APSP Cesare Benedetti di Mori

Manuale di gestione del protocollo informatico

(art.5 DPCM 03 dicembre 2013)

Sommario

PARTE PRIMA - INTRODUZIONE E ATTI PRELIMINARI

1. Introduzione

Il presente manuale, previsto dall'art.5 del D.P.C.M. 03/12/2013, descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico e per la gestione dei flussi documentali e degli archivi.
L'adozione del sistema di protocollo informatico e la gestione informatica dei documenti, la cui finalità è quella di migliorare l'efficienza interna degli uffici dell'Ente attraverso l'eliminazione del cartaceo e la razionalizzazione dei flussi documentali, rispondono alle innovazioni introdotte dalla seguente normativa:

- Legge 7 agosto 1990, n. 241 - Nuove norme sul procedimento amministrativo e di diritto di accesso ai documenti amministrativi e successive modifiche ed integrazioni;
- DPCM 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428;
- DPR 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- DPR 7 aprile 2003, n. 137 - regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma delI'art. 13 del D. Lgs. 23 gennaio 2002, n. 10;
- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali;
- D.Lvo 7 marzo 2005, n. 82 recante il Codice dell'Amministrazione Digitale
- DPCM 3 dicembre 2013, recante regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis,47,57-bis e 71 del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005.

1.2 Finalità del manuale

Le disposizioni normative sulla gestione informatica dei documenti consentono, inoltre, di migliorare la trasparenza dell'azione amministrativa attraverso una stretta sinergia tra le strutture organizzative dell'Ente. Il Manuale di gestione è uno strumento complesso che in alcune parti deve necessariamente subire aggiornamenti frequenti, ma che costituisce un punto di riferimento per chiunque operi all'interno dell'ente o abbia scambi documentali con esso.

1.3 Definizioni

Ai fini del presente manuale si intende:

- per Amministrazione, l'Azienda Pubblica di Servizi Alla Persona Cesare Benedetti di Mori, d'ora in poi denominata "Azienda";
- per AOO (Area Organizzativa Omogenea), l'"Azienda" costituita da diverse unità organizzative responsabili (UOR) che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali;
- per Ufficio di Spedizione, si intende l'ufficio protocollo, nel quale la corrispondenza viene convogliata per essere poi inoltrata alle Poste;
- per documento amministrativo si intende ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, prodotti o, comunque, utilizzati ai fini dell'attività amministrativa;
- per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico, redatto in conformità delle regole tecniche

previste dalla legge, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'art. 2712 del Codice Civile;

- per documento analogico si intende un documento amministrativo prodotto su supporto non informatico. Di norma un documento analogico è un documento cartaceo;
- per versione analogica di un documento informatico, una copia, di norma cartacea, di un documento prodotto in origine su supporto informatico;
- per firma elettronica (firma digitale debole), l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- per firma elettronica avanzata (firma digitale), la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare il controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- per firma elettronica qualificata, la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma elettronica;
- per gestione dei documenti, l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione nell'ambito del sistema di classificazione d'archivio adottato; essa verrà effettuata mediante sistemi informativi autorizzati;
- per protocollo, l'insieme delle procedure e degli elementi attraverso i quali i documenti vengono trattati sotto il profilo giuridico -gestionale;
- per protocollo informatico (o sistema di gestione informatica dei documenti), l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dall'amministrazione per la gestione dei documenti;
- per segnatura di protocollo, l'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso;
- per classificazione, l'attività che consente di organizzare tutti i documenti correnti prodotti dall'Amministrazione, secondo uno schema articolato di voci (il cd. titolario) che descrive l'attività del soggetto produttore identificandone funzioni e competenze;
- per assegnazione, l'operazione d'individuazione dell'ufficio competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
- per titolario di classificazione, un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'Amministrazione, che consente di classificare, in maniera logica, sistematica e coerente, la documentazione archivistica, che venga prodotta o comunque acquisita dall'Amministrazione, durante lo svolgimento dell'attività amministrativa;
- per fascicolo, l'unità archivistica che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare.

1.4 Atti di organizzazione preliminari

Con l'entrata in vigore del protocollo informatico, l'Azienda ha provveduto all'adozione di specifici atti di organizzazione per perseguire gli obiettivi organizzativi e funzionali sottoriportati, così come previsto dal decreto legislativo 3 febbraio 1993, n. 29 (e successive modificazioni) e in armonia con le disposizioni già previste dal DPR 20 ottobre 1998, n. 428 art 3 (oggi confluito nel DPR 445/2000).

Questo Ente ha provveduto ad adempiere ai sopracitati atti di organizzazione nel seguente modo:

a) individuazione delle Aree Organizzative Omogenee come Settori della struttura nelle quali adottare il protocollo unico.
b) individuazione delle Unità Organizzative Responsabili come Uffici in cui è articolata ciascuna AOO e che afferiscono al protocollo unico.
c) introduzione del protocollo unico ed eliminazione dei protocolli interni;
d) approvazione di un titolario di classificazione.

