COMUNE
LATISANA

***Tenuta del protocollo informatico, gestione dei flussi documentali e degli archivi***

# Manuale di gestione documentale

**Adottato con deliberazione della Giunta comunale n. 20 del 09/02/2021**

**INDICE**

## SEZIONE I

## DEFINIZIONI E AMBITO DI APPLICAZIONE

**Premessa**
Secondo quanto previsto dalle Regole tecniche sul protocollo, introdotte con il DPCM 03 dicembre 2013, e a norma delle previsioni contenute nelle Regole tecniche sui documenti informatici introdotte con il DPCM 13 novembre 2014, le pubbliche amministrazioni sono tenute ad adottare un manuale di gestione documentale che descriva il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e non oltre a fornire le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

A norma delle citate regole tecniche, la predisposizione del manuale è un'attività affidata al Responsabile della gestione documentale, ossia al soggetto che si occupa di definire, all'interno di una determinata Area Organizzativa Omogenea (AOO - una struttura o un insieme di strutture aventi regole comuni di gestione documentale) le politiche di gestione dei flussi, il trattamento e la sicurezza informatica dei documenti, la tenuta del protocollo, l'archiviazione, e la conservazione dei documenti.

### Art. 1
### Ambito di applicazione

1. Il presente Manuale di gestione dei documenti è adottato ai sensi degli articoli 3 e 5 DPCM 31 ottobre 2000 e del DPCM 3 dicembre 2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice di amministrazione digitale di cui al decreto legislativo n. 82 del 2005" e descrive il sistema di gestione e conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione delle attività dei flussi documentali e degli archivi.
2. Disciplina, inoltre, i criteri e le regole per la registrazione, classificazione, fascicolazione e archiviazione dei documenti, oltre che la gestione dei flussi documentali del Comune di Latisana.

### Art. 2
### Definizioni

1. Ai fini del presente manuale di gestione si intende per:

   a) "**AMMINISTRAZIONE**", il Comune di LATISANA
   b) "**TESTO UNICO**", il D.P.R. 20.12.2000, n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
   c) "**C.A.D**.", il D. Lgs. 7.3.2005, n. 82 recante "Codice dell'Amministrazione Digitale";
   d) "**REGOLE TECNICHE PI**", il D.P.C.M. 3.12.2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71 del C.A.D.";
   d-bis) "**REGOLE TECNICHE CONS**", D.P.C.M. 3,12,2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"
   e) "**AOO**", l'Area Organizzativa Omogenea;
   f) "**RPA**", il Responsabile del Procedimento Amministrativo;
   g) "**RSP**", il Responsabile per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi;
   h) "**UOP**", l'Unità Organizzativa di registrazione di Protocollo, cioè l'ufficio che svolge attività di registrazione di protocollo;

i) "**UU**", l'Ufficio Utente, cioè l'ufficio destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali; in linea di massima ogni UU corrisponde a un Servizio o Area dell'Amministrazione.

## SEZIONE II

## DISPOSIZIONI GENERALI

### Art. 3
### Aree organizzative omogenee

1. Per la gestione dei documenti, l'Amministrazione istituisce un'unica Area Organizzativa Omogenea (AOO).
2. L'Area Organizzativa Omogenea comprende l'insieme degli uffici utente che la compongono con la loro articolazione gerarchica e fa riferimento all'organigramma attuale del Comune.
3. Nell'Area Organizzativa Omogenea così individuata è istituito il Servizio di Protocollo che cura la gestione dei flussi documentali e archivi, che nel prosieguo sarà definito semplicemente Servizio di Protocollo, afferente all'Area Affari Generali dell'Ente.

### Art. 4
### Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali

1. Ai sensi della normativa vigente**,** l'Amministrazione è dotata del Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali, individuandolo nel Servizio di Protocollo dell'Ente succitato.
2. Al Servizio è preposto il Responsabile della già menzionata Unità Organizzativa.
3. Il Servizio svolge i seguenti compiti:
   a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
   b) garantisce che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della normativa vigente;
   c) vigila sulle attività di produzione e conservazione del registro giornaliero di protocollo;
   d) cura, di concerto con l'Area Sistemi Informativi ed e-Government e Insiel S.p.A., che le funzionalità del sistema, in caso di guasti o anomalie, vengano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
   e) cura, di concerto con l'Area Sistemi Informativi ed e-Government, la conservazione delle copie di cui alla normativa vigente;
   f) vigila sul buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
   g) provvede alle operazioni di annullamento delle registrazioni di protocollo;
   h) vigila sull'osservanza delle disposizioni del presente Manuale di gestione da parte del personale autorizzato e degli incaricati, di concerto con il Segretario generale dell'Ente e con il personale dell'Area Sistemi Informativi ed e-Government.

### Art. 5
### Unicità del protocollo informatico

1. Nell'ambito dell'Area Organizzativa Omogenea la numerazione delle registrazioni di protocollo è unica e progressiva.
2. Essa si chiude al 31 dicembre di ciascun anno solare e ricomincia all'inizio dell'anno successivo.
3. 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 sono strettamente correlati tra loro.

4. 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.
5. Per la gestione dei documenti è adottato un modello organizzativo che prevede la partecipazione attiva di più soggetti e uffici, ognuno dei quali è abilitato a svolgere soltanto le operazioni di propria competenza. I responsabili di Servizio/Area e d'ufficio si fanno carico della correttezza della protocollazione degli atti eseguita dagli utenti da loro dipendenti, abilitati alle registrazioni di protocollo.

## SEZIONE III

## CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

### Art. 6
### Conservazione delle copie del registro informatico di protocollo

**1.** Ai sensi della normativa vigente, il registro giornaliero di protocollo è trasmesso con procedura automatizzata entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

### Art. 7
### Caselle di Posta elettronica

1. L'AOO è dotata della casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA) e nel Registro delle Pubbliche Amministrazioni di cui all'art. 16 comma 12 del D.L. 179/2012 gestito dal Ministero della Giustizia; questa casella costituisce l'indirizzo virtuale dell'AOO e di tutti gli uffici che ad essa fanno riferimento.
2. La casella di Posta Elettronica Certificata dell'Ente (comune.latisana@certgov.fvg.it) è accessibile per la ricezione e protocollazione in ingresso solo dall'Ufficio Protocollo, mentre per l'invio e relativa protocollazione in uscita è accessibile dagli utenti dei diversi servizi abilitati all'applicativo.
3. Una seconda casella di Posta Elettronica Certificata dell'Ente (polizialocale.latisana@certgov.fvg.it) associata al servizio di Polizia Locale, è accessibile per la consultazione della corrispondenza e protocollazione in entrata e uscita, all'Ufficio Protocollo e agli utenti del servizio di Polizia Locale abilitati.
4. Riguardo alla protocollazione delle PEC citate, si utilizza la numerazione unica del protocollo generale.
5. Il portale del servizio SUAP (Sportello Unico Attività Produttive) e il portale del servizio SUE (Sportello Unico Edilizia) sono interconnessi e integrati con la PEC e il servizio di protocollo generale dell'Ente. Pertanto, alla corrispondenza elettronica, viene assegnata automaticamente una registrazione e segnatura di protocollo univoca e consultabile sia dai portali menzionati e sia dall'applicativo di protocollo in uso.
6. Ogni Servizio/Area è dotato di e-mail istituzionale non certificata, le mail sono riportate nel sito istituzionale sezione "Trasparenza" secondo quanto stabilito dal D.L. 33/2013.

