

Allegato "A" alla delibera di Giunta Provinciale N.319 del 15/12/2010

PROVINCIA DI RIMINI  
Servizio Organizzazione e Affari Giuridico amministrativi,  
Politiche Giovanili, Pari Opportunità

**MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI  
FLUSSI DOCUMENTALI E DELL'ARCHIVIO CORRENTE**  
(DPCM 31 ottobre 2000)

<b>SEZIONE I</b> <b>DEFINIZIONI ED AMBITO DI APPLICAZIONE</b>
--

**Articolo 1****Ambito di applicazione**

Il presente manuale di gestione dei documenti è adottato ai sensi del D.P.C.M. 31.10.2000, del D.P.R. 445/2000 e del D.Lgs. 82/2005. Esso disciplina le attività di formazione registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali e dei procedimenti amministrativi dell'Amministrazione Provinciale di Rimini.

**Articolo 2****Definizioni**

Ai fini del presente manuale s'intende:

- a) per *Amministrazione*, la Provincia di Rimini
- b) per *archiviazione ottica*, l'operazione che genera, su un supporto di memorizzazione, una registrazione contenente la versione iniziale di una istanza di un documento informatico;
- c) per *archivio corrente*, la parte di documentazione relativa agli affari ed ai procedimenti in corso di trattazione, o comunque verso i quali sussiste un interesse corrente;
- d) per *archivio di deposito*, la parte di documentazione relativa ad affari esauriti, non più occorrenti quindi alla trattazione degli affari in corso, ma non ancora destinata istituzionalmente alla conservazione permanente e alla consultazione da parte del pubblico;
- e) per *archivio storico*, il complesso di documenti relativi ad affari esauriti e destinati, previa operazioni di scarto, alla conservazione permanente per garantire in forma adeguata la consultazione al pubblico;
- f) per *area organizzativa omogenea* un insieme di funzioni e di strutture, individuate dall' Amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato;
- g) per *assegnazione*, l'operazione d'individuazione dell'ufficio utente competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono.
- h) per *classificazione*, l'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;

- i) per *documento amministrativo*, ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa;
- j) per *documento informatico*, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- k) per *fascicolazione*, l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi,
- l) per *fascicolo*, l'unità archivistica che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare;
- m) per *firma digitale*, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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;
- n) per *gestione dei documenti*, l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'Amministrazione, nell'ambito del sistema di classificazione adottato;
- o) per *impronta di un documento informatico*, una sequenza di simboli binari in grado di identificarne univocamente il contenuto;
- p) per *piano di conservazione degli archivi*, il piano, integrato con il sistema di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
- q) per *Registrazione di protocollo*, l'operazione che consente di individuare in modo univoco il singolo documento all'interno dell'archivio e a certificarne in modo inoppugnabile la data entro la quale esso è entrato a far parte dell'archivio del soggetto produttore. Insieme degli elementi rilevanti sul piano giuridico-probatorio e obbligatori nella registrazione a protocollo.
- r) 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;
- s) per *Servizio*, il Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61, comma 1, del testo unico;
- t) per *sistema di gestione informatica dei documenti*, l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'Amministrazione per la gestione dei documenti;

- u) per *supporto di memorizzazione*, il mezzo fisico atto a registrare permanentemente informazioni rappresentate in modo digitale, su cui l'operazione di scrittura comporti una modifica permanente ed irreversibile delle caratteristiche del supporto stesso;
- v) per *Testo Unico*, il “Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”, pubblicato con DPR 28 dicembre 2000, n. 445;
- w) per *titolario di classificazione* un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell' analisi delle competenze dell' Amministrazione, al quale deve ricondursi la molteplicità dei documenti prodotti, per consentirne la sedimentazione secondo un ordine logico che rispecchi storicamente lo sviluppo dell'attività svolta
- x) per *ufficio utente*, un ufficio dell'area organizzativa omogenea che utilizza i servizi messi a disposizione dal sistema di gestione informatica dei documenti.

<b>SEZIONE II</b> <b>DISPOSIZIONI GENERALI</b>
---

### **Articolo 3**

#### **Aree organizzative omogenee**

Ai fini della gestione dei documenti l'Amministrazione individua una sola area organizzativa omogenea denominata "Provincia di Rimini" e composta dall'insieme di tutte le sue strutture. La Provincia di Rimini è accreditata all'Indice della Pubblica Amministrazione (IndicePA) ai sensi del DPCM 31.10.2000.

L'IndicePA costituisce un punto di riferimento per l'individuazione e l'accesso alle strutture organizzative e ai servizi telematici offerti dalla Pubblica Amministrazione centrale e locale.

Nell'IndicePA sono, inoltre, pubblicate tutte le informazioni necessarie per lo scambio di messaggi di posta elettronica attraverso le caselle istituzionali associate ai sistemi di **protocollo informatico**. Il codice identificativo dell'Area Organizzativa Omogenea nell'Indice della Pubblica amministrazione è "p\_rn".

### **Articolo 4**

#### **Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi**

Nell'ambito dell'area organizzativa omogenea è istituito, nell'ambito del Servizio Organizzazione e Affari Giuridico Amministrativi, il Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Esso è funzionalmente individuato nell'Ufficio Protocollo e fa capo al Responsabile di questa struttura.

Nei casi di vacanza, assenza o impedimento del Responsabile, la direzione del Servizio è affidata al delegato. Al Servizio sono assegnati i compiti di cui all'articolo 61, comma 3, del Testo Unico (DPR 445/2000).

### **Articolo 5**

#### **Unicità del protocollo informatico**

Nell'ambito dell'area organizzativa omogenea la numerazione delle registrazioni di protocollo è unica e rigidamente progressiva. Essa si chiude al 31 dicembre e ricomincia da 1 all'inizio di ogni anno.

Il numero di protocollo è costituito da almeno sette cifre numeriche, ai sensi dell'articolo 57 del Testo Unico.

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 (art. 53 del Testo Unico).

### **Articolo 6**

#### **Eliminazione dei protocolli interni**

Con l'entrata in funzione del sistema di gestione informatica dei documenti sono eliminati tutti i sistemi di registrazione dei documenti alternativi al protocollo informatico. All'interno della Provincia di Rimini non esistono protocolli paralleli al Protocollo Generale.

## **Articolo 7**

### **Modello organizzativo adottato per la gestione dei documenti**

Per la gestione dei documenti è adottato un modello organizzativo di tipo decentrato che prevede la partecipazione attiva di più soggetti ed uffici utente, ognuno dei quali è abilitato a svolgere soltanto le operazioni di propria competenza. Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei documenti, ovvero l'identificazione degli uffici utente e del personale abilitati allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea, sono riportate nell'allegato n. 1 e sono costantemente aggiornate a cura del Responsabile dell'Ufficio Protocollo.

<b>SEZIONE III</b> <b>FORMAZIONE DEI DOCUMENTI</b>
---

## **Articolo 8**

### **Modalità di formazione dei documenti e contenuti minimi**

I documenti sono di norma prodotti con sistemi informatici, ai sensi dell'articolo 3 del D. Lgs. 12 febbraio 1993, n. 39.

Sui documenti sono riportate le seguenti informazioni:

- denominazione e stemma dell'Amministrazione;
- indicazione dell'area organizzativa omogenea e dell'ufficio utente che ha prodotto il documento;
- indirizzo completo con numero di telefono e fax;
- indirizzo di posta elettronica;
- data completa, luogo, giorno, mese, anno dell'atto;
- numero degli allegati, se presenti;
- oggetto del documento;
- sottoscrizione del Responsabile, o dei Responsabili, quando prescritta; se trattasi di documento in formato digitale, firma digitale del Responsabile del procedimento e/o del responsabile del provvedimento finale. Se trattasi di un documento cartaceo, sigla autografa del Responsabile del procedimento e/o del responsabile del provvedimento finale.

