



**COMUNE DI CASALGRANDE**

**MANUALE DI GESTIONE DOCUMENTALE E**  
**CONSERVAZIONE**

## **INDICE**

### **PARTE I** **DISPOSIZIONI GENERALI E ORGANIZZAZIONE**

- Art. 1 Definizioni
- Art. 2 Ambito di applicazione
- Art. 3 Aree Organizzative Omogenee
- Art. 4 Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi
- Art. 5 Responsabile della gestione documentale

### **PARTE II** **FORMAZIONE DEI DOCUMENTI**

- Art. 6 Modalità di formazione del documento informatico
- Art. 7 Redazione/formazione del documento amministrativo informatico
- Art. 8 Il documento amministrativo informatico costituito dal corpo della PEC istituzionale
- Art. 9. Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale
- Art. 10. Validazione temporale
- Art. 11 Formato dei documenti e firme digitali
- Art. 12. Redazione/formazione del documento amministrativo analogico
- Art. 13 Segnatura di protocollo
- Art. 14 Sigillo elettronico qualificato

### **PARTE III** **INVIO E RICEZIONE DEI DOCUMENTI**

- Art. 15 Invio e ricezione dei documenti
- Art. 16 Invio dei documenti amministrativi informatici
- Art. 17 Duplicato del documento informatico e analogico
- Art. 18 Copia per immagine su supporto informatico di documenti informatici e analogici
- Art. 19 Estratto informatico di documento amministrativo informatico
- Art. 20 Copia analogica di documento amministrativo informatico
- Art. 21 Ricezione della corrispondenza su supporto analogico
- Art. 22 Apertura della corrispondenza analogica in entrata
- Art. 23 Copie per immagine su supporto informatico di documenti analogici in entrata
- Art. 24 Validità dei documenti informatici in entrata
- Art. 25 - Documenti trasmessi tra pubbliche amministrazioni
- Art. 26 Rilascio di ricevute attestanti la consegna dei documenti

### **PARTE III** **REGISTRAZIONE DEI DOCUMENTI**

- Art. 27 Il protocollo informatico: requisiti tecnologici e funzionalità

- Art. 28 Registrazione di protocollo
- Art. 29 Documenti soggetti a registrazione obbligatoria di protocollo
- Art. 30 Interoperabilità e cooperazione applicativa
- Art. 31 Il registro giornaliero di protocollo
- Art. 32 Annullamento o modifica delle registrazioni di protocollo
- Art. 33 Riservatezza delle registrazioni di protocollo
- Art. 34 Registro di emergenza

#### **PARTE IV**

#### **FLUSSI DI LAVORAZIONE DEI DOCUMENTI**

- Art. 35 Consegna dei documenti
- Art. 36 Smistamento ed assegnazione dei documenti
- Art. 37 Presa in carico dei documenti
- Art. 38 Classificazione dei documenti
- Art. 39 Fascicolazione dei documenti e tipologie di fascicoli
- Art. 40 Formazione, implementazione, gestione ed elenco minimo di metadati descrittivi
- Art. 41 Fascicoli ibridi o misti
- Art. 42 Tenuta degli archivi correnti, dei fascicoli e delle serie documentarie

#### **PARTE V**

#### **SICUREZZA DEI SISTEMI E DEI DOCUMENTI INFORMATICI**

- Art. 43 Misure di sicurezza nella formazione e gestione dei documenti
- Art. 44 Misure tecniche di sicurezza informatica dei sistemi
- Art. 45 Misure di sicurezza del sistema informativo integrato di gestione documentale
- Art. 46 Misure di sicurezza del sistema informativo integrato di gestione documentale
- Art. 47 Misure di sicurezza informatica di carattere organizzativo-gestione dei profili abilitativi

#### **PARTE VI**

#### **GESTIONE DELL'ARCHIVIO DI DEPOSITO**

- Art. 48 Archivio di deposito
- Art. 49 Trasferimento dei documenti all'Archivio di deposito (fascicoli analogici o ibridi)
- Art. 50. Sistema di conservazione dei documenti informatici
- Art. 51. Responsabile della conservazione
- Art. 52. Oggetti della conservazione
- Art. 53. Formati ammessi per la conservazione
- Art. 54 Modalità e tempi di trasmissione dei pacchetti di versamento
- Art. 56 Accesso al Sistema di conservazione
- Art. 57. Selezione e scarto dei documenti
- Art. 58. Misure di sicurezza e monitoraggio dei documenti digitali

Appendice A: glossario DPCM 3 dicembre 2013

Allegato 1 Aree Organizzative Omogenee

Allegato 2 – Nomina del Responsabile della Gestione documentale

Allegato 3 – Abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica dei

documenti

Allegato 4 – Titolario di classificazione

Allegato 5 - Funzionalità del sistema di gestione informatica dei documenti

Allegato 6 – Manuale di conservazione

Allegato 7 – Contratto di servizio per la conservazione digitale

Allegato 8 – Registro di emergenza

## **PARTE I DISPOSIZIONI GENERALI E ORGANIZZAZIONE**

### **Art. 1 Definizioni**

Ai fini del presente manuale si applicano le definizioni contenute nelle Linee Guida AGID sulla formazione, gestione e conservazione dei documenti informatici in vigore dal 1° gennaio 2022.