Una volta introdotti questi strumenti si è passati alla descrizione di un sistema informativo documentale efficace, efficiente ed economico, che garantisce la comunicazione interna ed esterna e il monitoraggio sui flussi documentali.

1.5 Individuazione dell'Area organizzativa omogenea (AOO) – Settori di riferimento della struttura

Nell'Azienda sono stati considerati come Settori della struttura ciascuna "entità" dotata di autonomi poteri di organizzazione e gestione.
È stata individuata un'unica area organizzativa omogenea nell'Amministrazione di questa Azienda.
Un'area organizzativa omogenea è l'insieme definito delle unità organizzative responsabili (UOR) di una amministrazione che usufruiscono, in modo omogeneo e coordinato, di comuni servizi per la gestione dei flussi documentali.
All'interno della AOO il sistema di protocollazione è unico. Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, mentre è decentralizzato per la corrispondenza in uscita, attraverso tutti gli UOR.

1.5.1. Individuazione delle unità organizzative responsabili (UOR)- Uffici di riferimento

Una unità organizzativa responsabile (UOR) è un sottoinsieme di una AOO, cioè un complesso di risorse umane e strumentali cui sono state affidate competenze omogenee nell'ambito delle quali i dipendenti assumono la responsabilità nella trattazione di affari o procedimenti amministrativi. Nell'ambito dell'organigramma approvato dall'Azienda le UOR corrispondono alle Aree e ai Servizi contenuto nell'Allegato 1.

1.6 Individuazione del servizio per la gestione del protocollo informatico, dei flussi documentali e degli archivi e nomina del responsabile della gestione documentale

L'Amministrazione di questo Azienda ha individuato nel Direttore Amministrativo Dott.Antonino La Grutta il responsabile della gestione documentale (R.G.D.).
Il responsabile della gestione documentale ha assegnato all'ufficio protocollo, il compito di gestire il protocollo informatico, i flussi documentali e gli archivi, con a capo un responsabile individuato nella persona della sig.ra Moschini Raffaella in possesso dei requisiti professionali adeguati. Nel caso di vacanza, assenza o impedimento del responsabile dell'ufficio protocollo, il funzionamento dell'ufficio è affidato temporaneamente da parte del R.G.D. a uno dei dipendenti afferenti all'Area amministrativa.
Il responsabile della gestione documentale, coadiuvato dal responsabile dell'ufficio protocollo:

a) attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di protocollo informatico, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantisce che le operazioni di registratura e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo ("Distinta di protocollo");

d) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione dell'archivio;
e) vigila sull'osservanza delle disposizioni del presente regolamento.

La conservazione dell'integrità del sistema di protocollo informatico avviene a cura della Ditta incaricata.

1.7 Compiti del Responsabile della Gestione Documentale

Al Responsabile della gestione documentale sono, altresì, attribuiti i seguenti compiti:

a) predisporre lo schema di manuale di gestione e le sue modifiche e aggiornamenti;
b) proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico previsto dal decreto del Presidente della Repubblica n. 428/98;
c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il responsabile dei sistemi informativi automatizzati, con il responsabile della sicurezza dei dati personali di cui al D. Lgs. 30 giugno 2003, n. 196 e con il responsabile della trasparenza o suo delegato.
d) disporre tutti gli atti organizzativi per il funzionamento del protocollo informatico ivi compresi gli orari di apertura all'utenza e agli uffici dell'Azienda.

PARTE SECONDA – STRUMENTI INFORMATICI

2.1 Modalità di utilizzo di strumenti informatici per lo scambio di documenti

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche. Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati e i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse. Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi. La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n.28. Gli uffici della AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica, in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l'impiego della posta elettronica nelle pubbliche amministrazioni.

2.1.1 Requisiti degli strumenti informatici di scambio

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

- l'integrità del messaggio;

- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e di smistamento dei messaggi all'interno delle AOO;
- l'interconnessione tra AOO (ovvero l'interconnessione tra le UOP -Unità Organizzative di registrazione di Protocollo- e UOR -Unità Organizzative Responsabili- di una stessa AOO nel caso di documenti interni formali);
- la certificazione dell'avvenuto invio e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

2.1.2 Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. I messaggi ricevuti via PEC da persone fisiche hanno il valore di sottoscrizione con firma elettronica avanzata.