### Art. 8
### Sistema di classificazione dei documenti

1. A seguito dell'introduzione del protocollo unico di cui all'art. 5 e per garantire la corretta classificazione e organizzazione dei documenti nell'archivio, a partire dalla fase corrente, viene adottato il "Titolario di classificazione" di cui all'**Allegato A.**

## SEZIONE IV

## Formazione dei documenti

### Art. 9
### Principi generali

1. Secondo quanto previsto dalla normativa vigente, l'Amministrazione forma gli originali dei propri documenti con mezzi informatici.
2. Fermo restando quanto previsto al comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria.
3. Ogni documento per essere inoltrato in modo formale, all'esterno o all'interno dell'Amministrazione:
   a) deve trattare un unico argomento indicato in modo sintetico ma esaustivo, a cura dell'autore, nello spazio riservato all'oggetto;
   b) deve riferirsi a un solo protocollo;
   c) può fare riferimento a più fascicoli.
4. Le firme necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
5. Il documento deve consentire l'identificazione dell'Amministrazione mittente attraverso le seguenti informazioni:
   a) la denominazione e il logo dell'Amministrazione;
   b) l'indirizzo completo dell'Amministrazione;
   c) il codice fiscale dell'Amministrazione;
   d) l'indicazione completa dell'ufficio dell'Amministrazione che ha prodotto il documento corredata dai numeri di telefono e fax.
6. Il documento, inoltre, deve recare almeno le seguenti informazioni:
   a) il luogo di redazione del documento;
   b) la data (giorno, mese, anno);
   c) il numero di protocollo;
   d) il numero degli allegati (se presenti);
   e) l'oggetto del documento;
   f) se trattasi di documento informatico, la firma elettronica qualificata da parte del RPA e/o del responsabile del provvedimento finale;
   g) se trattasi di documento cartaceo, la sigla autografa da parte del RPA e/o del responsabile del provvedimento finale.

### Art. 10
### Formato dei documenti informatici

I documenti informatici prodotti dall'Amministrazione - quali rappresentazioni informatiche di atti, fatti o dati giuridicamente rilevanti ai sensi dell'art. 1, lett. p, del CAD – indipendentemente dal software utilizzato, prima della loro sottoscrizione con firma elettronica/digitale sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di conservazione.

In particolare, il formato PDF-A è previsto dalla normativa vigente in materia di conservazione, al fine di garantire la loro non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

1. I documenti ricevuti in un formato diverso da quelli prescritti dal presente manuale, se sottoscritti con firma digitale sono recepiti dal sistema e mantenuti e archiviati nel loro formato originale.
2. In riferimento anche ai documenti del servizio di conservazione sostitutiva si evidenzia che ai fini dell'invio in conservazione a norma, sarà privilegiato, ove possibile, l'utilizzo del formato PDF/A.

3. In base all'articolo 21, comma 2, del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - CAD), confermato dalle regole tecniche di cui al DPCM 22 febbraio 2013, il documento informatico non deve contenere macroistruzioni o codici eseguibili.
4. Di seguito vengono elencate le tipologie di formati idonei alla conservazione, l'Ente forma i propri documenti informatici utilizzando i formati di seguito elencati o, per singola classe documentale, adottandone un sottoinsieme:

| Estensione | Tipo/Sottotipo MIME | Descrizione |
|---|---|---|
| **PDF** | application/pdf | file documento pdf +<br>formato di sottoscrizione (PAdES) |
| **XML** | application/xml, text/xml | file di testo xml +<br>formato di sottoscrizione (XAdES) |
| **P7M** | application/pkcs7-mime | formato di sottoscrizione (CAdES-BES) |
| **RTF** | application/rtf | file documento rtf |
| **DOCX (OOXML)** | application/vnd.openxmlformats-<br>officedocument.wordprocessingml.document | file documento docx |
| **ODT** | application/vnd.oasis.opendocument.text | file documento odt |
| **XLSX (OOXML)** | application/vnd.openxmlformats-<br>officedocument.spreadsheetml.sheet | file di calcolo xlsx |
| **ODS** | application/vnd.oasis.opendocument.spreadsheet | file di calcolo ods |
| **ODP** | application/vnd.oasis.opendocument.presentation | file presentazione opd |
| **ODG** | application/vnd.oasis.opendocument. graphics | file grafica vettoriale odg |
| **ODB** | application/vnd.oasis.opendocument.base | file database odb |
| **DCM** | application/dicom | file contenitore per documenti sanitari |
| **GIF** | image/gif | file immagine gif |
| **JPG e JPEG** | image/jpeg | file immagine jpg e jpeg |
| **PNG** | image/png | file immagine png |
| **TIF e TIFF** | image/tiff | file immagine tiff |
| **BMP** | image/bmp | file immagine bmp |
| **TXT** | text/plain | file di solo testo non formattato txt |
| **HTML** | text/html | file di testo HTML |
| **EML** | message/rfc822 e message/rfc2822 | file messaggio posta elettronica eml |

| Estensione | Tipo | Descrizione |
|---|---|---|
| **TSR** | TimeStampResponse | marca temporale |
| **TST e TS** | TimeStampToken | marca temporale |
| **TSD** | TimeStampedData | formato contenitore |
| **M7M** | File firmato digitalmente e marcato | formato contenitore |

5. Eventuali altri formati diversi da quelli sopra elencati, o dal sottoinsieme adottato per la singola classe documentale, generano un'anomalia durante la fase di presa in carico e non vengono accettati dal sistema di conservazione a norma senza specifica autorizzazione da parte del Responsabile della Conservazione.
6. Come espressamente previsto dall'art. 4, comma 3, delle regole tecniche di cui al DPCM 22 febbraio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71", i documenti informatici non devono contenere macroistruzioni o codici eseguibili. In ogni caso l'Ente privilegia, ove possibile, l'utilizzo del formato PDF/A.
7. Si ricorda che, per ogni classe documentale, è configurabile un insieme di formati accettati e che il Responsabile della conservazione dell'ENTE, sotto la propria responsabilità, in accordo con REGIONE e INSIEL ha, in casi eccezionali, facoltà di estendere la tipologia di formati accettati motivandone contestualmente le ragioni.
8. La verifica della firma e la successiva estrazione degli oggetti firmati digitalmente può essere effettuata con qualsiasi software in grado di elaborare file firmati in modo conforme alla Deliberazione CNIPA (ora AGID) 21 maggio 2009 n. 45 e s.m.i.

## SEZIONE V

## RICEZIONE DEI DOCUMENTI

### Art. 11
### Ricezione dei documenti su supporto cartaceo

1. I documenti su supporto cartaceo possono pervenire all'Amministrazione attraverso:
   - il servizio postale;
   - la consegna diretta all'ufficio di protocollo;
   - gli apparecchi telefax.

2. I documenti che transitano attraverso il servizio postale vengono ritirati quotidianamente dalle persone autorizzate presso l'ufficio di Protocollo.
3. 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 system), sono trattati come quelli consegnati direttamente all'ufficio di protocollo.

**Art. 12**
**Ricezione dei documenti informatici**

1. La casella di Posta Elettronica Certificata dell'Ente è accessibile solo all'Ufficio Protocollo, che procede alla registrazione di protocollo previa verifica dell'integrità e leggibilità dei documenti stessi.
2. Qualora il messaggio di posta elettronica non sia conforme agli standard indicati dalla normativa vigente, la valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quella di una missiva non sottoscritta e comunque valutabile dal RPA.
3. Le disposizioni di cui al precedente comma 2 si applicano anche a tutte le caselle di posta elettronica non certificata istituite per i vari Servizi/Aree per consentire a tutti i cittadini l'accesso e la comunicazione dall'esterno.
4. Per le caselle di posta elettronica non certificata è a discrezione del Responsabile del Servizio o del dipendente a cui è affidata la gestione della casella di posta elettronica, la trasmissione al protocollo per un'acquisizione formale.
5. Per una migliore efficienza organizzativa, gli uffici sono stati invitati a richiedere la trasmissione della corrispondenza formale direttamente alla casella di Posta Elettronica Certificata dell'Ente.

**Art. 13**
**Rilascio di ricevute attestanti la ricezione di documenti analogici**

1. Qualora un documento cartaceo sia consegnato personalmente dal mittente o da altra persona incaricata e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'ufficio che lo riceve è autorizzato a fotocopiare il documento e ad apporre sulla copia la segnatura del protocollo dell'Amministrazione con la data e l'ora d'arrivo e la sigla dell'operatore.
2. In alternativa, l'ufficio che riceve il documento, se abilitato, esegue la registrazione di protocollo in arrivo e rilascia la fotocopia del documento con gli estremi della segnatura.