Ulteriori norme rilevanti ai fini della gestione documentale sono:

1. le disposizioni in materia di formazione dei documenti informatici, anche di natura amministrativa, e di digitalizzazione dell'attività amministrativa di cui al d.lgs. 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale*" (di seguito anche solo "CAD");
2. le disposizioni in materia di documentazione amministrativa di cui al D.P.R. 28 dicembre 2000, n. 445 "*Disposizioni legislative in materia di documentazione amministrativa*" (di seguito anche solo "TUDA");
3. le norme sul procedimento amministrativo di cui alla L. 7 agosto 1990, n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";
4. le disposizioni sulla trasparenza di cui al D.Lgs. 14 marzo 2013, n. 33 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
5. le disposizioni in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno di cui al Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio del 24 luglio 2014 (Regolamento "eIDAS");
6. le disposizioni sulla tutela della riservatezza dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "*Regolamento generale sulla protezione dei dati*" ("GDPR") e d.lgs. 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali*".

### **Art. 2 Ambito di applicazione**

Il Manuale è un documento interno di contenuto sia organizzativo che operativo, utile quale strumento di supporto ai processi decisionali e operativi e, pertanto, è destinato alla più ampia diffusione presso tutto il personale dell'ente. Il presente Manuale e i suoi allegati sono approvati con delibera di Giunta su proposta del Responsabile della gestione documentale dell'Ente. L'aggiornamento degli allegati, quando non comporta modifiche sostanziali ai contenuti del presente Manuale, è effettuato con determinazione del Responsabile della gestione documentale.

Con la pubblicazione nella sezione "Amministrazione Trasparente" del sito internet istituzionale (<https://www.comune.casalgrande.re.it/ilcomune/iregolamenti/>) il Manuale è reso noto anche esternamente all'ente. Deve, inoltre, essere capillarmente divulgato alle unità organizzative responsabili (UOR) dell'unica Area Organizzativa omogenea del Comune di Casalgrande (AOO), al

fine di consentire la corretta diffusione delle nozioni e delle procedure documentali. È prevista, infine, un'attività di formazione continua e permanente in materia di gestione documentale per tutte le unità organizzative responsabili del Comune su tutti i punti contenuti in questo manuale di gestione. In quest'ottica, il Manuale costituisce altresì un documento pubblico funzionale al perseguimento del principio di trasparenza dell'azione amministrativa.

### **Art. 3 Aree Organizzative Omogenee**

Per garantire una gestione documentale unitaria e coordinata, l'Amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) individuata con Deliberazione della Giunta Comunale n. 297 del 3/12/2003. Le UOR che afferiscono alla AOO sono definite con riferimento all'organigramma dell'Ente disponibile al link: <https://www.comune.casalgrande.re.it/ilcomune/amministrazionetrasparente>, possono essere oggetto di modifiche e integrazioni per effetto degli interventi sulla struttura organizzativa e sono descritte nell'allegato 1.

1. L'amministrazione è accreditata presso [www.indicepa.gov.it](http://www.indicepa.gov.it) dal 01/06/2010, codice IPA amministrazione c\_b893.
2. All'AOO è stata attribuita una casella di posta elettronica certificata presente sull'IPA e interoperabile con il protocollo informatico: [casalgrande@cert.provincia.re.it](mailto:casalgrande@cert.provincia.re.it), [demografici.casalgrande@cert.provincia.re.it](mailto:demografici.casalgrande@cert.provincia.re.it), e una casella di posta elettronica ordinaria (PEO) [urp@comune.casalgrande.re.it](mailto:urp@comune.casalgrande.re.it).

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

1. Nell'ambito dell'AOO di cui all'articolo 3, è istituito un servizio per la tenuta del protocollo informatico e dell'archivio che coincide con l'Ufficio protocollo e archivio, di seguito denominato Servizio, i cui estremi identificativi sono riportati nell'allegato n. 1. Tale servizio garantisce la corretta gestione, tenuta e tutela dei documenti, vigila sull'osservanza degli adempimenti previsti in ambito archivistico dalla normativa in materia di gestione documentale durante l'intero ciclo di vita dei documenti.
2. Al Responsabile del Servizio sono assegnati i seguenti compiti:
  - garantisce il corretto svolgimento delle attività di gestione dei documenti, nonché la formazione, gestione, conservazione e fruizione dell'archivio;
  - attribuisce il livello di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
  - garantisce che le operazioni di registrazione, segnatura, gestione dei documenti e dei flussi documentali si svolgano nel rispetto della normativa vigente;
  - garantisce la corretta produzione e l'invio in conservazione del registro giornaliero di protocollo;
  - garantisce che le funzionalità del sistema in caso di guasti o anomalie siano ripristinati entro ventiquattrore dal blocco delle attività e, comunque, nel più breve tempo possibile.
  - La notifica ai responsabili delle UOR dell'eventuale indisponibilità del sistema e l'attivazione del registro di emergenza
  - predispone e mantiene aggiornati il titolario di classificazione dei documenti e il piano di conservazione dell'archivio, compresi gli indici e tutti gli altri strumenti archivistici necessari;
  - autorizza le operazioni di annullamento delle registrazioni di protocollo;
  - vigila sull'osservanza delle disposizioni del presente manuale e tiene aggiornati gli allegati