2.1.3 Posta elettronica certificata

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.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo.
Allo scopo di effettuare la trasmissione di un documento da un'AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un text editor;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);
- firmare il documento (qualora ritenuto necessario oltre a quanto previsto dal coma 5 dell'art. 5 del d.P.C.m. 13 novembre 2014);
- assegnare il numero di protocollo in uscita al documento;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata (PEC), di norma riservata alla comunicazione verso l'esterno dell'Ente, consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione dell'AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.
I messaggi di ritorno, che sono classificati in:

- conferma di ricezione;
- notifica di eccezione;

- aggiornamento di conferma;
- annullamento di protocollazione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da un'AOO e sono codificati secondo lo stesso standard MIME.
Il servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.
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 notificazione per mezzo della posta nei casi consentiti dalla legge. Le ricevute vanno collegate al protocollo originale nell'apposita sezione "Documenti in originale – Ricevute pec".

2.1.4 Gestione dei documenti informatici: il sistema di protocollo informatico

Il sistema di protocollo informatico adottato dall'Ente è il modulo "Protocollo Informatico per la P.A". di SherpaWeb (di seguito "SherpaWeb"). La manualistica di descrizione e funzionamento del sistema è resa disponibile all'interno del programma stesso con la modalità "Help on line".
Il sistema di gestione informatica dei documenti:

- permette la corretta e puntuale registrazione di protocollo dei documenti in entrata e 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 sensibili e giudiziari;
- permette, se desiderato, la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio;
- garantisce l'identificabilità dell'utente che effettua la registrazione delle attività. Tali tracciature sono protette al fine di non consentire modifiche non autorizzate.
- garantisce l'immodificabilità delle informazioni relative alla segnatura del protocollo e dei documenti allegati;
- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro protocollo.

2.2 Modalità di produzione e di conservazione delle registrazioni di protocollo informatico

2.2.1. Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo é unico e la numerazione progressiva é unica indipendentemente dal modello organizzativo adottato. La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo. 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 cifre numeriche. Non e' 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 e' 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. I documenti con numero di protocollo differente vanno comunque tra loro collegati per il tramite dell'applicativo informatico per la protocollazione degli

atti in dotazione degli uffici. La documentazione che non é stata registrata dal servizio protocollo in entrata o in uscita, viene considerata giuridicamente inesistente presso l'amministrazione.

2.2.2. Registro giornaliero di protocollo

Il servizio protocollo provvede alla produzione del registro giornaliero, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione protocollo nell'arco del giorno precedente integrate con gli hash della segnatura e degli allegati inviati in conservazione con il riferimento al nome, al suo hash e al token di conservazione. Il registro giornaliero di protocollo, in formato XML, sarà a sua volta protocollato per l'invio in automatico alla conservazione sostitutiva.

2.2.3. Regole per la registrazione di protocollo

Su ogni documento ricevuto o spedito dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione sia dei dati obbligatori, sia di quelli facoltativi.
Tale registrazione è eseguita in due fasi, di norma immediatamente consecutive:

1) Prima fase: inserimento di tutti i dati obbligatori di segnatura e, facoltativamente, di tutti gli altri dati previsti nel programma:
   - il mittente che ha prodotto il documento (obbligatorio: dopo la protocollazione non sarà modificabile);
   - il destinatario del documento (obbligatorio: dopo la protocollazione non sarà modificabile);
   - l'oggetto del documento (obbligatorio: dopo la protocollazione non sarà modificabile);
   - i documenti allegati nella rubrica "Documenti in conservazione sostitutiva" (facoltativi: dopo la protocollazione non saranno modificabili).
   - Altri dati (facoltativi: saranno sempre integrabili e/o modificabili. Il programma gestisce automaticamente i log relativi alle modifiche apportate).

Le informazioni potranno essere memorizzate e successivamente richiamate per una verifica, modifica e integrazione.

2) Seconda fase: protocollazione vera e propria. Con l'apposita funzione, l'operatore ordina al programma di:
   - Attribuire al documento il numero di protocollo (registrato in forma non modificabile);
   - Assegnare la data di registrazione di protocollo (registrata in forma non modificabile);
   - Calcolare l'hash sulle informazioni di segnatura obbligatorie e sui documenti allegati nella rubrica "Documenti in originale – conservazione sostitutiva";
   - Inviare in conservazione sostitutiva gli allegati (completi di hash) memorizzati nella rubrica "Documenti in originale – conservazione sostitutiva";

2.2.4. Variazioni e annullamento delle registrazioni di protocollo

La correzione di errori verificatisi in fase di immissione di dati, comporta l'obbligo (previsto dalla normativa) di annullare l'intera registrazione di protocollo se il dato errato è riferito ad informazioni di segnatura. Proprio per questo il programma ne impedisce la modifica.
Se invece l'errore riguarda altre informazioni, queste possono essere modificate in caso di errori o aggiunte in caso di bisogno (esempio: documento precedente e/o successivo). Il programma tiene traccia dettagliata della modifica apportata e dell'operatore che l'ha eseguita.