## **Articolo 9**

### **Formato dei documenti informatici**

I documenti informatici prodotti dell'Amministrazione, indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantire la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

## **Articolo 10**

### **Sottoscrizione dei documenti informatici**

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni contenute nel testo unico ed alle regole tecniche di cui al DPCM 8 febbraio 1999 ed alla deliberazione AIPA 51/2000. L'Amministrazione si avvale pertanto dei servizi di una Certification Authority iscritta nell'elenco pubblico dei certificatori tenuto dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) (Ex AIPA).

<b>SEZIONE IV</b> <b>RICEZIONE DEI DOCUMENTI</b>
---

## **Articolo 11**

### **Ricezione dei documenti su supporto cartaceo**

I documenti su supporto cartaceo possono pervenire all'area organizzativa omogenea attraverso:

- a) il servizio postale tradizionale;
- b) la consegna diretta agli uffici utente;
- c) gli apparecchi telefax
- d) posta elettronica certificata.

I documenti che transitano attraverso il servizio postale tradizionale sono consegnati, quotidianamente, dagli addetti del Servizio Postale, all'Ufficio Protocollo.

I documenti consegnati direttamente agli uffici utente, se sono soggetti a registrazione di protocollo, sono fatti pervenire, a cura del personale che li riceve e nell'arco della stessa giornata, ai più vicini uffici abilitati alla registrazione di protocollo dei documenti in arrivo.

I documenti ricevuti con apparecchi telefax, se sono soggetti a registrazione di protocollo, in assenza di un sistema informatico che ne consente l'acquisizione in formato elettronico (fax management) sono trattati come quelli consegnati direttamente agli uffici utente. Con la disponibilità di un sistema di fax management si applicano, invece, le procedure previste per la ricezione dei documenti informatici.

E' fatto divieto, per il personale addetto allo smistamento della posta e al protocollo, di aprire le buste indirizzate alla polizia locale, con particolare riferimento alle pratiche di polizia giudiziaria che sono sempre sottoposte a segreto istruttorio.

Il personale addetto allo smistamento pertanto provvederà ad inoltrare i plichi pervenuti all'Ufficio di polizia locale che procederà all'apertura e alla conseguente protocollazione.

## **Articolo 12**

### **Ricezione dei documenti informatici**

La Provincia di Rimini è dotata di posta elettronica certificata (PEC). La **posta elettronica certificata** è uno strumento che permette di dare, ad un messaggio di posta elettronica, lo stesso valore di una raccomandata con ricevuta di ritorno tradizionale. La PEC può aggiungere inoltre la certificazione del contenuto del messaggio solo se in combinazione con un certificato digitale. Le comunicazioni di qualsiasi natura inviate per via telematica sono valide quali documenti originali se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato, oppure quando l'autore è identificato dal sistema informatico mediante la carta di identità elettronica o la carta nazionale dei servizi ai sensi dell'art.65 del Dlgs n.82/2005.

La ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata (PEC) riservata a questa funzione ed accessibile solo all'ufficio preposto alla loro registrazione di protocollo. L'indirizzo di tale casella di posta elettronica certificata è reso pubblico in una apposita sezione del sito web istituzionale.



Il Responsabile del Servizio provvede a renderlo pubblico utilizzando ogni possibile mezzo di comunicazione ed a trasmetterlo all' AIPA ai sensi dell'articolo 12, comma 2, lettera c), del D.P.C.M. 31 ottobre 2000.

I documenti informatici che pervengono direttamente agli uffici utente sono da questi valutati ai sensi dell'articolo 15, comma 7, del D.P.C.M. 31 ottobre 2000 e, se soggetti a registrazione di protocollo o ad altra forma di registrazione, immediatamente inoltrati all'indirizzo elettronico dell'ufficio preposto alla ricezione dei documenti informatici.

I documenti informatici non sottoscritti digitalmente e provenienti da un indirizzo di posta elettronica certificata sono considerati equivalenti ai documenti cartacei non firmati, ma di cui si ha certezza sulla provenienza ed integrità. Essi sono accettati dall'Amministrazione e regolarmente protocollati.

Al Responsabile del procedimento compete la valutazione della loro ammissibilità ai sensi dell'articolo 15, comma 7, del D.P.C.M. 31 ottobre 2000 nelle procedure cui si riferiscono.

I documenti in esame possono essere stampati e gestiti come documenti cartacei. In tal caso, su di essi sono riportati i dati sulla provenienza.

I documenti informatici sottoscritti digitalmente e provenienti da un indirizzo di posta elettronica non certificata sono considerati equivalenti ai documenti cartacei firmati, ma di cui non si ha certezza sulla provenienza ed integrità. Essi sono accettati dall'Amministrazione e regolarmente protocollati.

Al Responsabile del procedimento compete la valutazione della loro ammissibilità ai sensi dell'articolo 15, comma 7, del D.P.C.M. 31 ottobre 2000 nelle procedure cui si riferiscono.

I documenti in esame possono essere stampati e gestiti come documenti cartacei. In tal caso, su di essi sono riportati i dati sulla provenienza.

I documenti informatici non sottoscritti digitalmente e provenienti da un indirizzo di posta elettronica non certificata, sono considerati equivalenti a documenti cartacei non firmati di cui non si ha certezza sulla provenienza ed integrità. La loro accettazione è subordinata alla verifica che la loro produzione non sia legata ad eventi anomali quali:

- a) attacchi informatici;
- b) virus informatici;
- c) messaggi reiterati;
- d) scherzi o similari.

In caso di accettazione, spetta al Responsabile del procedimento la valutazione della loro ammissibilità ai sensi dell'articolo 15, comma 7, del D.P.C.M. 31 ottobre 2000 nelle procedure cui si riferiscono.

I documenti in esame possono essere stampati e gestiti come documenti cartacei. In tal caso, su di essi sono riportate le informazioni sulla provenienza.

## **Articolo 13**

### **Rilascio di ricevute attestanti la ricezione dei documenti**

Nel caso di ricezione dei documenti cartacei consegnati direttamente all'Ufficio Protocollo, il sistema di protocollo informatico, a seguito della avvenuta registrazione di protocollo, può rilasciare, mediante apposito comando, una ricevuta della presentazione del documento.

Nel caso di ricezione dei documenti informatici, la notifica al mittente dell'avvenuta ricezione è assicurata dal sistema di posta elettronica certificata utilizzato dall'Amministrazione.

<b>SEZIONE V</b> <b>REGISTRAZIONE DEI DOCUMENTI</b>
--

#### **Articolo 14**

##### **Documenti soggetti a registrazione di protocollo**

I documenti ricevuti e prodotti dagli uffici utenti, indipendentemente dal supporto sul quale sono formati, ad eccezione di quelli indicati al successivo articolo 15, sono registrati nel sistema di gestione informatica dei documenti.

#### **Articolo 15**

##### **Documenti non soggetti a registrazione di protocollo**

Sono esclusi dalla registrazione di protocollo: le Gazzette Ufficiali, i Bollettini Ufficiali e notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni. Le ricevute di pagamento in conto corrente postale, anche se trasmesse con lettera accompagnatoria, non vengono protocollate. Sono altresì esclusi dalla registrazione di protocollo i documenti già soggetti a registrazione particolare dall'Amministrazione elencati nell'allegato n. 2, per i quali si applicano le modalità di trattamento riportate nel medesimo allegato.

#### **Articolo 16**

##### **Registrazione di protocollo dei documenti ricevuti e spediti**

Per ogni documento ricevuto o spedito dall'area organizzativa omogenea è effettuata una registrazione di protocollo con il sistema di gestione informatica dei documenti.