### **Art. 5 Responsabile della gestione documentale**

1. A capo del Servizio è posto il Responsabile della gestione documentale cioè il Responsabile del Servizio protocollo e archivio, il cui nominativo e quello del suo vicario (nei casi di vacanza, assenza o impedimento) sono riportati nell'allegato n. 2.
2. Al Responsabile della gestione documentale sono assegnati i compiti di cui al paragrafo 3.4 delle Linee Guida AGID e art. 60 del TUDA:
  - predisporre e mantenere aggiornato il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici, nel rispetto della normativa in materia di trattamento dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione, e d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali;
  - definire e assicurare criteri uniformi di trattamento dei documenti e di classificazione e archiviazione, nonché di comunicazione interna tra le UOR e verso le AOO di altre amministrazioni;
  - predisporre, di concerto con il responsabile della conservazione, il responsabile dei sistemi informativi e con il responsabile del trattamento dei dati personali, il piano per la sicurezza informatica di continuità operativa, di protezione dei dati personali e di analisi del rischio;
  - sovrintendere e monitorare i processi e le attività che governano le fasi di formazione, gestione e versamento in conservazione dei documenti informatici;
  - formare correttamente la documentazione che andrà a costituire il pacchetto di versamento (PdV) e assicurare la sua trasmissione al sistema di conservazione con i formati concordati con il conservatore e secondo le modalità operative descritte nel manuale di conservazione del sistema di conservazione;
  - verificare l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

Il Responsabile della gestione documentale anche in riferimento alle funzioni proprie del referente dei sistemi informatici e della sicurezza informatica e del referente della protezione dei dati personali relativamente al sistema documentale può, sotto la propria responsabilità, delegare in tutto o in parte i propri compiti al personale posto sotto la propria direzione.

## **PARTE II – FORMAZIONE DEI DOCUMENTI**

### **Art. 6 Modalità di formazione del documento informatico**

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software (ad esempio, mediante programmi di scrittura delle suite *Libre Office*): in tal caso il documento informatico assume le caratteristiche di immutabilità e di integrità mediante la sottoscrizione con firma digitale/firma elettronica qualificata o con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi con PEC con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- acquisizione:
  - di un documento informatico per via telematica o su supporto informatico
  - della copia per immagine su supporto informatico di un documento analogico
  - della copia informatica di un documento analogico: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione (ad esempio, utilizzo di software gestionali verticali)

- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei *log* di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione. (ad esempio, generazione del registro di protocollo giornaliero)

### **Art. 7 Redazione/formazione del documento informatico**

Il documento amministrativo è qualsiasi rappresentazione, comunque formata, del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione.

Gli atti formati con strumenti informatici, nonché i dati e i documenti informatici detenuti dall'AOO, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie. Il documento informatico e le istanze, le dichiarazioni e le comunicazioni previste dalla legge sono soggette a registrazione di protocollo, segnatura, fascicolatura e repertoriazione.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità anche con la registrazione nel registro di protocollo unico per l'Area Organizzativa Omogenea (AOO), nei repertori e negli albi contenuti nel sistema di gestione documentale.

Il documento amministrativo informatico deve, di norma, contenere la denominazione del Comune di Casalgrande e l'indicazione di:

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati (indicare 0 *zero* se non presenti);
- Oggetto;
- Destinatario;
- Testo;
- Iniziali di redattore/responsabile;
- Sottoscrizione;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato. Le informazioni relative alla classificazione atte a identificare il fascicolo di competenza, la data di sottoscrizione, il numero di allegati sono inserite prima della sottoscrizione del documento.

Di norma, la data di sottoscrizione e la data di protocollazione coincidono.

### **Art. 8 Il documento amministrativo informatico costituito dal corpo della PEC istituzionale**

Il documento trasmesso/ricevuto con PEC ha lo stesso valore legale della raccomandata con avviso di ricevimento. In tal caso, l'avvenuta consegna del messaggio elettronico consente tra l'altro di ricorrere contro terzi. Di norma, si dovrebbe usare la PEC per trasmettere e/o ricevere un documento informatico, ma può accadere che la comunicazione/istanza ricevuta sia costituita dal mero corpo della *email*.



In questo caso si procede alla registrazione del messaggio in arrivo nel sistema di gestione documentale solo se il contenuto è rilevante al fine giuridico probatorio.

### **Art. 9 Il documento amministrativo informatico costituito dal corpo della e-mail istituzionale**

L'*email* costituisce un documento informatico sottoscritto con firma elettronica semplice, in quanto il mittente viene identificato inserendo il proprio *username* e la propria *password*.