**Art. 14**
**Rilascio di ricevute attestanti la ricezione di documenti informatici**

1. 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'Amministrazione.
2. Il sistema di gestione informatica dei documenti, in conformità alle disposizioni contenute nella Circolare AIPA 7 maggio 2001, n° 28 e s.m.i., provvede alla formazione e all'invio ai mittenti dei seguenti messaggi:
   - *messaggio di aggiornamento di conferma*: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza;
   - *messaggio di annullamento di protocollazione*: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
   - *messaggio di conferma di ricezione*: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'Amministrazione in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico;
   - *messaggio di notifica di eccezione*: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto.
3. Riguardo all'invio e ricezione dei documenti informativi inviati tramite il servizio di posta elettronica ordinaria seppur presenti le notifiche di ricezione, si evidenzia che esse non hanno alcun valore legale.

## SEZIONE VI

## REGISTRAZIONE DEI DOCUMENTI

### Art. 15
### Documenti soggetti a registrazione di protocollo

1. Per documento amministrativo si intende ogni rappresentazione, comunque formata (grafica, fotocinematografica, informatica o di qualsiasi altra specie di contenuto), di atti, fatti o cose giuridicamente rilevanti pervenuti a una Pubblica Amministrazione o da questa prodotti.
2. I documenti ricevuti, quelli spediti e quelli prodotti dagli uffici, a eccezione di quelli indicati al successivo articolo, indipendentemente dal supporto sul quale sono formati, sono soggetti a registrazione obbligatoria di protocollo, necessaria per assegnare validità giuridico-probatoria al documento stesso.

### Art. 16
### Documenti non soggetti a registrazione di protocollo

1. Sono esclusi dalla registrazione di protocollo:

- giornali, riviste, libri;
- materiale pubblicitario;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- corrispondenza interna che non ha, in modo diretto o indiretto, contenuto probatorio o comunque rilevanza amministrativa;
- atti preparatori interni;
- documenti interni di preminente carattere informativo;
- bolle di accompagnamento e documenti di trasporto merci;
- buoni d'ordine alle ditte, se predisposti su appositi bollettari;
- certificati relativi a situazioni retributive e contributive del personale dipendente;
- estratti conto bancari;
- avvisi di pagamento e comunicazioni di avvisi bancari;
- convocazioni della Giunta Comunale;
- deliberazioni del Consiglio Comunale, della Giunta Comunale, determinazioni, decreti e ordinanze dei Responsabili di Servizio e sindacali.

### Art. 17
### Registrazione di protocollo dei documenti su supporto cartaceo

1. Per ogni documento su supporto cartaceo, ricevuto o spedito dall'Amministrazione, è effettuata una registrazione di protocollo [cfr. art. 53, comma 1, del testo unico D.P.R. n. 445/2000 e s.m.i.]. Tale registrazione è eseguita in un'unica operazione, senza possibilità per l'operatore di inserire le informazioni in più fasi successive, ai sensi dell'articolo 53, comma 3, del testo unico. Ciascuna registrazione di protocollo contiene dati obbligatori e dati accessori.
2. I dati obbligatori sono [cfr. articolo 53, comma 1, del testo unico]:
   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.

3. Sono accessori gli elementi che assicurano una migliore utilizzazione dei documenti sotto il profilo giuridico, gestionale e archivistico. Essi sono:
   a) data di arrivo;
   b) luogo di provenienza, o di destinazione, del documento;
   c) numero degli allegati;
   d) descrizione sintetica degli allegati;
   e) estremi del provvedimento di differimento dei termini di registrazione;
   f) mezzo di ricezione o, in alternativa, mezzo di spedizione;
   g) unità organizzativa di competenza;
   h) copie per conoscenza;
   i) tipo di documento.

**Art. 18**
**Assegnazione e smistamento di documenti ricevuti in formato cartaceo**

1. Per l'assegnazione e lo smistamento dei documenti ricevuti in forma cartacea, la procedura è la seguente:
   a) La firma per ricevuta dei moduli (ad esempio: ricevute di ritorno per raccomandate, posta celere, corriere) è a cura dell'ufficio Protocollo.
   b) I documenti cartacei ricevuti, dopo le operazioni di registrazione e segnatura di protocollo, prima dell'inoltro all'ufficio competente vengono acquisiti digitalmente, il formato da usare ai fini della conservazione è il .pdf e, ove possibile il formato .pdf/A.
      b.1) L'Ufficio protocollo verifica la leggibilità, l'accessibilità e la qualità del file acquisito e verifica che il file sia associato alla rispettiva registrazione di protocollo.
      b.2) Tutti i tipi di documenti in formato A4, comunque separabili o leggibili dal supporto tecnico vengono digitalizzati con lo scanner. In caso di planimetrie o volumi non separabili si potrà comunque procedere a digitalizzare con lo scanner il frontespizio. La digitalizzazione completa con lo scanner potrà comunque avvenire anche in un secondo tempo rispetto alle procedure di protocollazione.
   c) dopo lo svolgimento delle operazioni di cui al precedente punto b), b.1) e b.2) da parte dell'Ufficio Protocollo, i documenti vengono smistati in cartelle, una per ogni area di competenza.
   d) Il responsabile d'Area in cui sottendono gli uffici UU (l'Ufficio Utente destinatario del documento), provvede alla presa in carico dei documenti e all'eventuale restituzione se non di competenza, con indicazione dell'ufficio destinatario effettivo.

2. La registrazione avviene, in ordine cronologico, in base all'arrivo della corrispondenza; eventuali situazioni di urgenza saranno valutate dal RSP (Responsabile per la tenuta del protocollo informatico) che potrà autorizzare, in via eccezionale, procedure diverse.

**Art. 19**
**Registrazione di protocollo dei documenti informatici**

1. La registrazione di protocollo di un documento informatico è eseguita dopo che l'operatore addetto ne ha verificato l'autenticità, la provenienza e l'integrità. Nel caso di documenti informatici in partenza, questa verifica è estesa alla validità amministrativa della firma [cfr. Circolare AIPA 7 maggio 2001, n° 28 e s.m.i].
2. Per i documenti informatici è prevista la registrazione delle stesse informazioni indicate per quelli su supporto cartaceo, con l'aggiunta, tra i dati obbligatori, dell'impronta del documento informatico, generata con la funzione di HASH SHA-256 e registrata in forma non modificabile [cfr. articolo 53, comma 1, lettera f), del testo unico D.P.R. n. 445/2000 e s.m.i.].

**Art. 20**
**Segnatura di protocollo**

1. L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.
2. La segnatura di protocollo sia per i documenti informatici che per quelli cartacei deve contenere obbligatoriamente, ai sensi della normativa vigente, le seguenti informazioni:
   a) l'indicazione in forma sintetica dell'Amministrazione;
   b) data e numero di protocollo del documento.
3. A integrazione degli elementi obbligatori di cui al precedente comma 2, la segnatura di protocollo può contenere le seguenti informazioni facoltative:
   a) denominazione dell'AOO;
   b) indice di classificazione.
   c) la tipologia di protocollo Arrivo/Partenza

**Art. 21**
**Segnatura di protocollo dei documenti su supporto cartaceo**

1. La segnatura di protocollo di un documento cartaceo è realizzata attraverso l'apposizione su di esso di un segno grafico il quale, di norma, è realizzato con un'etichetta autoadesiva corredata da codice a barre o timbro completo delle informazioni indicate nel precedente art. 20.