Ciascuna registrazione di protocollo contiene dati obbligatori e dati opzionali. I dati obbligatori sono:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente per i documenti ricevuti o, in alternativa, destinatario o destinatari, per i documenti spediti, registrati in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e numero di protocollo del documento ricevuto, se disponibili;
- f) impronta del documento informatico, se trasmesso per via telematica, generata impiegando una funzione (cd “funzione di hash”) e registrata in forma non modificabile
- g) . numero degli allegati

I dati opzionali, invece, sono:

- a) data di arrivo;
- b) descrizione sintetica degli allegati;
- c) mezzo di ricezione o, in alternativa, mezzo di spedizione;
- d) ufficio utente di competenza;
- e) copie per conoscenza;
- f) n) tipo di documento;

g) indicazione del livello di riservatezza, se diverso da quello standard applicato dal sistema (cfr. sezione XV del presente manuale).

I documenti in partenza dovranno riportare, di norma nella parte alta sinistra, una partizione dello spazio per l'apposizione, a mano o a stampa, del numero di protocollo e della classifica.

## **Articolo 17**

### **Registrazione di documenti informatici**

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica certificata è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio e sia ad uno o più file ad esso allegati (cfr. articolo 15, commi 1 e 2, del DPCM 31 ottobre 2000). Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto.

## **Articolo 18**

### **Documenti interni**

Per ogni documento prodotto dagli uffici utenti, non spedito a soggetti esterni, all'area organizzativa omogenea e non rientrante nelle categorie di documenti esclusi dalla registrazione ai sensi dell'articolo 15 del presente manuale di gestione, indipendentemente dal supporto sul quale è formato, è effettuata una registrazione di protocollo.

In questo caso i dati obbligatori sono:

- a) numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) ufficio utente che ha prodotto il documento, registrato in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) impronta del documento informatico, se trasmesso per via telematica, generata impiegando una funzione (cd "funzione di hash") e registrata in forma non modificabile;
- f) numero degli allegati.

I dati facoltativi, invece, sono:

- a) b) descrizione sintetica degli allegati;
- b) tipo di documento;
- c) indicazione del livello di riservatezza, se diverso da quello standard applicato dal sistema (cfr. sezione XV del presente manuale).

Il calcolo dell'impronta di cui al punto e) è effettuato per tutti i file allegati al documento informatico oggetto di registrazione.

Gli uffici abilitati alla registrazione di protocollo dei documenti interni, elencati nell'allegato n. 2, ricevono i documenti informatici da protocollare all'indirizzo elettronico interno dedicato a questa funzione.

## **Articolo 19**

### **Segnatura di protocollo**

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

Le informazioni minime apposte od associate al documento mediante l'operazione di segnatura sono quelle elencate nell'articolo 9 del D.P.C.M. 31 ottobre 2000, e precisamente:

- a) codice identificativo dell'Amministrazione;
- b) codice identificativo dell'area organizzativa omogenea (facoltativo in caso di coincidenza con l'Amministrazione);
- c) data di protocollo;
- d) progressivo di protocollo.

## **Articolo 20**

### **Annullamento delle registrazioni di protocollo**

Le registrazioni di protocollo possono essere annullate con una specifica funzione del sistema di gestione informatica dei documenti e su autorizzazione del Responsabile dell'Ufficio Protocollo.

Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema con un simbolo o una dicitura. L'operazione di annullamento è eseguita con le modalità di cui all'articolo 8 del D.P.C.M. 31 ottobre 2000.

## **Articolo 21**

### **Registro giornaliero di protocollo**

Il Responsabile del Servizio provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili i quali sono conservati a cura del soggetto individuato dall'Amministrazione ai sensi dell'articolo 5 comma 7 del D.P.C.M. 31.10.2000.

## **Articolo 22**

### **Registro di emergenza**

Il Responsabile del Servizio autorizza lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza ogni qualvolta per cause tecniche non sia possibile utilizzare il sistema.

Gli uffici autorizzati alla tenuta di un registro di emergenza sono elencati nell'allegato n. 1.

Si applicano le modalità di registrazione dei documenti sul registro di emergenza e di recupero delle stesse nel sistema di protocollo informatico di cui all'articolo 63 del Testo Unico.

## **Articolo 23**

### **Differimento dei termini di registrazione**

Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre le quarantotto ore dal ricevimento degli atti.

Eccezionalmente, il Responsabile del Servizio può autorizzare la registrazione in tempi successivi, fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo.

## **Articolo 24**

### **Deliberazioni di Giunta e Consiglio, determinazioni dirigenziali, decreti, ordinanze, contratti**

Le deliberazioni di Giunta e Consiglio, le determinazioni dirigenziali, i decreti, le ordinanze ed i contratti sono documenti già soggetti a registrazione particolare dell'Amministrazione e non vanno registrati al protocollo.

Questi documenti costituiscono delle serie archivistiche, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

- i dati identificativi di ciascun atto;
- i dati di classificazione e fascicolazione;
- il numero di repertorio che è un numero progressivo, annuale.

## **Articolo 25**

### **Documenti inerenti a gare d'appalto**

Le offerte inerenti a gare d'appalto sono registrate al protocollo in busta chiusa. Gli estremi di protocollo sono riportati sulla busta medesima.

Dopo l'apertura delle buste sarà cura dell'ufficio utente che gestisce la gara d'appalto riportare gli estremi di protocollo sul documento contenente l'offerta conservando la busta unitamente al contenuto.

## **Articolo 26**

### **Documenti su supporto cartaceo indirizzati nominativamente al personale dell'area organizzativa omogenea**

La posta indirizzata nominativamente al personale dell'area organizzativa omogenea, viene regolarmente aperta e registrata al 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 non è personale lo deve riconsegnare al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

## **Articolo 27**

### **Lettere anonime e documenti non firmati**

Le lettere anonime non sono registrate al protocollo, ma semplicemente inoltrate, se contengono informazioni o dati di interesse per l'Amministrazione, agli uffici utente di competenza, i quali valutano l'opportunità di dare seguito a queste comunicazioni ed individuano le eventuali procedure da sviluppare.

I documenti ricevuti non firmati, per i quali è invece prescritta la sottoscrizione, non sono registrati al protocollo, ma inoltrati agli uffici di competenza i quali individuano le procedure da seguire per risolvere queste situazioni.

## **Articolo 28**

### **Documenti ricevuti prima via fax e poi, successivamente, in originale su supporto cartaceo**

I documenti ricevuti via fax sono registrati al protocollo. Il documento trasmesso da chiunque ad una Pubblica Amministrazione tramite telefax, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale (art.3 DLgs 3/93 e art.43 c.6 Testo Unico). Qualora successivamente pervengano all'area organizzativa omogenea, tramite posta tradizionale, gli originali, agli stessi saranno attribuiti lo stesso numero e la stessa data di protocollo assegnati ai relativi fax. La segnatura deve essere sempre apposta sul documento e non sulla copertina di trasmissione che potrà essere conservata qualora riporti eventuali annotazioni.

## **Articolo 29**

### **Documenti di competenza di altre amministrazioni**

Qualora pervenga all'area organizzativa omogenea un documento di competenza di un altro ente, altra persona fisica o giuridica, lo stesso viene trasmesso a chi di competenza, se individuabile, altrimenti viene restituito al mittente.

Nel caso in cui un documento della fattispecie sopra indicata venga erroneamente registrato al protocollo, questi verrà spedito a chi di competenza, oppure restituito al mittente, con una lettera di trasmissione opportunamente protocollata.



<b>SEZIONE VI</b> <b>CLASSIFICAZIONE DEI DOCUMENTI</b>
---

### **Articolo 30**

#### **Piano di classificazione dell'archivio**

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'Ente. Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di 1° livello, 2° livello, 3° livello, ecc..

Il titolo individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni); le successive partizioni (classi, sottoclassi, ecc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente fra loro in una struttura ad albero rovesciato.