Le *email* inviate da una casella istituzionale del Comune di Casalgrande sono considerate sottoscritte con firma elettronica semplice e sono soggette a protocollazione solo se il contenuto è rilevante al fine giuridico probatorio. In questo caso si procede alla conversione dell'*email* in formato PDF/A prima di provvedere alla sua registrazione.

### **Art. 10 Validazione temporale**

Costituiscono validazione temporale:

- i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
- i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IT) (INRiM) con una differenza non superiore ad un minuto primo;
- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
- il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata;
- il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica.

### **Art. 11 Formato dei documenti e firme digitali**

- Il formato del documento informatico creato dal Comune di Casalgrande deve essere scelto tra i seguenti **formati standard**: .rtf, .docx, .odt, .pdf, .xlsx, .ods, .xml.
- Eventuali formati differenti possono essere utilizzati in relazione a specifiche e comprovate esigenze. Il formato del documento informatico, in ogni caso, deve essere preferibilmente individuato tra quelli previsti nell'Allegato 2 alle Linee guida dell'AgID ed adottato osservando le raccomandazioni ivi contenute.
- Le versioni del documento precedenti alla versione definitiva (bozze, minute, ecc.), possono essere salvate in un formato che ne consenta la modificabilità (ad esempio, .docx o .odt). La versione definitiva del documento, invece, è sempre preferibile sia in formato PDF.
- I documenti di maggiore rilevanza giuridico-amministrativa (ad esempio, gli atti del Sindaco e degli organi collegiali, i contratti, le determinazioni a contenuto provvedimentale, ecc.), prima della firma, devono essere convertiti in formato PDF/A (PDF non modificabile). I documenti in formato PDF e PDF/A sono sottoscritti con firma PADES.
- Nel caso il documento definitivo sia di un formato diverso dal PDF, la sottoscrizione avviene con firma CADES (.p7m).
- Se il documento è oggetto di conservazione deve essere predisposto il relativo formato PDF/A.

### **Art. 12 Redazione/formazione del documento analogico**



Il documento analogico è un documento formato su supporto analogico prodotto con strumenti analogici (ad es., documento scritto a mano) o con strumenti informatici (ad es., documento prodotto con un sistema di video scrittura) e stampato su carta.

I documenti analogici dotati di firma autografa aventi per destinatario un ente o un soggetto terzo, sono di norma redatti in due esemplari, un originale per il destinatario e una minuta da conservare agli atti nel fascicolo corrispondente.

Il documento amministrativo analogico in uscita è redatto su carta intestata e deve, di norma, contenere la denominazione del Comune di Casalgrande e l'indicazione di

- AOO/ UOR;
- Data di sottoscrizione;
- Classificazione;
- Indicazioni atte a individuare il fascicolo di competenza;
- Numero di allegati;
- Oggetto;
- Destinatario;
- Testo;
- Sottoscrizione;
- Sigla eventuali istruttori;
- Elementi identificativi del responsabile del procedimento.

Il documento è sottoscritto prima di essere protocollato; di norma la data di sottoscrizione e la data di protocollazione coincidono.

Ai sensi del DPCM 21 marzo 2013, per particolari tipologie di documenti analogici originali unici, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato.

Per documenti originali unici si intendono tutti quei documenti il cui contenuto non può essere desunto da altre scritture o documenti di cui sia obbligatoria la tenuta (ad es., i verbali di una commissione consiliare, etc.).

Pertanto, tutti i documenti su cui vengono apposti manualmente dati di registrazione a protocollo, sigle e firma autografa (che non sono sottoscritti con firma elettronica, semplice, avanzata o digitale), sono documenti amministrativi analogici.

### **Art.13 Segnatura di protocollo**

Nell'ambito del sistema di interoperabilità tra enti, la segnatura di protocollo consente l'individuazione in modo inequivocabile di ciascun documento (identificazione univoca e certa).

Nei documenti informatici, la segnatura viene associata in forma permanente e immutabile al documento principale e agli allegati che con esso formano il messaggio di protocollo. La segnatura viene creata e associata in forma automatica al documento, contemporaneamente alla sua protocollazione; in questo modo, le informazioni della segnatura di protocollo vengono memorizzate nel Sistema informativo integrato di gestione documentale.

La segnatura si compone dei seguenti dati:

- indicazione dell'amministrazione mittente (Codice IPA, identificativo del Comune di Casalgrande);

- indicazione della AOO mittente (Codice AOO, identificativo del Comune di Casalgrande nell'Indice dei Domicili digitali);
- indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
- numero progressivo di protocollo (generato automaticamente dal Sistema e registrato in forma non modificabile);
- data di registrazione (come sopra);
- oggetto del messaggio di protocollo;
- classificazione del messaggio di protocollo;
- fascicolo del messaggio di protocollo;
- mittente e destinatario;
- codice dell'unità che ha prodotto il documento;
- codice identificativo dell'unità a cui il documento è assegnato;
- identificazione degli allegati;
- impronta del documento principale e degli eventuali allegati.

Le informazioni della segnatura di protocollo sono parte dei dati di registrazione e sono rese disponibili, per i documenti informatici in uscita, in un file conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente dall'Agenzia per l'Italia digitale.