**Art. 22**
**Segnatura di protocollo dei documenti informatici**

1. I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche dell'Extensible Markup Language (XML) e compatibile con il Document Type Definition (DTD) reso disponibile dagli Organi competenti [cfr. art. 18, del DPCM 31 ottobre 2000 e Circolare AIPA 7 maggio 2001, n° 28 e s.m.i.].
2. Le informazioni minime incluse nella segnatura sono quelle elencate negli articoli 9 e 19 del DPCM 31 ottobre 2000, e precisamente:
   a) codice identificativo dell'amministrazione;
   b) codice identificativo dell'area organizzativa omogenea;
   c) data di protocollo;
   d) numero progressivo di protocollo.
3. Oltre alle informazioni sopra le informazioni minime previste comprendono:
   a) oggetto;
   b) mittente;
   c) destinatario o destinatari.
4. Nel caso di documenti informatici in partenza, si possono specificare opzionalmente anche le seguenti informazioni [cfr. art. 19, DPCM 31 ottobre 2000]:
   a) indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
   b) indice di classificazione;
   c) identificazione degli allegati;
   d) informazioni sul procedimento e sul trattamento.
5. La struttura ed i contenuti del file di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche di cui alla Circolare AIPA 7 maggio 2001, n° 28 e s.m.i..

**Art. 23**
**Annullamento delle registrazioni di protocollo**

1. Le registrazioni di protocollo possono essere annullate a cura del personale preposto al Servizio Protocollo, previa autorizzazione da parte del Responsabile del servizio protocollo (RSP).

2. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema con un simbolo o una dicitura [cfr. art. 54, del testo unico].
3. L'operazione di modifica o di annullamento di una registrazione di protocollo è eseguita con le modalità di cui all'articolo 8 del DPCM 31 ottobre 2000, e precisamente:
   a) fra le informazioni generate o assegnate automaticamente dal sistema e registrate in forma non modificabile, l'annullamento anche di una sola di esse determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo;
   b) delle altre informazioni, registrate in forma non modificabile, l'annullamento anche di un solo campo, che si rendesse necessario per correggere errori intercorsi in sede di immissione di dati, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica; così analogamente per lo stesso campo, od ogni altro, che dovesse poi risultare errato;
   c) le informazioni originarie, successivamente annullate, vengono memorizzate secondo le modalità specificate nell'art. 54, del Testo unico sulla documentazione amministrativa.

**Art. 24**
**Protocollazione di telefax**

1. Qualora al documento ricevuto mediante telefax faccia seguito l'originale, l'operatore addetto alla registrazione di protocollo deve attribuire all'originale la stessa segnatura del documento ricevuto mediante telefax.
2. Qualora, invece, si riscontri una differenza, anche minima, tra il documento ricevuto mediante telefax e il successivo originale, quest'ultimo deve essere ritenuto un documento diverso e, pertanto, si deve procedere ad una nuova registrazione di protocollo.
3. La segnatura di protocollo deve essere apposta sul documento e non sulla copertina di trasmissione.
4. La copertina del telefax e il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

**Art. 25**
**Protocollazione di corrispondenza digitale già pervenuta cartacea**

1. Qualora il documento ricevuto in formato cartaceo sia seguito da un invio digitale dello stesso, l'operatore addetto alla registrazione di protocollo deve in ogni caso apporre una nuova registrazione di protocollo, concatenandolo al documento precedentemente protocollato.

**Art. 26**
**Corrispondenza relativa alle gare d'appalto**

1. La corrispondenza relativa alla partecipazione alle gare d'appalto o dal cui involucro è possibile evincere che si riferisca alla partecipazione a una gara, non deve essere aperta, ma protocollata con l'apposizione della segnatura e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili e deve essere inviata all'ufficio competente che la custodisce sino all'espletamento della gara stessa.
2. Per motivi organizzativi, tutti gli uffici sono tenuti a informare preventivamente il Servizio Protocollo in merito alla scadenza di concorsi, gare e bandi di ogni genere.
3. Dopo l'apertura delle buste sarà cura dell'ufficio utente che gestisce la gara d'appalto riportare gli estremi di protocollo su tutti i documenti in esse contenuti.
4. Nel caso di procedure di gara avviate con strumenti telematici, i servizi di notifica dovranno essere definiti come previsti dai relativi sistemi.

**Art. 27**
**Documenti anonimi o non firmati**

Le lettere anonime sono registrate all'Ufficio di Protocollo, e inoltrate agli uffici utenti di competenza i quali valutano l'opportunità di dare seguito a queste comunicazioni.

**Art. 28**
**Corrispondenza personale o riservata**

1. La corrispondenza recante la dicitura "RISERVATA" o "PERSONALE" viene consegnata in busta chiusa al destinatario, accompagnata dalla ricevuta di cui al seguente articolo.
2. Il destinatario, se reputa che i documenti ricevuti debbano essere, comunque, protocollati, provvede a trasmetterli all'ufficio protocollo. In tale caso, il documento sarà protocollato con il livello di riservatezza assegnato dal Responsabile del Servizio Protocollo.
3. Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni è disponibile all'interno del sistema di protocollo informatico dell'Ente una specifica funzionalità che consente la gestione di un protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.

**Art. 29**
**Integrazioni documentarie**

1. Gli addetti al ricevimento della corrispondenza e alle registrazioni di protocollo non sono tenuti a verificare la completezza formale e sostanziale della documentazione pervenuta, ma unicamente a verificare la corrispondenza fra gli eventuali allegati dichiarati e gli allegati effettivamente presentati con la pratica.
2. La verifica di cui al comma 1 spetta all'ufficio competente o al RPA che, qualora ritenga necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente con le comunicazioni del caso.

**Art. 30**
**Protocollazione di un numero consistente di documenti**

1. Qualora si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso che in uscita, l'ufficio interessato deve darne comunicazione all'UOP di riferimento con sufficiente anticipo, al fine di concordare tempi e modi di protocollazione e di spedizione.

## SEZIONE VII

## DESCRIZIONE FUNZIONALE E OPERATIVA DEL SISTEMA DI PROTOCOLLO INFORMATICO

**Art. 31**
**Descrizione del sistema di protocollo informatico**

1. La descrizione funzionale e operativa del sistema di protocollo informatico in uso presso l'AOO è contenuta nell'**Allegato B** (Manuale operativo utente del Prodotto Gifra – Gestione Integrata Flussi e Registrazione Atti - a cura dell'Insiel S.p.A.) al presente Manuale di gestione documentale.

**Art. 32**
**Rilascio delle abilitazioni di accesso alle informazioni documentali**

1. Il controllo degli accessi è attuato al fine di garantire l'impiego del sistema informatico di protocollo esclusivamente secondo modalità prestabilite.
2. Gli utenti e gli operatori del servizio di protocollo hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni richieste dall'ufficio di appartenenza e alle rispettive competenze.
3. A ogni operatore di protocollo è assegnata, oltre alla credenziale di accesso al sistema delle procedure in uso presso l'Ente, consistente in "UserID" e "password", una autorizzazione d'accesso, definita "profilo" al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene. Ciò come descritto nell'allegato manuale operativo utente.

**Art. 33**
**Profili di accesso**

1. Sulla base delle richieste avanzate dagli uffici dell'Amministrazione, i diversi livelli di autorizzazione e i conseguenti differenti profili sono assegnati agli utenti dal RSP il quale, inoltre, provvede all'assegnazione di eventuali nuove autorizzazioni, alla revoca o alla modifica di quelle già assegnate.
2. A tal fine sono individuati i seguenti profili di accesso, ove corrispondono altrettanti livelli diversificati di accesso alle funzioni del sistema di protocollo informatico (ad esempio per uno o più Ufficio Utente o accesso ai vari livelli del protocollo riservato):
   a) Amministratore di sistema;
   b) Responsabile di protocollo;
   c) Operatore di protocollo;
   d) Utente di consultazione.