Titoli, classi, sottoclassi, etc, sono nel numero stabilito dal titolare di classificazione e non sono modificabili, né nel numero né nell'oggetto, se non per provvedimento esplicito della funzione di governo dell'amministrazione. Il titolare è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali. L'aggiornamento del titolare compete esclusivamente al vertice dell'amministrazione, su proposta del Responsabile del Servizio per la tenuta del Protocollo Informatico. La revisione, anche parziale del titolare, viene proposta quando è necessario ed opportuno. Dopo ogni modifica del titolare, il Responsabile del Servizio per la tenuta del Protocollo Informatico 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.

### **Articolo 31**

#### **Classificazione dei documenti**

Tutti i documenti ricevuti e prodotti dagli uffici utente dell'area organizzativa omogenea, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al titolare riportato nell'allegato n. 3°.

Gli uffici utente abilitati all'operazione di classificazione dei documenti sono elencati nell'allegato n. 1.

## SEZIONE VII

### ASSEGNAZIONE DEI DOCUMENTI

#### **Articolo 32**

##### **Unità di smistamento**

L'assegnazione agli uffici utente di competenza dei documenti ricevuti è effettuata dall'ufficio protocollo e da altre unità di smistamento.

Il processo di assegnazione dei documenti può coinvolgere più unità di smistamento, una di seguito all'altra, fino ad arrivare agli uffici utente incaricati dello svolgimento delle pratiche.

Nell'allegato n. 4 sono riportati gli uffici autorizzati dal Responsabile del Servizio all'assegnazione dei documenti ricevuti dall'area organizzativa omogenea e le unità di smistamento interno.

#### **Articolo 33**

##### **Modifica delle assegnazioni**

Nel caso di un'assegnazione errata, l'ufficio utente che riceve il documento è tenuto a trasmetterlo, nel più breve tempo possibile all'unità che ha effettuato l'assegnazione la quale provvederà a correggere le informazioni inserite nel sistema informatico e ad inviare il documento all'ufficio di competenza.

Il sistema di gestione informatica dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

#### **Articolo 34**

##### **Recapito dei documenti agli uffici utenti**

I documenti informatici ricevuti per via telematica sono resi disponibili agli uffici utente, attraverso la rete interna dell'Amministrazione, immediatamente dopo l'operazione di assegnazione.

Le immagini dei documenti cartacei acquisite con lo scanner sono resi disponibili agli uffici utente attraverso la rete interna dell'Amministrazione immediatamente dopo l'operazione di scansione.

I documenti ricevuti dall'area organizzativa omogenea su supporto cartaceo, anche se acquisiti in formato immagine con l'ausilio di scanner, sono consegnati agli uffici utente di competenza i quali hanno il compito di inserirli nei rispettivi fascicoli e conservarli fino al versamento nell'archivio di deposito.

Il ritiro giornaliero della posta in arrivo cartacea da parte degli uffici utente avviene presso gli uffici abilitati alla registrazione di protocollo entro le ore 13,00 di ogni giorno.

## SEZIONE VIII

### SCANSIONE DEI DOCUMENTI SU SUPPORTO CARTACEO

#### **Articolo 35**

##### **Documenti soggetti a scansione ed uffici abilitati**

I documenti ricevuti su supporto cartaceo, di formato inferiore od uguale all'A3, dopo le operazioni di registrazione e segnatura protocollo, sono acquisiti in formato immagine con l'ausilio di scanner.

I documenti di formato superiore all'A3 sono acquisiti in formato immagine solo se esplicitamente richiesto dagli uffici utenti di competenza, avvalendosi eventualmente dei servizi di una società esterna specializzata.

Il Responsabile dell'ufficio protocollo individua, con l'ausilio dei Responsabili dei procedimenti, i documenti da sottrarre al processo di scansione che nel ciclo di lavorazione dei documenti ricevuti segue le operazioni di registrazione e segnatura di protocollo.

Gli uffici abilitati all'operazione di scansione dei documenti sono elencati nell'allegato n. 1.

#### **Articolo 36**

##### **Modalità di svolgimento del processo di scansione**

Il processo di scansione si articola nelle seguenti fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche composto da più pagine, corrisponda un unico file in un formato standard abilitato alla conservazione;
- verifica della leggibilità delle immagini acquisite e della loro esatta corrispondenza con gli originali cartacei;
- collegamento delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;
- memorizzazione delle immagini, in modo non modificabile.

## SEZIONE IX

### FASCICOLAZIONE DEI DOCUMENTI

#### **Articolo 37**

##### **Identificazione dei fascicoli ed uffici abilitati alla loro formazione**

Tutti i documenti classificati, indipendentemente dal supporto sul quale vengono formati, sono riuniti in fascicoli.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di apertura che consente di registrare nel sistema informatico le seguenti informazioni:

- titolo e classe del titolario di classificazione nell'ambito delle quali il fascicolo si colloca;
- numero del fascicolo generato automaticamente dal sistema informatico;
- oggetto del fascicolo;
- anno di apertura;
- ufficio utente cui è assegnata la relativa pratica;
- livello di riservatezza, se diverso da quello standard applicato dal sistema (cfr. sezione XV del presente manuale).

Nell'allegato n. 1 sono elencati gli uffici abilitati all'operazione di fascicolatura dei documenti.

#### **Articolo 38**

##### **Processo di formazione dei fascicoli**

In presenza di un documento da inserire in un fascicolo, l'ufficio abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se esso si colloca nell'ambito di un affare o procedimento in corso, oppure se dà avvio ad una nuova pratica.

Se si colloca nell'ambito di un affare o procedimento in corso:

- seleziona il relativo fascicolo;
- collega la registrazione di protocollo del documento al fascicolo selezionato;
- invia il documento all'ufficio utente cui è assegnata la pratica il quale, se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo carteggio.

Se dà avvio ad una nuova pratica:

- esegue l'operazione di apertura del fascicolo di cui al precedente articolo 37;
- assegna la pratica ad un ufficio utente su indicazione del Responsabile del procedimento;
- collega la registrazione di protocollo del documento al fascicolo aperto;

- invia il documento ed il fascicolo all'ufficio utente cui è assegnata la pratica.

## **Articolo 39**

### **Modifica delle assegnazioni dei fascicoli**

Nel caso di un'assegnazione errata di un fascicolo o di una sua successiva riassegnazione, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'ufficio utente di competenza.

Il sistema di gestione informatica dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore che effettua la modifica con la data e l'ora di esecuzione.

## **Articolo 40**

### **Tenuta dei fascicoli dell'archivio corrente**

I fascicoli dell'archivio corrente sono formati a cura dei Responsabili di procedimento e conservati, fino al versamento nell'archivio di deposito, presso gli uffici utente cui sono state assegnate le pratiche.

## **Articolo 41 o 40bis**

### **Chiusura fascicolo**

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare. La data di chiusura si riferisce alla data dell'ultimo documento prodotto. Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura. Gli elementi che individuano il fascicolo sono gestiti dal soggetto che ha provveduto alla sua apertura, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

## SEZIONE X

### SPEDIZIONE DEI DOCUMENTI

#### **Articolo 42**

##### **Spedizione dei documenti su supporto cartaceo**

I documenti da spedire su supporto cartaceo sono trasmessi all'ufficio centrale di spedizione dopo che sono state eseguite le operazioni di registrazione di protocollo, segnatura di protocollo, classificazione e fascicolazione.

Essi sono trasmessi in busta chiusa, già intestata dagli uffici utente. Nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere, o altro mezzo che richieda una qualche documentazione da allegare alla busta, questa modulistica viene compilata a cura degli uffici utente.

All'ufficio centrale di spedizione competono le seguenti operazioni:

- pesatura, calcolo delle spese postali e tenuta della relativa contabilità.

Gli uffici utente devono far pervenire la posta in partenza all'ufficio centrale di spedizione entro e non oltre le ore 10,00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal Responsabile del Servizio che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

#### **Articolo 43**

##### **Spedizione dei documenti informatici**

I documenti informatici sono trasmessi all'indirizzo di posta elettronica certificata dichiarato dai destinatari abilitato alla ricezione della posta per via telematica.