PARTE TERZA - LE TIPOLOGIE DOCUMENTARIE

3.1 Tipologia dei documenti

I documenti si distinguono in:

a) documenti in arrivo: documenti, con rilevanza giuridico probatoria, prodotti da altri soggetti giuridici e acquisiti dall'Azienda nell'esercizio delle Sue funzioni;
b) documenti in partenza: documenti, con rilevanza giuridico probatoria, prodotti dal personale dell'Azienda nell'esercizio delle sue funzioni e spediti a soggetti giuridici differenti;
c) documenti interni: documenti scambiati tra i diverse unità organizzative responsabili (UOR) afferenti la medesima AOO.

I documenti vanno protocollati e gestiti secondo le disposizioni e le eccezioni previste nel presente regolamento. Il presente manuale individua i documenti da non protocollare.

3.2 Documenti interni

I documenti interni si distinguono in:

a) documenti di preminente carattere informativo;
b) documenti aventi rilevanza giuridica;

I documenti interni di preminente carattere informativo sono di norma memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra uffici e non vanno registrati.
I documenti interni aventi rilevanza giuridica sono quelli redatti dal personale nell'esercizio delle proprie funzioni e al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi, devono essere protocollati.

PARTE QUARTA - DESCRIZIONE DEI FLUSSI DOCUMENTALI

4.1 Modalità di produzione dei documenti interni

Fatto salvo quanto previsto dalla normativa per la formazione dei documenti informatici, i documenti interni prodotti dall'Azienda devono al minimo riportare, nella opportuna forma grafica, le seguenti informazioni:

- denominazione e logo dell'Azienda;
- indicazione unità organizzativa responsabile che ha prodotto il documento;
- data completa, luogo, giorno, mese, anno;
- oggetto del documento;
- sottoscrizione del Responsabile, o dei Responsabili, quando prescritta;.
- numero degli allegati, se presenti.

4.2 Ricezione dei documenti cartacei

I documenti su supporto cartaceo possono pervenire all'Azienda attraverso:

- il servizio postale;
- la consegna diretta;
- gli apparecchi telefax

I documenti arrivati, mediante uno qualunque dei mezzi citati, ad uffici non abilitati alla registrazione di protocollo sono fatti pervenire, a cura del personale che li riceve, all'Ufficio di Protocollo.

4.3 Ricezione dei documenti informatici

La ricezione dei documenti informatici indirizzati all'Azienda è assicurata tramite la casella o le caselle di posta elettronica certificata riservate a questa funzione.

4.4 Rilascio di ricevuta di un documento consegnato a mano

Se richiesto, l'Ufficio Protocollo appone il numero di protocollo assegnato, la data, la propria firma e timbro dell'Azienda su una fotocopia del documento consegnato a mano all'ufficio stesso. Tale fotocopia ha valore di ricevuta.

4.5 Rilascio di ricevuta di un documento informatico

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito è assicurata dal servizio di posta elettronica certificata utilizzato dall'Azienda.

4.6 Recapito e presa in carico dei documenti

I documenti ricevuti dall'Azienda al termine delle operazioni di registrazione, di segnatura di protocollo, di assegnazione sono fatti pervenire in originale agli uffici di competenza. Nel caso di un'assegnazione errata, l'ufficio utente che riceve il documento lo rinvia all'ufficio che glielo ha erroneamente assegnato. Il sistema di gestione informatica dei documenti tiene traccia di tutti questi passaggi.

4.7 Spedizione dei documenti su supporto cartaceo

I documenti da spedire su supporto cartaceo sono trasmessi all'Ufficio di Spedizione dopo che sono state eseguite le operazioni di registrazione di protocollo, segnatura di protocollo.
Gli UOR devono far pervenire la posta in partenza all'Ufficio di Spedizione entro gli orari stabiliti dal servizio. Eventuali situazioni di urgenza saranno valutate dal Responsabile della tenuta del protocollo.

4.8 Spedizione dei documenti informatici

La spedizione di un documento informatico avviene via posta elettronica. Il documento informatico dopo essere stato protocollato viene, se previsto nel procedimento, firmato digitalmente e spedito all'indirizzo di posta elettronica del destinatario.

PARTE QUINTA – REGISTRAZIONE DEI DOCUMENTI: REGOLE E MODALITÀ

5.1 Natura giuridica del registro di protocollo

Il registro di protocollo e un atto pubblico originario che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici. Il registro di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Il registro di protocollo, unico per tutta l'Azienda, si apre il 1° gennaio e si chiude il 31 dicembre di ogni anno.

5.2 Documenti soggetti a registrazione di protocollo

Sono oggetto di registrazione obbligatoria di protocollo i documenti ricevuti e spediti dall'Azienda, ad eccezione di quelli indicati al successivo articolo.

