-amministrativi o per scopi storici.

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15.

I RPA, in caso di necessità, possono richiedere la documentazione amministrativa tramite registrazione di protocollo con documento interno formale.
Nel caso di fascicoli/documenti informatici l'AOO ha accesso a tale documentazione tramite il sistema di gestione documentale.
Le singole pubbliche amministrazioni individuano, comunque, le categorie di documenti da esse formati o rientranti nella loro disponibilità sottratti all'accesso.

Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici, sempre nel rispetto dei principi definiti dal Regolamento Europeo – GDPR.

10.8. Modalità di esibizione

Il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione secondo le modalità descritte nel manuale di conservazione, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e modalità di accesso diverse, in funzione delle tipologie di dati personali trattati, nonché delle operazioni di trattamento consentite.

10.9. Consultazione da parte di personale esterno all'amministrazione

La consultazione dei documenti e le richieste di accesso agli atti da parte di personale esterno all'amministrazione, sono disciplinati dal vigente regolamento "Rapporto tra i cittadini e l'amministrazione comunale nello svolgimento delle attività e dei procedimenti amministrativi" - approvato con delibera di Consiglio Comunale n. 27 del 29/09/2010.

La richiesta di accesso ai documenti presentata all'Amministrazione viene protocollata dalla UOP che la riceve e che provvede ad assegnarla al servizio archivistico.

Nel caso di richieste di accesso ai documenti della sezione storica dell'archivio, le medesime devono essere inviate all'Amministrazione. Analoga richiesta di accesso può essere indirizzata alla Soprintendenza archivistica, utilizzando i moduli predisposti dalla stessa Soprintendenza archivistica, poiché, pur non essendo esplicitamente richiesta dalla normativa, essa è comunque utile a fini statistici e di tutela.

Nel caso di richieste di accesso a documenti informatici in conservazione a norma, il personale autorizzato provvede a recuperare il pacchetto di distribuzione come indicato nel paragrafo precedente.

L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico. La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, 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 rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

10.10. Consultazione da parte di personale interno all'amministrazione

Nel caso di fascicoli cartacei le UOR dell'amministrazione, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica previa apposita richiesta.

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

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa su un apposito modello contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, la UOR di appartenenza e la firma.

Copia della richiesta di consultazione viene conservata nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile del servizio archivistico.

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

Nel caso di accesso a fascicoli o documenti informatici, le formalità da assolvere quelle indicate nel paragrafo 10.7.

In qualsiasi 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.

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

11.1. Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di Gestione" su proposta del RGD con Deliberazione di Giunta Comunale.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia,
- efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal RGD

11.2. Pubblicità del presente manuale

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

Inoltre copia del presente manuale è:

- fornita a tutto il personale dell'AOO e se possibile, viene resa disponibile mediante la rete intranet;
- pubblicato sul sito istituzionale dell'amministrazione.

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