#### **Articolo 14 - Sigillo elettronico qualificato (documenti in uscita)**

Nell'ambito del sistema di interoperabilità tra enti, per tutti i documenti in uscita, il Sistema produce in automatico il sigillo elettronico qualificato, allo scopo di garantire integrità e autenticità alla segnatura di protocollo. Detto sigillo, equivalente ad una firma elettronica qualificata, afferisce non ad una persona fisica, bensì a una persona giuridica, nella fattispecie, all'Amministrazione Comune di Casalgrande.

Nello specifico, in fase di produzione della segnatura informatica delle registrazioni di protocollo informatico in uscita, con spedizione tramite PEC, il Sistema appone il sigillo elettronico qualificato in maniera trasparente all'utente, in quanto governato da apposito parametro.

L'apposizione del sigillo presuppone che la registrazione di protocollo disponga di un file, inteso come documento principale e dei metadati di classificazione. In assenza di tali requisiti, il sigillo non verrà apposto e, conseguentemente, non sarà possibile l'invio del documento via PEC.

- Nei casi di eventuale malfunzionamento della procedura di apposizione del sigillo elettronico, è prevista la possibilità di gestire manualmente la spedizione via PEC del messaggio senza segnatura.

### **PARTE III**

#### **INVIO E RICEZIONE DEI DOCUMENTI**

##### **Art. 15 Invio e ricezione dei documenti**

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

- documenti in arrivo;
- documenti in partenza;
- documenti interni (scambiati tra UOR).

La comunicazione tra l'Area Organizzativa Omogenea – AOO del Comune di Casalgrande e le AOO appartenenti a differenti PA avviene nel rispetto delle indicazioni fornite dall'allegato 6 delle Linee guida AgID. È cura del Responsabile della gestione documentale valutare periodicamente la congruità dei metadati con le disposizioni normative e, se necessario, adottare le opportune azioni per promuoverne l'adeguamento tecnico funzionale.

La trasmissione di documenti dal Comune alle altre pubbliche amministrazioni avviene mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; in ricezione tali modalità sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

Ai fini della verifica della provenienza le comunicazioni sono valide se soddisfano una delle seguenti condizioni:

- a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- b) sono dotate di segnatura di protocollo;
- c) è possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente;
- d) sono trasmesse attraverso sistemi di posta elettronica certificata.

#### **Art. 16 Invio dei documenti amministrativi informatici**

La spedizione dei documenti amministrativi informatici avviene a cura dell'ufficio competente sul procedimento, al termine delle operazioni di sottoscrizione, registrazione di protocollo, segnatura, classificazione e fascicolazione dei documenti stessi.

La consegna dei documenti verso altre amministrazioni, imprese, ordini professionali, dipendenti o cittadini che hanno fornito il loro domicilio digitale, avviene mediante l'utilizzo della posta elettronica certificata dell'unità organizzativa (Settore-Servizio-Ufficio), titolare del procedimento. Più precisamente, una volta protocollate, le lettere in uscita e i relativi allegati, sono inviati all'indirizzo elettronico dichiarato dal destinatario. Non sono previsti altri utilizzi delle caselle PEC.

Il Sistema garantisce l'archiviazione automatica delle ricevute elettroniche di avvenuta accettazione e consegna telematica del documento inviato, associando le stesse alla relativa registrazione di protocollo. È cura dell'ufficio mittente controllare sulla Scrivania virtuale l'eventuale ritorno di notifiche di mancata consegna dei documenti inviati e, sulla maschera della registrazione di protocollo, le ricevute di consegna e le notifiche di eccezione (rifiuto del documento da parte del destinatario). Se l'indirizzo elettronico del destinatario non è certificato, è attestata solo l'avvenuta spedizione della lettera (Ricevuta di accettazione dell'invio).

L'attestazione di avvenuta spedizione e consegna digitale è disponibile solo registrando singolarmente i destinatari ed il relativo indirizzo digitale. Nel caso di destinatari multipli, il Sistema consente la creazione di specifiche liste di distribuzione, al fine di facilitare la predisposizione dei metadati.

Per i soggetti esclusi da obbligo di domicilio digitale è prevista la spedizione tramite posta tradizionale, raccomandata, o consegna a mano di copia analogica del documento digitale conservato (cioè predisposto e disponibile) presso il Comune di Casalgrande. Dette copie analogiche, tratte dagli originali digitali tramite procedura prevista dal Sistema (funzionalità "Copia conforme"), recanti l'indicazione a mezzo stampa del responsabile pro tempore, in sostituzione della firma autografa hanno la stessa efficacia probatoria dell'originale digitale da cui sono tratte. Sono escluse da questa modalità le certificazioni rilasciate dall'Amministrazione, da utilizzarsi nei rapporti tra privati.

## **Art. 17 Duplicato del documento informatico e analogico**

Il duplicato del documento informatico è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto. I duplicati informatici hanno il medesimo valore giuridico del documento informatico da cui sono tratti se prodotti in conformità delle regole tecniche.