Per la spedizione dei documenti informatici l'Amministrazione si avvale del servizio di Posta Elettronica Certificata offerto da un certificatore iscritto nell'elenco pubblico tenuto dal CNIPA, ai sensi dell'articolo 27, comma 3, del Testo Unico.

Gli uffici trasmettono i documenti informatici in partenza, all'indirizzo elettronico di PEC, dopo aver eseguito le operazioni di registrazione di protocollo, segnatura di protocollo, classificazione e fascicolazione.

L'ufficio di spedizione provvede:

- ad effettuare l'invio telematico utilizzando i servizi di PEC offerti dal certificatore scelto dall'Amministrazione;
- a verificare l'avvenuto recapito dei documenti spediti per via telematica;
- ad archiviare le ricevute elettroniche collegandole alle registrazioni di protocollo dei rispettivi documenti spediti.

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

della 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 (cfr. articolo 17, comma 1, del Testo Unico).

## SEZIONE XI

### FLUSSO DI LAVORAZIONE DEI DOCUMENTI

#### **Articolo 44**

##### **Flusso di lavorazione dei documenti ricevuti**

Le fasi della gestione dei documenti ricevuti sono:

- a) ricezione (cfr. sezione IV)
- b) registrazione e segnatura di protocollo (cfr. sezione V)
- c) scansione, se si tratta di documenti su supporto cartaceo (cfr. sezione VIII)
- d) assegnazione (cfr. VII)
- e) classificazione (cfr. sezione VI)
- f) fascicolazione (cfr. sezione IX)

#### **Articolo 45**

##### **Flusso di lavorazione dei documenti spediti**

Le fasi della gestione dei documenti spediti sono:

- a) produzione (cfr. sezione III)
- b) registrazione e segnatura di protocollo (cfr. sezione V)
- c) classificazione (cfr. sezione VI)
- d) fascicolazione (cfr. sezione IX)
- e) spedizione (cfr. sezione X)

#### **Articolo 46**

##### **Flusso di lavorazione dei documenti interni**

Le fasi della gestione dei documenti interni sono:

- a) produzione (cfr. sezione III)
- b) registrazione e segnatura di protocollo (cfr. sezione V)
- c) classificazione (cfr. sezione VI)
- d) fascicolazione (cfr. sezione IX)



## SEZIONE XII

### GESTIONE DEI FLUSSI DOCUMENTALI

#### **Articolo 47**

##### **Comunicazioni informali tra uffici utente**

Per comunicazione informale tra uffici utente si intende uno scambio di informazioni, con o senza documenti allegati, del quale non si ritiene necessario tenere traccia in archivio.

Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica e non interessano il sistema di protocollo informatico.

#### **Articolo 48**

##### **Scambio di documenti tra uffici utente**

La trasmissione di documenti da un ufficio ad un altro, per lo svolgimento di procedimenti amministrativi complessi, avviene con le seguenti modalità:

a) l'ufficio mittente:

- produce la lettera di trasmissione e la registra nel sistema di protocollo informatico, specificando il codice del fascicolo o sottofascicolo nel quale si colloca;
- trasmette la lettera con gli eventuali allegati all'ufficio destinatario.

b) l'ufficio destinatario:

- acquisisce i documenti ed effettua l'operazione di "presa in carico" fissando così la data di ricezione;
- in base alle attività da svolgere:
  - apre un nuovo fascicolo impostando la relazione di "collegato" all'unità archivistica indicata dall'ufficio mittente nella lettera di trasmissione;
  - in alternativa, nei casi più semplici, produce il documento di risposta "concatenandolo" a quello ricevuto senza aprire un altro carteggio.

Nel caso in cui un ufficio utente richieda ad un'altra UO lo sviluppo di un sub procedimento, la trasmissione dei documenti avviene con le seguenti modalità:

a) l'ufficio mittente:

- produce la lettera di trasmissione e la registra nel sistema di protocollo informatico
- apre il sottofascicolo o l'insero nel quale l'unità destinataria dovrà inserire i documenti prodotti nell'ambito del sub procedimento richiesto;
- inserisce la lettera con gli eventuali allegati nel sottofascicolo o insero e invia il tutto all'ufficio destinatario

b) l'ufficio destinatario:

- acquisisce il sottofascicolo o l'insero ed effettua l'operazione di "presa in carico" fissando così la data di ricezione;
- sviluppa la propria azione amministrativa inserendo i documenti nell'unità archivistica predisposta dall'ufficio mittente

- al termine, rinvia tutta la documentazione all'ufficio mittente con un'apposita funzione del sistema

Attivando la gestione elettronica dei documenti, tutte le operazioni di cui ai commi 1 e 2 sono svolte direttamente su computer senza movimentare la carta. La lettera di trasmissione viene prodotta a partire da un modello elettronico predefinito; la sottoscrizione della lettera è assicurata con una firma elettronica; i documenti allegati sono file selezionati dall'archivio informatico; l'invio dei documenti e dei fascicoli avviene in forma elettronica mediante una specifica funzione del sistema di protocollo informatico.

<b>SEZIONE XIII</b> <b>ARCHIVIAZIONE DEI DOCUMENTI</b>
---

Il piano di conservazione dell'archivio dell'area organizzativa omogenea, comprendente il titolario di classificazione ed il massimario di scarto, è riportato nell'allegato n. 3.

#### **Articolo 49**

#### **Memorizzazione dei documenti informatici e delle rappresentazioni digitali dei documenti cartacei**

I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo. Le rappresentazioni digitali dei documenti su supporto cartaceo, acquisite con l'ausilio di scanner, sono memorizzate nel sistema, in modo non modificabile, al termine del processo di scansione.

#### **Articolo 50**

#### **Versamento dei fascicoli nell'archivio di deposito**

All'inizio di ogni anno, gli uffici utente individuano i fascicoli cartacei che sono da versare nell'archivio di deposito in quanto relativi ad affari o procedimenti conclusi, o comunque non più necessari allo svolgimento delle attività correnti. Dopo di che li inviano all'archivio di deposito con un'apposita funzione del sistema di protocollo informatico, curando anche il trasferimento fisico degli eventuali carteggi.

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

Il Responsabile dell'ufficio protocollo cura la formazione e la conservazione di un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.

#### **Articolo 51**

#### **Archiviazione ottica**

##### Fascicoli cartacei

Il personale preposto alla gestione dell'archivio di deposito, a seguito del versamento dei fascicoli da parte degli uffici utente, effettua l'operazione di archiviazione su supporti di memorizzazione sostitutivi del cartaceo, in conformità alle disposizioni di cui all'articolo 7 della deliberazione AIPA 23 novembre 2000, n° 51.

#### Fascicoli informatici nativi

I documenti informatici, come i relativi fascicoli, sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

Il processo di conservazione digitale prende avvio immediatamente al termine della procedura di archiviazione digitale

Le informazioni relative alla gestione informatica dei documenti costituiscono parte integrante del sistema di indicizzazione e di organizzazione dei documenti che sono oggetto delle procedure di conservazione sostitutiva.

Dei documenti prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.

Si applicano in ogni caso, per l'archiviazione e la custodia dei documenti contenenti dati personali, le disposizioni di legge sulla tutela della riservatezza dei dati personali.

### **Articolo 52**

#### **Selezione e scarto archivistico**

Nel piano di conservazione dell'archivio, inserito nel sistema di gestione informatica dei documenti, insieme al titolare di classificazione è presente anche un massimario di scarto. Gli operatori dell'archivio di deposito, pertanto, possono utilizzare questo sistema per produrre annualmente l'elenco dei documenti e dei fascicoli per i quali è trascorso il periodo obbligatorio di conservazione e che quindi sono suscettibili di scarto archivistico.