## SEZIONE VIII

## RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, DI ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

**Art. 34**
**Ufficio Protocollo**

1. Nell'ambito dell'Area Affari Generali, il Servizio di Protocollo svolge le funzioni relative alla tenuta e alla gestione del protocollo informatico, dei flussi documentali, ampiamente descritte in tutto il presente Manuale di gestione; esso inoltre:
   a) costituisce il punto centralizzato di ricevimento della corrispondenza indirizzata all'Amministrazione;
   b) costituisce il punto centralizzato di spedizione della corrispondenza in partenza dall'Amministrazione;
   c) cura la tenuta dell'Albo Pretorio per la pubblicazione degli atti registrati di competenza dell'ufficio;
   d) cura lo smistamento agli uffici competenti di destinazione della corrispondenza ricevuta dall'Amministrazione e di quella interna tra gli uffici;
   e) gestisce le caselle di Posta Elettronica Certificata dell'AOO, relativamente alla posta in arrivo e in partenza;
   f) gestisce il ricevimento delle gare;
   g) gestisce la corrispondenza delle persone residenti presso la Casa comunale.

**Art. 35**
**Registro giornaliero di protocollo**

1. La produzione del registro giornaliero di protocollo avviene, quotidianamente, mediante creazione automatica, dell'elenco dei protocolli e delle informazioni ad essi connesse, registrati nell'arco di uno stesso giorno.
2. Il registro giornaliero di protocollo è il registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti.
3. Nel sistema di conservazione sostitutiva è istituita la classe REGPROT, dove in riferimento all'art. 7, comma 5 delle "Regole tecniche sul protocollo informatico", è definito che il registro giornaliero di protocollo deve essere trasmesso al Sistema di Conservazione entro la giornata lavorativa successiva

**Art. 36**
**Registro di emergenza**

1. 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.
2. In condizioni di emergenza si applicano le modalità di registrazione e di recupero dei dati descritte nell'articolo 63 del testo unico, e precisamente:
   - 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, per cause di eccezionale gravità, il Responsabile del Servizio 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.
   - 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 delle 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 provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza

**Art. 37**
**Differimento dei termini di registrazione**

1. Le registrazioni di protocollo dei documenti ricevuti sono effettuate in giornata e comunque non oltre le quarantotto ore dal ricevimento degli atti.
2. Eccezionalmente, il Responsabile del Servizio può differire con apposito provvedimento la registrazione di protocollo dei documenti ricevuti, fissando comunque un limite di tempo e conferendo valore, nel caso di scadenze predeterminate, al timbro datario d'arrivo per quanto riguarda la corrispondenza cartacea ed alla data od orario di ricezione nella casella di posta elettronica certificata quanto alla corrispondenza digitale.

## SEZIONE IX

## REGOLE DI ASSEGNAZIONE E RECAPITO E PRESA IN CARICO DEI DOCUMENTI

### Art. 38
### Il processo di assegnazione dei documenti

1. Con l'assegnazione si procede all'individuazione dell'UU (Ufficio Utente) destinatario del documento, mentre l'attività di smistamento consiste nell'inviare il documento protocollato ed assegnato all'UU medesimo, come meglio specificato negli articoli successivi. Tale assegnazione avviene anche mediante una notifica consistente in un messaggio di posta elettronica all'ufficio che riporta gli estremi della protocollazione.
2. L'assegnazione può essere estesa a tutti i soggetti ritenuti interessati.
3. L'UU, mediante il sistema di protocollo informatico, provvede alla presa in carico dei documenti assegnati o al rinvio alla UOP (Unità Organizzativa di registrazione di Protocollo) degli stessi se non di competenza.
4. Nel caso di assegnazione errata, l'UU che riceve il documento, lo restituisce all'UOP che procede a una nuova assegnazione e a un nuovo smistamento.
5. I termini per la definizione del procedimento amministrativo che, eventualmente, prende avvio dal documento, decorrono, comunque, dalla data di protocollazione.
6. Il sistema di gestione informatica dei documenti memorizza tutti i singoli passaggi conservandone, per ciascuno di essi, l'identificativo dell'operatore, la data e l'ora di esecuzione.
7. La traccia risultante dalle operazioni di cui al comma precedente definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo e i conseguenti riflessi sotto il profilo della responsabilità.

### Art. 39
### Modifica delle assegnazioni

1. Nel caso di un'assegnazione errata, l'ufficio che riceve il documento, se è abilitato all'operazione di smistamento, provvede a modificare i dati nel sistema informatico e a trasmettere l'atto all'unità organizzativa di competenza, altrimenti lo rinvia all'ufficio che glielo ha erroneamente assegnato il quale apporterà le correzioni necessarie.
2. Il sistema di gestione informatica dei documenti tiene traccia di tutti questi passaggi, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

### Art. 40
### Formazione e identificazione dei fascicoli

1. Tutti i documenti registrati nel sistema informatico e classificati, indipendentemente dal supporto sul quale sono formati, devono essere riuniti in fascicoli.
2. La formazione di un nuovo fascicolo avviene con l'operazione di "apertura" che comporta, al minimo, la registrazione delle seguenti informazioni da parte degli Uffici abilitati:
   - indice di classificazione;
   - tipo di procedimento;
   - numero del fascicolo;
   - oggetto del fascicolo;
   - data di apertura;
   - unità organizzativa assegnataria del procedimento.

### Art. 41
### Fascicolazione dei documenti

1. Per ogni procedimento l'Amministrazione raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati. Tutti i documenti prodotti o ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
2. Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento.

3. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sotto fascicolo o inserto, secondo l'ordine cronologico di registrazione.
4. Quando un nuovo documento viene recapitato all'Amministrazione l'ufficio competente stabilisce, anche con l'ausilio delle funzioni di ricerca del sistema di protocollo informatico, se il documento debba essere collegato ad un procedimento in corso, e pertanto debba essere inserito in un fascicolo già esistente, oppure se il documento si riferisce ad un nuovo procedimento per cui è necessario aprire un nuovo fascicolo.
5. Ogni ufficio può creare e gestire fascicoli autonomamente, inserendo al proprio interno tutti i documenti che ritiene necessari.
6. Un documento può stare all'interno di più fascicoli diversi.
7. Il portale del servizio SUAP (Sportello Unico Attività Produttive) e il portale del servizio SUE (Sportello Unico Edilizia) sono interconnessi e integrati con la PEC e il servizio di protocollo generale dell'Ente. Oltre all'assegnazione univoca della registrazione e segnatura di protocollo i sistemi propongono la medesima fascicolazione dei documenti, consultabile sia dai portali menzionati e sia dall'applicativo di protocollo in uso.

**Art. 42**
**Spedizione dei documenti su supporto cartaceo**

1. I documenti da spedire su supporto cartaceo sono trasmessi agli uffici abilitati all'operazione di spedizione dopo che sono state eseguite le operazioni di registrazione di protocollo, segnatura di protocollo, classificazione, scansione e fascicolazione.
2. 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, la relativa modulistica viene compilata a cura dell'Ufficio Utente che produce il documento.

**Art. 43**
**Spedizione dei documenti informatici**

1. Lo scambio dei documenti soggetti alla registrazione di protocollo è effettuato mediante messaggi 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 e integrazioni [cfr. art. 15, comma 1, del DPCM 31 ottobre 2000].
2. Le modalità di composizione e scambio dei messaggi, il formato della codifica, le misure di sicurezza, sono conformi alle disposizioni contenute nella Circolare AIPA 7 maggio 2001, n° 28 e successive modifiche e integrazioni.
3. I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.
4. Per la spedizione dei documenti informatici, l'Amministrazione si avvale di un servizio di "posta elettronica certificata" offerto da un soggetto in grado di assicurare la riservatezza e la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti, facendo ricorso al "time stamping" e al rilascio di ricevute elettroniche.
5. L'operazione di spedizione di un documento informatico è eseguita dopo che sono state completate le operazioni di verifica della validità amministrativa della firma, registrazione di protocollo, segnatura di protocollo, classificazione e fascicolazione.

**Art. 44**
**Documenti soggetti a scansione e uffici abilitati**

1. I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura protocollo, sono acquisiti mediante il processo di scansione.
2. Il processo di scansione si articola nelle seguenti fasi:
   - acquisizione 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, accessibilità e qualità delle scansioni acquisite;
   - collegamento delle scansioni alle rispettive registrazioni di protocollo, in modo non modificabile.