Pertanto, a differenza delle copie di documenti informatici, che si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i duplicati informatici non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza. Il duplicato di un documento analogico è la riproduzione di un documento analogico originale distrutto o smarrito che lo sostituisce a tutti gli effetti legali: ad esempio, il rilascio della carta di identità etc.

## **Art. 18 Copia per immagine su supporto informatico di documenti informatici e analogici**

La copia di documento informatico è un documento informatico che, mediante processi e strumenti idonei, assicura la corrispondenza della copia alle informazioni del documento informatico di origine attraverso l'utilizzo di uno dei formati idonei ai sensi della normativa vigente. La copia di documento informatico è, dunque, un documento informatico che muta il formato del documento originario o che muta il supporto del documento originario informatico (ad es., il salvataggio di un file in un formato differente: da *.doc* a *.pdf*, oppure da *.doc* a *.ods*).

Le copie del documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta, fermo l'obbligo di conservazione dell'originale informatico.

È possibile produrre la copia su supporto informatico di documenti amministrativi in origine su supporto analogico. La copia informatica ha il medesimo valore dell'originale analogico da cui è tratta se attestata conforme dal funzionario a ciò delegato nei modi stabiliti dalla legge. L'attestazione di conformità può essere inserita nel documento informatico contenente la copia informatica o può essere prodotta come documento separato contenente un riferimento temporale e l'impronta di ogni copia.

In entrambi i casi l'attestazione dev'essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l'impronta di ogni copia o estratto informatico oggetto dell'attestazione.

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

Le copie informatiche di documenti analogici, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali hanno la medesima efficacia probatoria degli originali se a esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma digitale o altra firma elettronica qualificata e

dichiarazione di conformità:

- per “rilascio” si intende la consegna di un supporto fisico idoneo a ricevere la memorizzazione della rappresentazione corrispondente al documento analogico e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale;
- per “spedizione” si intende l’inoltro telematico del/dei file corrispondenti per il tramite di un sistema di posta elettronica o di altro sistema di comunicazione informatica e della dichiarazione di conformità munita della firma elettronica del pubblico ufficiale.

Le copie per immagine su supporto informatico di documenti originali formati su supporto analogico hanno la medesima efficacia probatoria degli originali, se:

- la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le *Linee guida* AgID;
- sono formate nel rispetto delle *Linee guida* AgID e se la loro conformità all’originale non è espressamente disconosciuta.

#### **Art. 19 Estratto informatico di documento amministrativo informatico**

La copia che riproduce solo una parte del contenuto del documento viene definita “estratto”.

L’estratto di uno o più documenti informatici, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua l’estratto, hanno la stessa efficacia probatoria dell’originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell’attività, l’attestazione di conformità può essere inserita nello stesso documento informatico contenente l’estratto, oppure prodotta come documento informatico separato; in entrambi i casi l’attestazione dev’essere sottoscritta con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; se prodotta come documento informatico separato, questo deve contenere un riferimento temporale e l’impronta di ogni copia o estratto informatico oggetto dell’attestazione.

#### **Art. 20 Copia analogica di documento amministrativo informatico**

La copia analogica di documento amministrativo informatico è, di norma, la stampa cartacea.

La copia su supporto analogico di documento informatico, sottoscritto con firma elettronica avanzata, qualificata o digitale, per avere la stessa efficacia probatoria dell’originale da cui è tratta, deve essere certificata come conforme all’originale in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire tale attestazione nell’esercizio delle sue funzioni (copia “autentica”) salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l’obbligo di conservazione dell’originale informatico.

#### **Art. 21 Ricezione della corrispondenza su supporto analogico**

La corrispondenza in arrivo consegnata al Servizio protocollo, brevi manu dagli utenti, rispetta i seguenti orari, tutti i giorni feriali negli orari di apertura al pubblico pubblicizzati sul sito istituzionale del Comune.

I documenti consegnati direttamente agli uffici dell’AOO che non sono abilitati alla protocollazione in arrivo, se soggetti a registrazione di protocollo, sono fatti pervenire al Servizio a cura del personale che li riceve e nell’arco della stessa giornata.

I documenti consegnati direttamente agli uffici dell’AOO che sono abilitati alla protocollazione in arrivo

(ufficio protocollo e anagrafe), se soggetti a registrazione di protocollo, sono fatti pervenire a cura del personale che li riceve e nell'arco della stessa giornata agli operatori dello stesso ufficio cui compete l'attività di protocollazione. L'addetto allo smistamento dell'Ufficio Protocollo riceve i documenti analogici pervenuti all'Ente e colloca nel casellario della posta in arrivo la documentazione non soggetta a registrazione, in particolare: giornali, quotidiani, posta ordinaria restituita in quanto non recapitata, le buste contenenti le carte di identità, passaporti rilasciati dal Ministero dell'Interno e per le quali è stato richiesto il ritiro presso l'Ufficio anagrafe. Lo stesso dicasi per le licenze di porto d'armi rilasciate dal Sindaco brevi manu.