I documenti selezionati per la conservazione permanente sono trasferiti, contestualmente agli strumenti che ne garantiscono l'accesso, nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

## SEZIONE XIV

### GESTIONE DEI PROCEDIMENTI AMMINISTRATIVI

#### **Articolo 53**

##### **Elenco dei procedimenti amministrativi**

L'Amministrazione costituisce una banca dati dei procedimenti amministrativi, sulla base del "Regolamento sui procedimenti amministrativi e sul diritto di accesso ai documenti amministrativi" approvato con deliberazione di Consiglio Provinciale, registrando, per ciascuno di essi, al minimo, le seguenti informazioni:

- la denominazione;
- l'ufficio utente di competenza;
- il Responsabile del procedimento;
- il termine di conclusione;
- classificazione;
- tipo fascicolo (tipologia, oggetto, ecc.).

#### **Articolo 54**

##### **Avvio dei procedimenti amministrativi e registrazione dei loro stati di avanzamento**

Nell'ambito dell'operazione di assegnazione dei fascicoli agli uffici utente di competenza, gli uffici abilitati provvedono a dare avvio ai relativi procedimenti amministrativi.

In questo modo, il sistema di gestione informatica dei documenti fissa, automaticamente per ogni procedimento i seguenti dati:

- il Responsabile del procedimento;
- il termine di scadenza;
- l'iter procedimentale.

La registrazione degli stati di avanzamento avviene a cura dei Responsabili dei procedimenti, in modo manuale o automatico. Nel primo caso, gli stati di avanzamento sono aggiornati dal personale che svolge le pratiche; nel secondo caso, è il software che muove i fascicoli e registra in automatico l'evolversi dell'azione amministrativa.

## SEZIONE XV

### ACCESSIBILITÀ AL SISTEMA DI GESTIONE INFORMATICADEI DOCUMENTI

#### **Articolo 55**

##### **Accessibilità da parte degli utenti appartenenti all'area organizzativa omogenea**

La riservatezza delle registrazioni di protocollo e dei documenti informatici è garantita dal sistema attraverso l'uso di profili utente e password, od altre tecniche e dispositivi di autenticazione sicura.

L'operatore che effettua la classificazione inserisce il livello di riservatezza richiesto per il documento in esame, se diverso da quello standard applicato automaticamente dal sistema.

In modo analogo, l'ufficio che effettua l'operazione di apertura di un nuovo fascicolo ne determina anche il livello di riservatezza, se diverso da quello standard applicato automaticamente dal sistema.

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

Sono riservati:

- i documenti che contengono "dati sensibili" ai sensi di legge;
- i documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'azione amministrativa.

I livelli di riservatezza gestiti dal sistema, il livello standard applicato automaticamente e le relative abilitazioni all'accesso interno delle informazioni documentali sono riportati nell'allegato 5.

#### **Articolo 56**

##### **Accesso esterno**

L'accesso al sistema informatico dei documenti da parte di utenti esterni è realizzato anche mediante l'impiego di sistemi di riconoscimento ed autenticazione sicura basati sulla carta d'identità elettronica e sulla firma digitale.

Sono rese disponibili tutte le informazioni necessarie e sufficienti all'esercizio del diritto di accesso ai documenti amministrativi.

#### **Articolo 57**

##### **Accesso da parte di altre pubbliche amministrazioni**

L'accesso al sistema di gestione informatica dei documenti da parte di altre pubbliche amministrazioni è realizzato applicando le norme ed i criteri tecnici emanati per la realizzazione della rete unitaria delle pubbliche amministrazioni.

Le informazioni rese disponibili sono:

- il numero e la data di protocollo, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;
- il numero e la data di protocollo del documento ricevuto, ottenuti attraverso il numero e la data di protocollo attribuiti dall'amministrazione al documento spedito.

<p>SEZIONE XVI</p> <p>PIANO DI SICUREZZA INFORMATICA RELATIVO ALLA FORMAZIONE, GESTIONE, TRASMISSIONE, INTERSCAMBIO, ACCESSO E CONSERVAZIONE DEI DOCUMENTI INFORMATICI</p>
--

## Articolo 58

### **Sicurezza del Sistema Informativo Automatizzato**

Un sistema informativo automatizzato si definisce sicuro quando soddisfa le seguenti proprietà:

- **Disponibilità:** l'informazione ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio.
- **Integrità:** l'informazione ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tali operazioni.
- **Autenticità:** garanzia e certificazione della provenienza dei dati.
- **Confidenzialità o Riservatezza:** l'informazione che contiene può essere fruita solo dalle persone autorizzate

La sicurezza del sistema informativo automatizzato va intesa non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali", ma anche come "limitazione degli effetti causati dall' eventuale occorrenza di tali cause".

## Articolo 59

### **Piano della Sicurezza Informatica**

Il piano per la sicurezza informatica, riconosce la validità dei documenti che costituiscono il Documento Programmatico sulla Sicurezza dei dati personali, in seguito denominato DPSS, approvato da ultimo con deliberazione di Giunta Provinciale n.60/2010 del 24.03.2010.

Il piano è relativo alla formazione, gestione, trasmissione, interscambio, accesso e conservazione dei documenti informatici, ai sensi dell'articolo 4, comma 1, lettera c), del DPCM 31 ottobre 2000 e all'articolo 10 della deliberazione AIPA 51/2000. Il Piano considera, in base all'art.10, c.3 della deliberazione AIPA n.51 del 23.11.2000 i seguenti aspetti:

- analisi del rischio,
- politiche di sicurezza,
- interventi operativi,
- piano della formazione.

Il Piano è predisposto dal Responsabile dei sistemi informativi automatizzati d'intesa con il Responsabile del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi e con il Responsabile della sicurezza dei dati personali di cui al D.Lgs 196/2003, e successive modificazioni ed integrazioni, e nel rispetto delle misure minime di sicurezza previste dal regolamento di attuazione emanato con DPR 318/99, come dettato dall'art.4, comma 1 lett.c) del DPCM 31.10.2000.

Il piano fa parte del manuale di gestione di cui alle regole tecniche emanate ai sensi del D.P.R. 20 ottobre 1998, n. 428 (art. 10 c. 2 Deliberazione AIPA 51/2000).

Il piano è sottoposto a verifica e viene aggiornato con cadenza almeno biennale (art. 10 c. 4 Deliberazione AIPA 51/2000).



## **Articolo 60**

### **Individuazione dei beni da proteggere**

Gli elementi del sistema informativo automatizzato che necessitano di protezione sono le risorse hardware, le risorse software, i supporti di memorizzazione e i dati trattati.

L'elenco delle risorse hardware, software e dei supporti di memorizzazione, (secretato per ragioni di sicurezza) è parte integrante del Documento Programmatico sulla Sicurezza dei dati personali, in seguito denominato DPSS, approvato da ultimo con deliberazione di Giunta Provinciale n.72/2009 del 24.03.2009 e viene predisposto e mantenuto costantemente aggiornato dal Responsabile dei sistemi informativi automatizzati.

I dati trattati, ai sensi della legge 196/2003 e dell'allegato alla citata deliberazione di Giunta Provinciale n.72/2009 del 24.03.2009, tenuti su supporti gestiti dai singoli Servizi sono censiti e sottoposti ad apposite misure di sicurezza con propria determinazione dal responsabile del trattamento, individuato nella deliberazione di Giunta Provinciale n.72/2009 del 24.03.2009.

L'elenco delle banche dati centrali è allegato (secretato per ragioni di sicurezza) al DPSS ed i dati ivi contenuti sono sottoposti a misure di protezione a carico del Responsabile dei sistemi informativi automatizzati.

## **Articolo 61**

### **Individuazione delle minacce**

Gli elementi che minacciano il patrimonio informativo sono riportati in allegato al DPSS.

L'elenco delle minacce, (secretato per ragioni di sicurezza) viene predisposto e mantenuto costantemente aggiornato dal Responsabile dei sistemi informativi automatizzati.