## SEZIONE X

## ARCHIVIAZIONE DEI DOCUMENTI CARTACEI

**Art. 45**
**Archivio corrente**

1. L'Archivio corrente è costituito dalla documentazione relativa all'attività corrente e alla trattazione degli affari in corso. Tale materiale è conservato presso gli Uffici Utente nella cui competenza rientra la gestione di ogni singolo affare.
2. All'inizio di ogni anno ciascun Ufficio Utente procede alla sistemazione dei fascicoli conclusisi nell'anno precedente. Tale operazione prevede una preliminare operazione di controllo ed eliminazione delle carte ininfluenti per la conservazione, quali appunti manuali e copie di atti già presenti in originale. I documenti residui devono essere riordinati e raccolti in fascicoli, contenenti sul dorso l'oggetto sintetico della pratica, l'ufficio di competenza, l'anno di riferimento.
3. La trasmissione dei fascicoli all'archivio di deposito dell'Ente avviene con periodicità in relazione alle diverse esigenze di ciascun ufficio. La consultazione dei fascicoli cartacei archiviati si svolge su specifica richiesta da parte del responsabile dell'ufficio utente.

## SEZIONE XI

## ARCHIVIAZIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

**Art. 46**
**Archiviazione dei documenti**

1. I documenti informatici di particolari dimensioni, se non acquisibili tramite i sistemi di protocollo, sono archiviati su supporti ottici di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.
2. Le rappresentazioni digitali dei documenti cartacei, acquisite con l'ausilio di scanner, sono archiviate su supporti ottici di memorizzazione, in modo non modificabile, dopo le operazioni di registrazione e segnatura di protocollo e al termine del processo di scansione.
3. Detti documenti possono essere altresì riversati e archiviati nel sistema informatico dell'Ente nelle cartelle di competenza di ciascun ufficio.

**Art. 47**
**Conservazione digitale**

1. La conservazione dei documenti archiviati in formato digitale avviene con le tecnologie e le procedure di cui alla Deliberazione AIPA 13 dicembre 2001, n. 42. e s.m.i..
2. Le informazioni relative alla gestione informatica dei documenti costituiscono parte integrante del sistema di indicizzazione ed organizzazione dei documenti che sono oggetto delle procedure di conservazione sostitutiva [cfr. art. 62, comma 4, del testo unico].
3. Gli standard di riferimento per la conservazione sostitutiva sono quelli elencati nell'allegato 2 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1º ottobre 2014 e sono:
   a) ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
   b) ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

c) ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
d) ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
e) UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
f) ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

**Art. 48**
**Ruoli e responsabilità della conservazione**

1. Le informazioni sulle funzioni e le competenze del Responsabile della Conservazione sostitutiva sono illustrate principalmente nell'articolo 5 della Delibera CNIPA 11/2004, espressamente richiamato dall'articolo 3, comma 2, del DM 23/01/2004. Secondo tale fonte, il Responsabile della Conservazione:
   - definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza;
   - organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
   - archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente a ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
     - descrizione del contenuto dell'insieme dei documenti;
     - estremi identificativi del Responsabile della Conservazione;
     - estremi identificativi delle persone eventualmente delegate dal Responsabile della Conservazione, con l'indicazione dei compiti alle stesse assegnati;
     - indicazione delle copie di sicurezza.
   - mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
   - verifica la corretta funzionalità del sistema e dei programmi in gestione;
   - adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
   - richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
   - definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
   - verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.
2. Le funzioni del Responsabile della Conservazione richiedono quindi competenze trasversali, di natura giuridica, fiscale, organizzativa e tecnico-informatica. In estrema sintesi, per adempiere correttamente ai propri compiti egli dovrà:
   - implementare e mantenere un idoneo sistema hardware e software, curandone i necessari aggiornamenti e adeguamenti tecnologici;
   - definire il sistema di conservazione, ovvero le procedure informatiche ed organizzative in grado di gestire, in piena conformità con la normativa fiscale e tecnica in vigore, il processo di Conservazione Sostitutiva;
   - verificare costantemente il corretto funzionamento tecnico dei processi di conservazione;
   - verificare nel tempo disponibilità e accessibilità dei programmi di conservazione dei supporti di memorizzazione, nonché la leggibilità dei documenti conservati;
   - definire e implementare le procedure organizzative e informatiche atte a esibire, a fronte di richieste delle autorità fiscali, la documentazione conservata.

**Art. 49**
**Servizio archiviazione e di conservazione sostitutiva**

1. Il Servizio di archiviazione elettronica dei documenti è svolto dal "Servizio Informatico", dell'Amministrazione che cura la gestione dei server in cui sono memorizzati i dati dell'Ente, che dal 2020 sono presenti sui server di Insiel a seguito dell'adesione del servizio regionale di dominio Comuni FVG.
2. Il Sistema informatico per l'archiviazione dei dati, garantisce che le informazioni in esso memorizzate siano sempre consultabili ed estraibili.
3. Il servizio della conservazione sostitutiva dei dati, erogato tramite apposita convenzione dalla Regione FVG per il tramite di Insiel, garantisce che le informazioni in esso memorizzate siano sempre consultabili ed estraibili. È nominato un responsabile per la conservazione che sovrintende al processo di conservazione dei documenti informatici, secondo quanto previsto dalla normativa vigente.
4. Il Servizio della conservazione sostituiva dei documenti è supportato dal "Servizio Informatico" dell'Amministrazione e definito con il RSP dell'Amministrazione (Responsabile per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi).
5. Il gestore del servizio è Insiel, tratta il servizio di conservazione offerto in convenzione dalla Regione FVG, attualmente per le seguenti classi documentali:
   - Atti deliberativi: classe documentale "ADWEB";
   - Contratti: classe documentale "CONTRATTO";
   - Registro giornaliero di protocollo: classe documentale "REGPROT";
   - Corrispondenza elettronica: classe documentale "COREL";
   - Famiglia di classi documentali "FATTURAZIONE ELETTRONICA", che comprende:
     - Fatturazione elettronica: classe documentale "FLUSSO_FATTURE"
     - Fatturazione elettronica: classe documentale "FATTURA"
6. Per informazioni dettagliate sulle modalità di erogazione del servizio si rimanda alla seguente documentazione in allegato.
   - Manuale di conservazione sostitutiva **Allegato C;**
   - Classi documentali **Allegato C1;**
   - Compiti dell'outsourcer e descrizione del processo **Allegato D.**

## SEZIONE XII

## SICUREZZA E POLITICHE D'USO DEI SISTEMI INFORMATICI

**Art. 50**
**Piano per la sicurezza**

1. Il Piano per la sicurezza informatica, ai sensi della normativa che ne prevedeva l'attuazione, attualmente si integra e attua nel rispetto delle Misure minime di sicurezza ICT per le pubbliche amministrazioni (AgID) adottate dall'Amministrazione e dall'ente gestore del servizio in outsourcing di conservazione sostitutiva.
2. A ciò si integrano le misure minime di sicurezza ancora vigenti previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e del più recente Regolamento UE GDPR n. 679 del 2016 " Regolamento generale per la protezione dei dati personali"; come normativa europea in materia di protezione dei dati.

**Art. 51**
**Politiche e attività di sicurezza**

**A - Politiche d'uso del sistema informativo**

1. Sono gestiti dall'Amministrazione i sistemi di accesso a Internet, l'Intranet, la Extranet e i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete dati, il software applicativo, i

sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, eccetera. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima. L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione e il supporto di tutto il personale (impiegati funzionari e responsabili) dell'Amministrazione e i loro interlocutori che operano con l'informazione del sistema informatico. É responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste politiche e comportarsi in accordo con le medesime.

2. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione. Le regole sono illustrate per proteggere gli utenti e l'Amministrazione. L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di infezioni da virus informatici, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.
3. Queste politiche si applicano a tutti gli utenti dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ecc…) e agli utenti delle aziende outsourcer includendo tutto il personale affiliato con terze parti.
4. Gli utenti del sistema informativo devono essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima. Gli utenti sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi generati e conservati. Le singole aree o settori sono responsabili delle personalizzazioni e richieste inerenti all'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli utenti seguono le politiche generali dell'Amministrazione e in caso di incertezza, devono consultare il loro responsabile. Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma Amministratori di rete e/o Amministratori di sistema) possono monitorare gli apparati, i sistemi e il traffico di rete dati.
5. Il personale dell'Amministrazione deve porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle stesse. Gli utenti sono tenuti a mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati a utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali (UserID e password). Le password devono essere cambiate con il primo accesso al sistema informativo nei sistemi che lo consentono e successivamente, con frequenza periodica in relazione alla tipologia dei dati trattati. Coloro che trattano dati personali, sensibili o giudiziari il periodo di cambio della password personale si riduce a tre mesi rispetto a sei mesi standard. I periodi indicati inerenti al cambio della password personale sono dettati dalla normativa vigente, pertanto nel caso di aggiornamenti in tale contesto, l'Amministrazione sarà tenuta al rispetto e adeguamento. Tutte le postazioni di lavoro (PC da scrivania e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate, per brevi periodi, dai titolari attraverso l'attivazione automatica del salva schermo protetto da password o tramite la messa in stand-by. Poiché le informazioni archiviate nei PC portatili e sui supporti removibili sono particolarmente vulnerabili, su essi dovrebbero essere esercitate particolari attenzioni (ad esempio crittografando i dati sensibili).
   Tutti i PC, i server e i sistemi di elaborazione in genere, che sono connessi in rete interna dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione e aggiornato. Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere minacce informatiche come virus, eccetera.

**B - Politiche inerenti alle minacce informatiche**

1. Le minacce informatiche costituiscono la causa principale di disservizio e di danno alle Amministrazioni. I danni causati all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia. Tali minacce informatiche, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali. Per ogni esigenza, è necessario stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative a Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro tali minacce. Queste politiche riguardano tutte le apparecchiature di rete dati, di sistema e utente (PC) connesse alle reti informatiche.

Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di corretta gestione e utilizzo delle risorse e servizi ICT descritte. Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione o servizio validato. Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione. Si ricorda di non aprire mai file o macro ricevuti con messaggi da mittente sconosciuto, sospetto, ovvero palesemente non di fiducia, e cancellare immediatamente tali oggetti sia dalla posta che dal cestino. Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati. Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi. Non scaricare mai messaggi da siti o sorgenti sospette. Evitare lo scambio diretto e il riuso di supporti rimovibili (CD, DVD, pen drive, schede di memoria, ecc…) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'Amministrazione e, anche in questo caso, verificare prima la bontà del supporto e relativi file con un antivirus.

2. Tutti gli incaricati al trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione. Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati. Il software acquisito deve essere sempre controllato e verificato perché sia di uso sicuro prima che sia installato. È proibito l'uso di qualsiasi software diverso da quello fornito e validato dall'Amministrazione.

**C - Politiche per le azioni consuntive**

1. Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione e diffusione da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza o suo delegato e contestualmente al responsabile dei Sistemi Informativi, per procedere a:
   - verificare se ci sono altri sistemi infettati con la stessa minaccia informatica;
   - verificare se la minaccia informatica ha diffuso dati;
   - identificare la minaccia informatica;
   - attivare le misure adatte a eliminare la minaccia informatica rilevata e bonificare il sistema infetto;
   - installare l'antivirus e servizi di sicurezza adatti su tutti gli altri sistemi che ne sono sprovvisti;
   - diffondere la notizia dell'evento, all'interno dell'Amministrazione e nelle ulteriori modalità definite dalla normativa vigente.

**D - Politiche d'uso non accettabile**

1. Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse a eccezione degli amministratori di sistema o di rete). In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione. L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.
   Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:
   - Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi.
   - Copie non autorizzate di materiale protetto da copyright (diritto d'autore).
   - L'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali e internazionali.
   - Introduzione di programmi non autorizzati nella rete o nei sistemi dell'Amministrazione.
   - Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da remoto.
   - Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale non inerente all'attività d'ufficio o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.
   - Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
   - Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.

- Realizzare brecce nelle difese periferiche della rete dati del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:
  - accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione;
  - attività e tecniche di intercettazione, sniffing attivo e passivo;
- Eseguire qualsiasi forma di monitor di rete per leggere i dati in transito.
- Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
- Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
- Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di utenti a terze parti esterne all'Amministrazione.

**E - Attività di messaggistica e comunicazione**

1. Le attività seguenti sono rigorosamente proibite senza nessuna eccezione:
   - Inviare messaggi di posta elettronica non inerenti all'attività d'ufficio, o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
   - Ogni forma di molestia via e-mail o telefonica o con altri mezzi.
   - Invio di messaggi non legati alle attività d'ufficio a un grande numero di destinatari/utenti di news group (news group spam).

## Art. 52
## NORME TRANSITORIE E FINALI

1. Dalla data di entrata in vigore del presente documento si intendono abrogate e comunque da disapplicare le eventuali norme comunali in materia non compatibili con la presente disciplina.
2. Per quanto non espressamente previsto dal presente documento si rinvia alle disposizioni legislative in materia, anche sopravvenute, se ed in quanto applicabili.

## GLOSSARIO

**AMMINISTRAZIONI PUBBLICHE**
Quelle indicate nell'art. 1, comma 2 del D. Lgs. 30 marzo 2001, n. 165;

**ARCHIVIO**
L'archivio è la raccolta ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione sono collegati tra loro in un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono. Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, esso viene diviso in tre sezioni: corrente, di deposito e storico;

**ARCHIVIO CORRENTE**
È costituito dal complesso dei documenti relativi ad affari e procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale;

**ARCHIVIO DI DEPOSITO**
È costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico;

**ARCHIVIO STORICO**
È costituito da complessi di documenti relativi ad affari e procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa effettuazione delle operazioni di scarto, alla conservazione perenne;

**ARCHIVIAZIONE ELETTRONICA**
Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione (art. 1 della Deliberazione CNIPA 19 febbraio 2004, n. 11);

**ASSEGNAZIONE**
L'operazione dell'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;

**BANCA DI DATI**
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (art. 4, comma 1, lett. o) del D. Lgs. n. 196/2003);

**BLOCCO**
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento; (art. 4, comma 1, lett. d) del D. Lgs. n. 196/2003);

**CERTIFICATO**
Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche (art. 1, comma 1, lett. f) del D.P.R. n. 445/2000);

**CERTIFICATORE**
Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art. 1, comma 1, lett. g) del D. Lgs. n. 82/2005);

**CLASSIFICAZIONE**
L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;

**COMUNICAZIONE**
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4, comma 1, lett. l) del D. Lgs. n. 196/2003);

**CONSERVAZIONE SOSTITUTIVA**
Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004, n. 11;

**CREDENZIALI DI AUTENTICAZIONE**
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (art. 4, comma 3, lett. d) del D. Lgs. n. 196/2003);

**DATI GIUDIZIARI**
I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u), del D.P.R. 13 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4, comma 1, lett. e) del D. Lgs. n. 196/2003);

**DATI IDENTIFICATIVI**
I dati personali che permettono l'identificazione diretta dell'interessato (art. 4, comma 1, lett. c) del D. Lgs. n. 196/2003);

**DATI SENSIBILI**
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4, comma 1, lett. ddd) del D. Lgs. n. 196/2003);

**DATO ANONIMO**
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (art. 4, comma 1, lett. n) del D. Lgs. n. 196/2003);

**DATO PERSONALE**
Qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4, comma 1, lett. b) del D. Lgs. n. 196/2003);

**DATO PUBBLICO**
Il dato conoscibile da chiunque (art. 1, comma 1, lett. n. del D.Lgs. n. 82/2005);

**DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA'**
Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti che siano a diretta conoscenza di questi , resa nelle forme previste dall'art. 1, comma 1 lett. h) del D.P.R. 28 dicembre 2000, n. 445;