Qualora un documento cartaceo venga consegnato personalmente dall'interessato, o da altra persona incaricata, e venga richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, gli uffici abilitati possono rilasciare una fotocopia del primo foglio dopo avervi apposto il timbro meccanico riportante la data di arrivo e la sigla dell'operatore. In alternativa, l'ufficio ricevente che esegue la registrazione di protocollo rilascia la ricevuta prodotta automaticamente dal sistema di gestione informatica dei documenti. Appone sul documento ricevuto l'intestazione "Comune di Casalgrande" e la data di ricezione mediante un timbro meccanico a inchiostro nero indelebile.

## **Art. 22 Apertura della corrispondenza analogica in entrata**

La corrispondenza in entrata su supporto cartaceo riportante la dicitura "riservato", "personale", "confidenziale", "S.P.M." o altre similari, non è aperta, ma consegnata in busta chiusa al destinatario il quale, dopo averne preso visione, se valuta che il documento ricevuto non è riservato ai sensi della normativa vigente in materia di privacy, è tenuto a trasmetterlo con la massima celerità all'ufficio preposto alla registrazione di protocollo in arrivo.

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

Per quanto riguarda la corrispondenza pervenuta per errore sia in formato analogico che in formato digitale perché di competenza dell'Unione Tresinaro Secchia, il servizio protocollo

- registra in entrata la corrispondenza e la trasmette al servizio protocollo dell'Unione Tresinaro Secchia se si tratta di documento informatico
- produce una copia informatica del documento analogico, ne registra l'ingresso a sistema e lo trasmette al servizio protocollo dell'Unione Tresinaro Secchia se si tratta di documento analogico

## **Art. 23 Copie per immagine su supporto informatico di documenti analogici in entrata**

1. I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e classificazione, possono essere acquisiti in formato digitale.
2. il processo di scansione si articola nelle seguenti fasi:
  - a) acquisizione delle immagini in modo che ad ogni documento, anche composto da più pagine, corrisponda un unico file di formato PDF/A;
  - b) verifica della qualità delle immagini acquisite e inserimento nel sistema di gestione informatica dei documenti.
  - c) collegamento delle immagini alle rispettive registrazioni di protocollo con la contestuale acquisizione delle loro impronte digitali;
  - d) memorizzazione delle immagini e delle relative impronte digitali nel sistema di gestione informatica dei documenti, in modo non modificabile.
3. I documenti ricevuti dall'Amministrazione su supporto cartaceo, ancorché digitalizzati con l'ausilio di scanner, al termine delle operazioni di registrazione, segnatura di protocollo, classificazione e assegnazione, sono fatti pervenire in originale agli uffici di competenza. Qualora la copia per immagine del documento analogico fosse prodotta al fine di sostituire l'originale, la conformità viene garantita mediante l'apposizione della firma digitale o firma elettronica avanzata da parte di chi effettua il raffronto.

## **Art. 24 Validità dei documenti informatici in entrata**

I documenti informatici in entrata soddisfano il requisito della forma scritta qualora presentati in via telematica, con qualsiasi mezzo telematico o informatico idoneo ad accertarne la provenienza. Detta condizione è garantita qualora sia presente almeno uno dei seguenti requisiti:

- documento sottoscritto in forma autografa, scansionato e presentato unitamente alla scansione della copia del documento di identità;
- documento trasmesso dal richiedente o dal dichiarante dal proprio domicilio digitale, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare;
- documento trasmesso tramite portali predisposti per la fruizione di servizi on line, da soggetti identificati tramite il Sistema pubblico di identità digitale (SPID) o con la carta di identità elettronica o con la carta nazionale dei servizi.

## **Art. 25 - Documenti trasmessi tra pubbliche amministrazioni**

Ai fini del procedimento amministrativo, le comunicazioni tra il Comune di Casalgrande e le altre pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica certificata o in cooperazione applicativa; la loro validità è determinata dalla possibilità di verificarne la provenienza, condizione assolta dalla presenza di almeno uno dei seguenti requisiti:

- sottoscrizione del documento tramite firma digitale o altro tipo di firma elettronica qualificata;
- segnatura di protocollo e sigillo elettronico qualificato;
- trasmissione dei documenti attraverso cooperazione applicativa;
- trasmissione dei documenti attraverso sistemi di posta elettronica certificata.

All'interno del documento, l'indicazione del nominativo del soggetto responsabile del contenuto del documento, coincidente con il nominativo del sottoscrittore digitale, consentirà di esplicitare la fonte e la responsabilità dell'immissione e della trasmissione dell'atto, conferendo validità al contenuto del documento, fino a querela di falso.

## **Art. 26 Rilascio di ricevute attestanti la consegna dei documenti**

Nel caso di documenti informatici in arrivo su una delle caselle PEC del Comune, provenienti da casella PEC, il Sistema invia al mittente un messaggio contenente la ricevuta di avvenuta consegna. Nel caso di istanze formate attraverso l'utilizzo dei portali messi a disposizione dall'Ente, la ricevuta di acquisizione dell'istanza viene prodotta in automatico dal Sistema nel momento stesso dell'inoltro dell'istanza, completa di segnatura di protocollo.