## **Articolo 62**

### **Individuazione delle contromisure**

Le contromisure di natura fisica, logica ed organizzativa, da adottare al fine di ridurre i rischi individuati, (secretate per ragioni di sicurezza) sono riportate in allegato al DPSS.

Le contromisure si suddividono in misure di sicurezza fisica, misure di sicurezza elettroniche, politiche di sicurezza, piano di monitoraggio e piano di recupero.

Nell'ambito delle politiche di sicurezza è stato adottato un apposito regolamento relativo all'accesso e all'uso della rete informatica e telematica, approvato con deliberazione di Giunta Provinciale n.88 del 29/4/2003 e successive modificazioni e integrazioni.

Si deve prevedere un piano di recupero in caso di evento disastroso, ovvero la descrizione dei criteri e delle modalità adottate per il ripristino della disponibilità dei sistemi e dei dati, in caso di danneggiamento o distruzione.

Le contromisure di cui al presente articolo sono di competenza del Responsabile del trattamento qual ora la banca dati sia creata e gestita nell'ambito del singolo Servizio.

Si devono descrivere i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamento dei dati dell'Amministrazione affidato all'esterno della struttura del titolare.

L'elenco delle contromisure, secrete per ragioni di sicurezza, viene predisposto e mantenuto costantemente aggiornato dal Responsabile dei sistemi informativi automatizzati.

### **Articolo 63**

#### **Norme per il personale**

Tutti i dipendenti dell'Amministrazione concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito dalle politiche di cui all'art.59, in particolare relativamente all'utilizzo delle risorse informatiche, all'accesso ai sistemi e ai dati e all'uso della password (art.3, c.1 del Reg. utilizzo attrezzature informatiche).

### **Articolo 64**

#### **Il piano della formazione**

L'introduzione del piano per la sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, è accompagnata da un piano per la formazione di cui al DPSS.

Il piano della formazione viene predisposto e aggiornato con cadenza almeno biennale dal Responsabile della formazione dell'Amministrazione d'intesa con il Responsabile dei sistemi informativi automatizzati.

## SEZIONE XVII

### FUNZIONALITÀ DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Questa sezione del manuale riporta la descrizione funzionale e tecnica del sistema di gestione informatica dei documenti, denominato “IRIDE”, utilizzato dall’Amministrazione. Nei singoli paragrafi della Sezione sono riportati i riferimenti normativi relativi all’argomento

#### **Articolo 65**

##### **La generalità delle funzioni del sistema Iride**

Sono le funzioni riportate nel manuale utente del prodotto allegato al manuale di gestione informatica dei documenti. Sono quelle riconducibili ai vari moduli di IRIDE:

1. gestione protocollo informatico;
2. iter pratiche e procedimenti amministrativi;
3. gestione segreteria

#### **Articolo 66**

##### **Sistema operativo utilizzato per la gestione informatica dei documenti di cui all’articolo 7, commi 1 e 6 del DPCM 31 Ottobre 2000**

Requisiti minimi di sicurezza del sistema operativo dell’elaboratore [DPCM31.10.00/7/1]

- a) La gestione degli accessi avviene tramite la dichiarazione di “Utenti/Ruoli” dotati di password cui fa riscontro una univoca identificazione ed autenticazione da parte del sistema.
- b) La protezione delle informazioni relative a ciascun utente/ruolo nei confronti degli altri avviene tramite la dichiarazione di specifiche “Regole” abilitabili per ciascun ruolo.
- c) La garanzia di accesso alle risorse esclusivamente per gli utenti/ruoli abilitati si ottiene combinando opportune “Regole” per i ruoli ed attivando per gli stessi ruoli la visibilità di appositi “Livelli di sicurezza” registrati sui documenti sui quali si vogliono apporre particolari criteri di sicurezza o riservatezza.
- d) La registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo da garantirne la identificazione viene assicurata in quanto l’applicativo garantisce la registrazione cronologica degli eventi e ne segnala l’autore in fase di registrazione del documento di protocollo.
- e) La garanzia delle conformità alle specifiche indicate nella circolare AIPA n.31 del 21 giugno 2001 sono affidate al sistema operativo (Windows 2008 R2) e del Database relazionale (SQL Server 2005) che completano il sistema di gestione del protocollo dell’Ente.

## Articolo 67

### **Le misure di sicurezza di cui all'articolo 7, commi 2,3, 4 del DPCM 31 Ottobre 2000**

- a) Sono garantite dalla disponibilità dei meccanismi che consentano il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti in condizioni di sicurezza nel rispetto delle disposizioni in materia di tutela delle persone e degli altri soggetti rispetto al trattamento dei dati personali. [DPCM31.10.00/7/2]

Il sistema consente la definizione e la attribuzione di differenti diritti di accesso ai singoli utenti/ruoli abilitati al sistema e permette il controllo selettivo sull'accesso alle risorse oltre ad inibire o meno l'accesso ad alcune funzionalità, anche mediante la creazione di profili di utente. A questo scopo:

1. si attivano per il singolo ruolo opportune "regole";
2. si dà visibilità dei documenti abilitando il ruolo ad opportuni "livelli di sicurezza";  
si inibiscono al ruolo le "abilitazioni" all'uso di alcune funzionalità e/o strumenti.

Per quanto riguarda i documenti contenenti dati sensibili, con particolare riferimento alle pratiche di polizia giudiziaria, verrà definita una regola di protezione per il ruolo Polizia Provinciale. In questo modo tutto quello che tale ruolo protocollerà avrà un livello di sicurezza PP e sarà visibile solo al ruolo autore e ai destinatari interni.

- b) tracciamento da parte del sistema di protocollo informatico di qualsiasi evento di modifica delle informazioni trattate e individuazione del suo autore. [DPCM311000/7/3]

Il sistema Iride effettua la registrazione cronologica degli eventi (ne segnala l'autore, la data e l'ora sia in fase di registrazione del documento di protocollo, che in fase di modifica dandone visibilità) . In questo ultimo caso (modifica) è in grado di produrre anche un Registro (report) delle modifiche dei documenti di protocollo. Nota: gli eventi di modifica sono "catturati" da appositi triggers installati nel Database.

- c) Protezione delle registrazioni di tracciamento da modifiche non autorizzate. [DPCM31.10.00/7/4]

Le registrazioni inerenti agli eventi di modifica delle informazioni e relativi autori sono memorizzate in un archivio cronologico (log) che viene reso immutabile da parte di utenti non autorizzati tramite la corretta gestione di permessi/accessi sulla Tabella LOG\_IRIDE del Database relazionale SQL dell'applicativo.

## Articolo 68

### **Le misure tecniche atte a garantire la non modificabilità delle registrazioni di protocollo e del registro giornaliero di protocollo**

- La non modificabilità viene garantita:
  - a. dalla definizione di specifiche "regole" per gli utenti/ruoli;

- b. dalla attivazione di specifici “trigger” atti a registrare ovvero tenere traccia dei possibili eventi di modifica effettuati sui documenti di protocollo.
- La tenuta della copia giornaliera del registro di protocollo prevede:
  - a. La produzione della stampa giornaliera del registro (report di Access);
  - b. L’esportazione e conversione della stessa stampa in un file in formato PDF;
  - c. L’archiviazione della stampa giornaliera su supporto magnetico non riscrivibile (CD).
  - d.

## **Articolo 69**

### **Le misure tecniche atte ad assicurare la contemporaneità delle operazioni di registrazione e segnatura di protocollo**

- Al momento della conferma della registrazione del protocollo corrente, viene reso disponibile l’utilizzo di un tasto funzionale “Timbro” che consente la produzione/apposizione della segnatura sul documento cartaceo. L’apposizione avviene a cura dell’operatore.