5.3 Documenti non soggetti a registrazione di protocollo

Sono esclusi dalla registrazione di protocollo:

- le gazzette ufficiali,
- i bollettini ufficiali e notiziari della pubblica amministrazione,
- i materiali statistici,
- gli atti preparatori interni,
- i giornali, le riviste, i libri, i materiali pubblicitari,
- gli inviti a manifestazioni,
- tutti i documenti non sottoscritti,
- pubblicazioni e convocazioni a corsi di formazione e/o aggiornamento,
- atti di mera gestione interna del personale,
- i documenti erroneamente indirizzati all'Azienda (da trasmettere a chi di competenza, se individuabile, o, altrimenti, da restituire al mittente);
- atti relativi alle operazioni attinenti al censimento della popolazione o di altri censimenti particolari;
- la corrispondenza interna esclusa quella che in modo diretto o indiretto ha contenuto probatorio e comunque attiene alla gestione dei procedimenti amministrativi;

5.4 Casi particolari

5.4.1 Documenti inerenti a gare di appalto

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 deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.
È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.
Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RGD e il RP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

5.4.2 Registrazione fatture

Le fatture ricevute dall'Amministrazione con o senza lettera di trasmissione devono essere registrate in ossequio a quanto previsto dall'art.42 del D.L. 66/2014 e dal consequenziali atti organizzativi adottati dall'Azienda.

5.4.3 Documenti su supporto cartaceo indirizzati nominativamente al personale

La posta indirizzata nominativamente al personale dell'Azienda viene aperta e registrata all'Ufficio Protocollo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale". In questo caso viene recapitata in busta chiusa al destinatario il quale, dopo averla aperta e preso visione del contenuto, se valuta che il documento ricevuto debba essere protocollato lo deve riconsegnare all'Ufficio protocollo.

5.4.4 Lettere anonime e documenti non firmati

Le lettere anonime non sono registrate all'Ufficio di Protocollo, ma inoltrate, se contengono informazioni o dati di interesse per l'Azienda, al Direttore Amministrativo il quale valuta l'opportunità di dare seguito a queste comunicazioni. I documenti ricevuti non firmati, per i quali è invece prescritta la sottoscrizione, sono inoltrati agli UOR di competenza da parte del responsabile del Servizio per la tenuta del protocollo, il quale vi appone la data di ricevuta del documento.

5.5 Uso della posta elettronica

Con riferimento alla normativa in vigore, l'Azienda ha provveduto ad attivare la casella di posta elettronica certificata amministrazione@pec.apsp-cesarebenedetti.it
L'Azienda può istituire specifiche caselle di posta elettronica, anche certificata, per trattare peculiari tipologie documentali, anche oggetto di registrazione particolare. Gli indirizzi di tali caselle sono riportati nell'indice delle amministrazioni e pubblicati nel sito aziendale.

5.6 Registrazione di protocollo dei documenti su supporto cartaceo: elementi obbligatori ed elementi accessori

L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in un'unica operazione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di registrazione o modifica dei dati. La registrazione di protocollo contiene elementi obbligatori ed elementi accessori. La registrazione degli elementi obbligatori del protocollo è rilevante sul piano giuridico in quanto contiene le indicazioni necessarie e fondamentali per l'univoca, certa, efficace ed immediata identificazione dei documenti. La registrazione degli elementi accessori del protocollo è rilevante sul piano amministrativo, organizzativo e gestionale.

5.6.1 Gestione delle registrazioni di protocollo

Le registrazioni di protocollo sono costituite da informazioni presenti o transitate su SherpaWeb che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano come oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.
Le registrazioni di protocollo devono essere immodificabili ed effettuate contemporaneamente alla segnatura (art. 5 comma n. del d.P.C.m. 3 dicembre 2013).
La segnatura è costituita obbligatoriamente dalle seguenti informazioni così come previsto dagli art. 9 e 21 del d.P.C.m. 3 dicembre 2013:

a) codice identificativo dell'amministrazione;
b) codice identificativo dell'AOO;
c) codice identificativo del registro ("REGISTRO DI PROTOCOLLO" attribuito automaticamente dal programma)
d) data di protocollo
e) progressivo di protocollo
f) l'oggetto
g) il mittente
h) il destinatario o i destinatari
i) i documenti allegati registrati nella rubrica "Documenti in originale – conservazione sostitutiva" perché trattandosi di documenti esterni al programma, lo stesso non può tracciarne le eventuali modifiche così come previsto dall'art. 8 del d.P.C.m. 3 dicembre 2013. Inoltre, inviando i documenti allegati in conservazione sostitutiva, si rispettano le indicazioni contenute nel d.P.C.m. 13 novembre 2014.

Dette informazioni sono rese immodificabili con le tecniche riportate più avanti in questa sezione.