**DICHIARAZIONE SOSTITUTIVA DI DICHIARAZIONE**
Il documento sottoscritto dall'interessato, prodotto in sostituzione del certificato (art. 1, comma 1, lett. g) del D.P.R. n. 445/2000);

**DIFFUSIONE**
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (art. 4 del D. Lgs. n. 196/2003);

**DOCUMENTO**
Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica (art. 1, comma 1, lett. a) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

**DOCUMENTO AMMINISTRATIVO**
Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa (art. 1, comma 1, lett. a) del D.P.R. n. 445/2000);

**DOCUMENTO ANALOGICO**
Documento formato utilizzato una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art. 1, comma 1, lett. b) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

**DOCUMENTO ANALOGICO ORIGINALE**
Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1 della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

**DOCUMENTO ARCHIVIATO**
Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (art. 1, comma 1, lett. h) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);

**DOCUMENTO CONSERVATO**
Documento sottoposto al processo di conservazione;

**DOCUMENTO INFORMATICO**
Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; (art. 1, D.Lgs. 82/2005 CAD);
**DOCUMENTO DI RICONOSCIMENTO**
Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consentano l'identificazione personale del titolare (art. 1, comma 1, lett. c) del D.P.R. n. 445/2000);
**DOCUMENTO D'IDENTITA'**
La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare (art. 1, comma 1, lett. d) del D.P.R. n. 445/2000);
**DOCUMENTO D'IDENTITA' ELETTRONICO**
Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno d'età (art. 1, comma 1, lett. e) del D.P.R. n. 445/2000);
**ESIBIZIONE**
Operazione che consente di visualizzare un documento conservato e di ottenerne copia (art. 1, comma 1, lett. n) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
**EVIDENZA INFORMATICA**
Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1, comma 1, lett. f) del D.P.C.M. 13 gennaio 2004);
**FASCICOLAZIONE**
L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;
**FASCICOLO**
Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se non è infrequente la creazione di fascicoli formati da insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc);
**FIRMA DIGITALE**
Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1, comma 1, lett. s) del D. Lgs. n. 82/2005);
**FIRMA ELETTRONICA**
L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica (art. 1, comma 1, lett. q) del D. Lgs. n. 82/2005);
**FIRMA ELETTRONICA QUALIFICATA**
La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma quale l'apparato strumentale usato per la creazione della firma elettronica (art. 1, comma 1, lett. r) del D. Lgs. n. 82/2005);
**FORMAZIONE DEI DOCUMENTI INFORMATICI**
Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa (art. 1 della Deliberazione AIPA del 23 novembre 2000, n. 51);
**FUNZIONE DI HASH**
Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit) una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali (art. 1, comma 1, lett. e) del D.P.C.M. 13 gennaio 2004);

**GARANTE (della Privacy)**
L'autorità di cui all'articolo 153 del D. Lgs. 30 giugno 2003, n. 196, istituita dalla legge 31 dicembre 1996, n. 675 (art. 4, comma 1, lett. q) del D. Lgs. n. 196/2003);
**GESTIONE INFORMATICA DEI DOCUMENTI**
L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici (art. 1, comma 1, lett. l) del D. Lgs. n. 82/2005);
**INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI**
Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
**LEGALIZZAZIONE DI FIRMA**
L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa (art. 1, comma 1, lett. l) del D.P.R. n. 445/2000); 32
**LEGALIZZAZIONE DI FOTOGRAFIA**
L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato (art. 1, comma 1, lett. n) del D.P.R. n.445/2000);
**MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE**
Il massimario di selezione e scarto è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sottoripartizioni del titolario e indica quali documenti debbano essere conservati permanentemente (e quindi versati dopo quaranta anni nella sezione storica dell'archivio) e quali, invece, possono essere destinati al macero dopo cinque, dieci, quindici, venti anni, ecc. o secondo le esigenze dell'Amministrazione. Ne consegue il Piano di Conservazione periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
**MEMORIZZAZIONE**
Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del D.P.R. n. 445/2000 così come modificato dall'articolo 6 del D. Lgs. 23 gennaio 2002, n. 10 (art. 1 comma 1, lett. f) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
**MISURE MINIME DI SICUREZZA**
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del D. Lgs. 30 giugno 2003, n. 196 (art. 4, comma 3, lett. a) del D. Lgs. n. 196/2003), oltre alle MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015).
**PAROLA CHIAVE**
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri e altri dati in forma elettronica (art. 4, comma 3, lett. e) del D. Lgs. n. 196/2003);
**ORIGINALI NON UNICI**
I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi (art. 1, comma 1, lett. v) del D. Lgs. n. 82/2005);
**PROFILO DI AUTORIZZAZIONE**
L'insieme delle informazioni, univocamente associate ad una persona che consente di individuare a quali dati essa può accedere, nonché i trattamenti ed essa consentiti (art. 4, comma 3, lett. f) del D. Lgs. n. 196/2003);
**PUBBLICO UFFICIALE**
Il notaio, salvo quanto previsto dall'art. 5 , comma 4, della presente deliberazione e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del D.P.R. n. 445/2000 (art. 1, lett. q) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
**RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI**
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali (art. 4, comma 1, lett. g) del D. Lgs. n. 196/2003);
**RIFERIMENTO TEMPORALE**
Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, comma 1, lett. g) del D.P.C.M. 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (art. 1, comma 1, lett. i) del D.P.R. n. 68/2005);

**RIVERSAMENTO DIRETTO**
Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (art. 1. comma 1, lett. n) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
**RIVERSAMENTO SOSTITUTIVO**
Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica (art. 1, comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11);
**SEGNATURA INFORMATICA**
L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML, ed incluse in un messaggio protocollato, come previsto dall'art. 18, comma 1 del D.P.C.M. 31 ottobre 2000 (art. 1 dell'allegato A della Circolare AIPA del 7 maggio 2001, n. 28);
**SEGNATURA DI PROTOCOLLO**
L'apposizione o l'associazione all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso (Glossario dell'IPA – Indice delle Pubbliche Amministrazioni);
**SISTEMA DI CLASSIFICAZIONE**
Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata (art. 2, comma 1, lett. h) del D.P.C.M. 31 ottobre 2000);
**SISTEMA DI AUTORIZZAZIONE**
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente (art. 4, comma 3, lett. g) del D. Lgs. n. 196/2003);
**SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI**
L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti (art. 1, comma 1, lett. r) del D.P.R. n. 445/2000).

## RIFERIMENTI NORMATIVI

**Legge 7 agosto 1990 n° 241**
Nuove norme in materia di procedimenti amministrativi e di diritto di accesso ai documenti amministrativi

**Decreto del Presidente della Repubblica 20 ottobre 1998 n° 428**
Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche

**Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000**
Regole tecniche per il Protocollo Informatico

**Decreto del Presidente della Repubblica 28 dicembre 2000 n° 445**
Testo unico sulla documentazione amministrativa

**Decreto Presidente della Repubblica 7 aprile 2003 n° 137**
Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del Decreto Legislativo 23 gennaio 2002 n° 10

**Decreto Legislativo 30 giugno 2003 n° 196**
Codice in materia di protezione dei dati personali

**Decreto del Presidente del Consiglio dei Ministri 14 ottobre 2003**
Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi

**Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013**
Regole tecniche per il protocollo informatico ai sensi degli articoli 40 *-bis* , 41, 47, 57 *-bis* e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

**Decreto Legislativo 7 marzo 2005, n. 82**
Codice Amministrazione Digitale

**Decreto Legislativo 26 agosto 2016, n. 179**
Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche. (16G00192) (GU Serie Generale n.214 del 13-9-2016)

**Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni – AgID**
Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015

**Regolamento UE GDPR n. 679 del 2016**
Regolamento UE generale per la protezione dei dati personali