## **Articolo 70**

### **Le modalità di trattamento delle informazioni annullate o modificate**

- a. Esistenza di una funzione di annullamento delle informazioni non modificabili delle registrazioni e/o dell’intera registrazione [TU4452000/54/1] e [DPCM311000/8]
  - b. Memorizzazione delle informazioni annullate nella base di dati [TU4452000/54/1] e [DPCM311000/8]
1. E’ sufficiente dichiarare gli utenti/ruoli per i quali abilitare la “regola” che consente agli stessi di annullare una registrazione di protocollo.
  2. L’annullo si ottiene richiedendo la cancellazione dalla form del protocollo. Occorre obbligatoriamente indicare il motivo dell’annullamento (estremi del provvedimento di autorizzazione). Dopo la conferma non è più possibile modificare tale protocollo che risulterà comunque visibile con l’indicazione di protocollo annullato.
  3. Nel Report REGISTRO di PROTOCOLLO viene aggiunta l’evidenza dei protocolli annullati.

## **Articolo 71**

### **Le funzioni per la gestione del registro di emergenza ed il conseguente recupero automatico dei dati**

E’ stata implementata la nuova gestione del registro di emergenza di protocollo. Nel caso uno o più uffici di protocollo siano impossibilitati a protocollare a causa di un guasto tecnico possono continuare il loro lavoro utilizzando la seguente procedura:

- a. L’ufficio apre un registro cartaceo in cui annota gli estremi di protocollo assegnando nel contempo un numero progressivo a partire da 1 e la data.

- b. L'ufficio annota sul documento cartaceo il numero e la data specificando chiaramente la dicitura "REGISTRO DI EMERGENZA"
- c. Quando il guasto viene riparato l'utente inserisce tutti i protocolli presenti nel registro cartaceo seguendo la normale procedura di protocollazione.
- d. Attraverso il bottone "R.Emer." introduce i dati UFFICIO,NUMERO e DATA corrispondenti al registro di emergenza.
- e. Un protocollo di emergenza assume quindi 2 numeri: uno fittizio che segue la normale numerazione di protocollo e uno invece con validità giuridica assegnato manualmente in emergenza.
- f. La procedura IRIDE indica chiaramente quando un protocollo è di emergenza attraverso opportune scritte di colore rosso.
- g. La procedura inoltre permette la ricerca dei protocolli di emergenza (sia dalla pagina di ricerca che da quella di protocollo) e la stampa di un particolare registro
- h. All'atto dell'inserimento di un protocollo di emergenza la procedura controlla unicamente che non esistano altri protocolli di emergenza con stesso Ufficio, Numero, Data.

## **Articolo 72**

### **Le modalità di trasmissione, ricezione, verifica, registrazione ed archiviazione dei documenti informatici**

- Riguarda principalmente aspetti della "Interoperabilità".

## **Articolo 73**

### **Il calcolo della impronta dei documenti informatici (DPCM31.10.00/17/2 e TU445/2000/53/1/f)**

L'impronta di un documento è una stringa a lunghezza fissa (memorizzata nel campo DOC\_TESTI.DAT\_IMPRONTA) ottenuta attraverso l'applicazione di un algoritmo detto di "hash" ad una sequenza di byte. Lo scopo è quello di assicurare una corrispondenza certa tra la sequenza di byte e la stringa ottenuta. In IRIDE viene applicata ai campi BLOB allo scopo di certificare la non modificabilità dell'oggetto contenuto nel blob. Per ulteriore sicurezza quando la firma è stata apposta il documento non risulta modificabile. Due bottoni "Impronta" e "Verifica" permettono la gestione di questa nuova funzionalità. Attualmente non è prevista la cancellazione di una impronta.

## **Articolo 74**

### **La segnatura di protocollo dei documenti di cui agli articoli 9, 18 e 19 del DPCM 31 ottobre 2000**

- a. *Presenza nella segnatura di protocollo delle informazioni minime per l'identificazione univoca di ciascun documento: codice identificativo dell'Amministrazione, codice identificativo della AOO, progressivo di protocollo, data di protocollo. [DPCM31.10.00/9/1]*

La segnatura/timbratura riproduce i dati essenziali del protocollo corrente :

- Denominazione dell'Ente
- Numero progressivo unico per l'Ente;
- Data: giorno mese anno;
- Classifica

***b. I dati relativi alla segnatura di protocollo di un documento trasmesso da una AOO sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file, conforme alle specifiche XML 1.0 (raccomandazione W3C 10 febbraio 1998), conforme con un file DTD (Documento Type Definition) di cui alla circolare AIPA n. 28 del 7/5/2001, ovvero alla sua versione più recente. [DPCM31.10.00/18/1]***

- La segnatura XML viene generata dalle funzionalità di trasmissione dei documenti fra AOO che riguardano gli aspetti della "Interoperabilità".

***c. Il sistema deve supportare e/o integrare strumenti di firma elettronica ai fini della sottoscrizione dei documenti informatici e alla loro gestione (visualizzazione, verifica della firma). [DPCM31.10.00/18/3]***

- Iride integra strumenti di firma elettronica e ne consente la gestione sia in termini di apposizione della firma, sia di verifica che di visualizzazione.

***d. Requisito di completezza della segnatura informatica [DPCM31.10.00/19/1] - [DPCM31.10.00/19/2]***

- La segnatura XML risponde ai requisiti di completezza; riguarda aspetti della "Interoperabilità".

## **Articolo 75**

### **Le funzionalità per lo scambio di documenti informatici tra uffici utente e tra aree organizzative omogenee**

Lo scambio dei documenti informatici tra uffici viene effettuato tramite l'utilizzo dello strumento scrivania (virtuale) associata ad uno o più utenti/ruoli. La movimentazione e la visibilità dei documenti scambiati fra scrivanie viene assicurata dalla associazione delle varie tipologie di documenti ad un "Iter". I movimenti vengono espletati dal motore esecutore dei passi operativi di ciascun specifico iter.

Per la descrizione particolareggiata di tutte le funzioni di Iride si fa riferimento al manuale utente fornito dal produttore di Iride conservato agli atti dell'Amministrazione.

## SEZIONE XVIII

### DISPOSIZIONI FINALI

#### **Articolo 76**

##### **Pubblicità**

Il presente manuale è pubblicato e reso accessibile mediante l'inserimento nel sito Internet della Provincia <http://www.provincia.rimini.it> e comprensivo di tutti gli allegati sulla Intranet della Provincia di Rimini.

#### **Articolo 77**

##### **Modalità di aggiornamento**

Il manuale sarà oggetto di aggiornamento periodico e comunque ogni qualvolta si renda necessario per intervenuti mutamenti a livello organizzativo, normativo e tecnologico, con apposito provvedimento dell'organo competente.

#### **Articolo 78**

##### **Norme transitorie**

Le operazioni di formazione, ricezione, trasmissione, gestione ed archiviazione dei documenti informatici presuppongono la disponibilità di una piattaforma tecnologica di firma elettronica conforme alla normativa vigente, di un servizio di posta elettronica certificata e, in generale, di un impianto informatico avanzato e posto in sicurezza che al momento della stesura del manuale di gestione potrebbe non essere completamente disponibile.

Quindi i seguenti articoli possono entrare in vigore in un momento successivo alla pubblicazione del manuale, qualora si attivino le relative procedure:

Sezione III: art. 9, 10

Sezione IV. art. 12

Sezione V art. 17

Sezione VII: art. 34

Sezione VIII: art: 35, 36

Sezione IX: art. 37, 38

Sezione X: art. 42

Sezione XIII: art. 48, 50;

Sezione XIV: art. 53.



Allegati
----------

allegato n° 1: abilitazioni all'utilizzo del sistema di gestione informatica dei documenti

allegato n° 2: elenco dei documenti esclusi dalla registrazione di protocollo e soggetti a registrazione particolare

allegato n° 3: a) piano di classificazione dei documenti  
b) piano di conservazione dell' archivio della Provincia

allegato n° 4: uffici abilitati all'assegnazione dei documenti

allegato n° 5: livelli di riservatezza e corrispondenti logiche di protezione