Altre informazioni inserite nel protocollo sono modificabili ed il programma traccia le modifiche apportate, i riferimenti temporali e l'Operatore che le ha eseguite.
L'immodificabilità delle registrazioni di segnatura protocollo e le scritture di sicurezza (tracciatura delle modifiche) sono costituite:

- dai log delle registrazioni in SherpaWeb relativamente alle informazioni modificabili (tutte tranne quelle che costituiscono la segnatura);
- dagli "hash" calcolati automaticamente da SherpaWeb. L'hash è l'impronta informatica generata da una funzione matematica che trasforma un "dato" di qualunque lunghezza (input) in una sequenza di caratteri di lunghezza fissa (output) relativamente limitata. In pratica, applicando una funzione di hash ad un record o ad un file o addirittura ad un intero hard disk, si ottiene una sequenza alfanumerica che rappresenta una sorta di "impronta digitale" dei dati e viene detta valore di hash. Le funzioni di hash presentano principalmente due proprietà importanti, anche dal punto di vista forense:
  - è praticamente impossibile che due testi diversi abbiano lo stesso valore di hash o che, dato un valore di hash ricavato da un certo testo, si possa creare un testo differente che generi lo stesso hash;
  - è praticamente impossibile ricostruire il testo originario disponendo solo del valore di hash.

Quindi, se i dati sui quali è stato calcolato il valore di hash cambiano anche di una sola virgola, il nuovo valore di hash sarà completamente diverso a garanzia che i dati non sono stati modificati.
Gli hash sono calcolati automaticamente da SherpaWeb su:

- le informazioni di segnatura del protocollo;
- su ciascuno dei documenti allegati e registrati nella rubrica "Documenti in originale – conservazione sostitutiva" (peraltro l'hash è un dato obbligatorio per la conservazione sostitutiva);
- dalla conservazione sostitutiva dei documenti allegati al protocollo e registrati nella rubrica "Documenti in originale – conservazione sostitutiva" completi di hash e di token restituito dal sistema di conservazione sostitutiva. In presenza di più allegati, i documenti vengono inviati in conservazione sostitutiva singolarmente e non consegnati in un pacchetto di aggregazione in modo tale che gli stessi possano essere utilizzati senza la necessità di estrapolarli ("estratto informatico" art. 6 comma 3 del d.P.C.m. 13 novembre 2014);
- dalla conservazione sostitutiva del registro di protocollo, completo degli hash indicati in precedenza e dei token restituiti dal sistema di conservazione sostitutiva dei documenti allegati.

5.6.2 Individuazione degli elementi accessori della registrazione di protocollo

La registrazione di protocollo, in armonia con la normativa vigente, può prevedere elementi accessori che assicurano una migliore utilizzazione dei documenti sotto il profilo giuridico, gestionale ed archivistico rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili. Gli elementi accessori sono i seguenti:

a) luogo di provenienza o di destinazione del documento;
b) numero degli allegati;
c) descrizione sintetica degli allegati;
d) estremi del provvedimento di differimento dei termini di registrazione;
e) mezzo di ricezione o di spedizione;
f) ufficio utente di competenza;
g) copie per conoscenza;
h) tipologia del documento.

5.7 Segnatura di protocollo

L'Operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione di protocollo.

5.7.1 Segnatura di protocollo dei documenti su supporto cartaceo

La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso ed è realizzata attraverso l'apposizione su di esso di un timbro di protocollo o attraverso l'apposizione di etichette sulle quali sono riportate le seguenti informazioni:

a) il numero progressivo di protocollo;
b) la data di protocollo;
c) denominazione dell'Azienda;
d) indicazione del UOR o ufficio utente destinatario.

5.8 Registro di emergenza

Il Responsabile del servizio per la tenuta del protocollo autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su apposito registro di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore il Responsabile del servizio per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 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'area organizzativa omogenea. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino della funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che sarà inserito nel campo note e che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.

5.9 Differimento dei termini di registrazione

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque nel più breve tempo possibile. Eccezionalmente, con provvedimento motivato, il Responsabile del servizio può autorizzare la registrazione in tempi maggiori, fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo.

PARTE SESTA - GESTIONE DEI DOCUMENTI E DEI FLUSSI DOCUMENTALI

6.1 Gestione e strumenti dell'archivio corrente

6.1.1 Titolario di classificazione

Per titolario di classificazione si intende un quadro alfanumerico di riferimento per l'archiviazione, la conservazione e la individuazione dei documenti. Il piano di classificazione è soggetto a revisione periodica e compete al Responsabile del servizio, che si atterrà a quanto disposto dalla normativa vigente in materia di formazione e conservazione degli archivi degli enti pubblici. Dopo ogni modifica del titolario di classificazione, il Responsabile del servizio per la tenuta del protocollo 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.

6.1.2 Classificazione dei documenti

Tutti i documenti, devono essere classificati in base al titolario adottato dall'Azienda. Per "classificazione" si intende, l'applicazione del titolario di classificazione, cioè l'assegnazione al documento della categoria, della classe, e numero del fascicolo. Il titolario adottato da questo Ente è descritto nell'allegato 2.
Per ragioni di uniformità redazionale e di normalizzazione del lessico archivistico è stata adottata la seguente nomenclatura del titolario:

- Titolo: primo grado divisionale
  - Classe: secondo grado divisionale
    - Categoria: terzo grado divisionale
      - Sottocategoria: quarto grado divisionale
        - Fascicolo: quinto grado divisionale

6.1.3 Identificazione dei fascicoli

Tutti i documenti sono riuniti in fascicoli.

6.1.4 Fascicolazione dei documenti

La fase di fascicolazione comprende le attività finalizzate alla formazione dei fascicoli, ovvero delle unità archivistiche che riuniscono tutti i documenti relativi ad uno stesso affare o procedimento amministrativo. Qualora un documento dia luogo all'avvio di un autonomo affare o procedimento, l'ufficio abilitato all'operazione di fascicolazione, segnala gli estremi di fascicolazione perla registrazione di protocollo del documento e indica l'ufficio a cui è assegnata la pratica, il quale assicura l'inserimento fisico del documento nel relativo fascicolo. Se dà avvio ad una nuova pratica, apre un nuovo fascicolo e collega la registrazione di protocollo del documento al fascicolo aperto prima di assegnare la pratica all'ufficio competente. In ogni caso, il sistema di gestione informatica dei documenti tiene traccia di tutti i passaggi che subiscono i fascicoli e i documenti in essi contenuti, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

6.1.5 Archiviazione dei documenti

L'archiviazione dei documenti formatisi presso l'Azienda nel corso dell'esercizio delle sue attività e legati da un vincolo necessario, avviene quando gli stessi non hanno più rilevanza per lo svolgimento dell'attività stessa e vengono selezionati per la conservazione.

6.2 Gestione e strumenti dell'archivio di deposito

6.2.1 Gestione dell'archivio di deposito

L'Azienda non dispone di un archivio informatizzato. Il presente manuale prende in considerazione i problemi derivanti dall'archiviazione di documenti cartacei, rinviando al futuro la definizione delle problematiche connesse all'informatizzazione dell'archivio. Periodicamente gli uffici utente individuano i fascicoli cartacei relativi ad affari e procedimenti conclusi che vanno trasmessi all'archivio di deposito. Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. Il Responsabile del servizio per la tenuta del protocollo deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito. La gestione dell'archivio di deposito, la selezione periodica dei documenti (scarto archivistico), la formazione e gestione dell'archivio storico dell'Azienda saranno disciplinati da apposito provvedimento regolamentare.

6.2.2 Conservazione dei documenti informatici

La conservazione dei documenti informatici viene fatta attraverso InfoCert Spa con sede legale in Piazza Sallustio n. 9 00187 Roma - Cap. Sociale Euro 17.704.890,00 interamente versato - P. iva 07945211006 – CCIAA Roma 1064345 – con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11 e successive modifiche.
Il manuale di conservazione redatto InfoCert Spa è depositato sul sito dell'Agenzia per l'Italia Digitale ed è reperibile al seguente link:
http://www.agid.gov.it/sites/default/files/documentazione/manuale_conservazione_infocert.pdf

PARTE SETTIMA - PROCEDURE PER L'ACCESSO AI DOCUMENTI AMMINISTRATIVI E LA TUTELA DEI DATI PERSONALI

7.1 Accesso ai documenti informatici in sherpaweb

Le autorizzazioni ed il controllo degli accessi è assicurato utilizzando l'apposito modulo di SherpaWeb denominato "Gerarchie e autorizzazioni di accesso" che:

- Consente l'accesso al programma protocollo per ciascun utente o gruppi di utenti attraverso l'assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- Consente e obbliga il cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- Assicura la tracciatura di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate;
- Consente a ciascun utente di SherpaWeb di accedere solamente ai documenti che gli sono stati direttamente assegnati;
- Impedisce che i documenti vengono visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio;
- Impedisce ogni accesso diretto ai sistemi essendo disponibili esclusivamente in modalità Cloud Computing.

7.2 Accesso ad altri documenti informatici

Il sistema operativo del server è configurato in modo tale da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy" con particolare riferimento al trattamento dei dati sensibili e giudiziari;

7.3 Criteri e modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali

Il presente capitolo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali gestite dal Sistema di protocollo SherpaWeb.

7.3.1. Abilitazioni di accesso interno alle informazioni documentali

Il controllo degli accessi è il processo che garantisce l'impiego dei servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite. Le autorizzazioni ed il controllo degli accessi è assicurato utilizzando l'apposito modulo di SherpaWeb denominato "Gerarchie e autorizzazioni di accesso". Gli utenti del servizio di protocollo hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza. Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente:
  - pubblica che permette l'identificazione dell'utente da parte del sistema (userID);
  - privata o riservata di autenticazione (password) semplice o complessa, con obbligo modifica almeno semestrale;
- un profilo di autorizzazione al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio cui l'utente appartiene.

I diversi livelli di autorizzazione, descritti nel funzionigramma, sono assegnati agli utenti dal Responsabile della Gestione documentale. Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO sono costantemente aggiornate a cura del R.G.D.

7.3.2. Abilitazioni di accesso esterno alle informazioni documentali

La funzione di accesso esterno non è ancora attivata. E' attivabile con modalità simili a quelle previste per gli accessi interni attraverso il modulo di SherpaWeb denominato "Gerarchie e autorizzazioni di accesso". Gli utenti esterni del servizio hanno autorizzazioni di accesso personali che gli permettono di visualizzare soltanto i documenti a loro stessi riferiti. Ad ogni utente è assegnata:

- una credenziale di accesso, costituita da una componente:
  - pubblica che permette l'identificazione dell'utente da parte del sistema (userID);
  - privata o riservata di autenticazione (password) semplice o complessa, con obbligo modifica almeno semestrale;
- un profilo di autorizzazione al fine di limitare le operazioni di protocollo alle sole funzioni di lettura relativamente ai documenti di propria competenza.

Il livello di autorizzazione, descritto nel funzionigramma, è assegnato agli utenti dal Responsabile della Gestione Documentale. Le abilitazioni all'utilizzo delle funzionalità di consultazione del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli utenti esterni abilitati alla funzione sono costantemente monitorati a cura del R.G.D..

PARTE OTTAVA - PIANO DI SICUREZZA DEI DOCUMENTI INFORMATICI

8.1 Obiettivi del piano di sicurezza

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

8.1.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:
- i documenti e le informazioni trattati dalla AOO (Area organizzativa Omogenea) siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili 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.

8.1.2 Generalità

Il piano di sicurezza definisce:
- le politiche generali e particolari di sicurezza adottate all'interno della AOO;
- le modalità di accesso al servizio protocollo, di gestione documentale e archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano è soggetto a revisione con cadenza almeno biennale o può essere modificato anticipatamente a seguito di eventi gravi.
Sono state adottate le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti:
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;

- conservazione, a cura dell'Amministratore di sistema, delle copie di riserva dei dati e dei documenti negli stessi locali in cui è installato il sistema di elaborazione che ospita il programma di protocollo;
- impiego e manutenzione di un adeguato sistema antivirus;
- archiviazione giornaliera delle copie del registro di protocollo.

8.1.3 Formazione dei documenti - aspetti di sicurezza

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

I documenti della AOO sono prodotti con l'ausilio di applicativi di videoscrittura che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la sua riservatezza, il documento è sottoscritto con firma digitale.

8.1.4 Descrizione funzionale ed operativa del sistema di protocollo informatico

Il sistema di protocollo informatico adottato dall'Ente, il già citato "SherpaWeb", ha al proprio interno la manualistica di descrizione e funzionamento del sistema con la modalità "Help on line" che costituisce parte integrante e sostanziale del presente documento e che qui si richiama pur omettendone l'allegazione.
Inoltre, con il fornitore di SherpaWeb, è abilitato il servizio di assistenza telefonica al quale è possibile rivolgersi attraverso una semplice telefonata per il chiarimento di modalità operative legate al software oppure per la risoluzione di eventuali anomalie emerse durante la fruizione del servizio.

PARTE NONA - DISPOSIZIONI FINALI

9.1 Modalità di aggiornamento del manuale

Il manuale di gestione, in quanto disciplinare di organizzazione, è adottato con deliberazione del Consiglio di Amministrazione e aggiornato ogniqualvolta risulti necessario, a seguito di innovazioni normative o regolamentari, e tecnologiche con apposito provvedimento proposto dal Direttore dell'Azienda

9.2 Entrata in vigore del manuale di gestione

Il presente Manuale di Gestione, cosi come i successivi atti di revisione, entra in vigore dopo la sua approvazione e pubblicazione a termini di legge. In ottemperanza dell'art. 5, comma 3 del DPCM 3 dicembre 2013, il presente Manuale di Gestione viene reso accessibile nelle seguenti forme:

1. per il personale dell'Ente mediante pubblicazione sul sito Intranet;
2. per il pubblico mediante pubblicazione sul portale dell'Ente.

9.3 Norme di rinvio

Per tutto quanto non previsto dal presente Manuale di Gestione valgono le disposizioni di legge previste in materia.