Nel caso di documenti cartacei consegnati a mano, qualora richiesto dal consegnatario, è previsto il rilascio, tramite procedura di protocollo, della ricevuta attestante l'avvenuta protocollazione del documento. In alternativa, e su richiesta, è prevista la semplice apposizione del timbro datario, siglato dall'operatore ricevente, su copia del documento, prodotta dall'operatore.

## **PARTE III** **REGISTRAZIONE DEI DOCUMENTI**

## **Art. 27 Il protocollo informatico: requisiti tecnologici e funzionalità**

Il Comune di Casalgrande utilizza l'applicativo PRISMA – Gestione Protocollo Informatico fornito dal Gruppo FINMATICA. La descrizione funzionale del protocollo informatico è costituita dal Manuale Utente aggiornato alla release in uso (allegato n. 5).

1. Ai sensi del punto 3.1.5 delle Linee Guida Agid il sistema di protocollo informatico assicura che:



- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA;
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.
- l'univoca identificazione ed autenticazione degli utenti;
- la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette da modifiche non autorizzate, archiviate e conservate.

2. Il sistema di cui al comma 1 garantisce inoltre:

- a) il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
- b) il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate, archiviate e conservate.

La conformità del sistema di gestione informatica dei documenti ai requisiti minimi di cui ai commi 1 e 2 è attestata dal fornitore con idonea documentazione inclusa nella fornitura.

Il sistema di protocollo informatico dell'Amministrazione comprende la funzionalità minima, le funzionalità aggiuntive e le funzionalità interoperative, così come definite nel glossario riportato in appendice A.

## **Art. 28 Registrazione di protocollo**

Per registrazione di protocollo si intende l'apposizione o l'associazione al documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso. La registrazione si effettua di norma entro la giornata di arrivo o comunque entro 24 ore lavorative dal ricevimento o, se intercorrono dei giorni festivi o di chiusura programmata del Comune, nel primo giorno lavorativo utile. Ogni numero di protocollo individua un unico documento e gli eventuali allegati allo stesso e, di conseguenza, ogni documento con i relativi allegati reca un solo numero di protocollo immutabile.

La registrazione di protocollo per ogni documento è effettuata mediante la memorizzazione di elementi obbligatori immutabili, elementi obbligatori modificabili ed elementi non obbligatori e modificabili.

La registrazione degli elementi obbligatori immutabili del protocollo informatico non può essere modificata, integrata, cancellata ma soltanto annullata mediante un'apposita procedura in capo al Responsabile dell'Ufficio Archivio e Protocollo e al suo personale. L'immutabilità e l'immutabilità della registrazione di protocollo sono garantite dal sistema di gestione documentale.

Ciascuna registrazione di protocollo contiene dati obbligatori e dati accessori.

I dati obbligatori non modificabili sono:

- a) numero di protocollo, generato automaticamente dal sistema;
- b) data di registrazione di protocollo, assegnata automaticamente dal sistema;
- c) mittente per i documenti ricevuti, o destinatario per i documenti spediti;
- d) oggetto del documento;
- e) impronta del documento informatico
- f) numero degli allegati
- g) descrizione degli allegati

Gli elementi obbligatori modificabili sono:

- a) unità organizzativa responsabile del procedimento, affare,
- b) attività (UOR);

- c) responsabile del procedimento amministrativo (RPA);
- d) classificazione archivistica;
- e) fascicolo.

Gli elementi non obbligatori modificabili sono:

- a) Recapiti del mittente
- b) Collegamento ad altri fascicoli
- c) Tipologia del documento
- d) Durata della conservazione
- e) altri tipi di annotazioni

1. Le registrazioni di protocollo sono effettuate con il sistema di gestione informatica dei documenti in un'unica soluzione, ad esclusione di interventi intermedi, anche indiretti, da parte degli operatori.
2. La numerazione delle registrazioni di protocollo dei documenti di un'A.O. è unica e progressiva. Essa si chiude il 31 dicembre di ogni anno e ricomincia da 1 all'inizio dell'anno successivo.
3. Il numero di protocollo è costituito da sette cifre numeriche.
4. Nella visualizzazione del numero di protocollo le posizioni più significative mancanti vengono riempite con gli '0' (zero).
5. Le lettere anonime sono registrate al protocollo generale indicando nel campo mittente la dicitura "anonimo". Fanno eccezione, e pertanto sono distrutte, quelle lettere anonime e quelle comunicazioni elettroniche il cui contenuto non riguarda le funzioni dell'Amministrazione ed è totalmente irrilevante per la comunità in genere.
6. Qualora dalla mancata registrazione a protocollo del documento nella medesima giornata lavorativa di ricezione possa venir meno un diritto di terzi, è prevista la protocollazione differita, cioè il differimento dei termini di registrazione, indicando in sede di protocollazione la data di arrivo del documento (campo specifico) e, nel campo note, le motivazioni del differimento.

## **Art. 29 Documenti soggetti a registrazione obbligatoria di protocollo**

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dal Comune, ossia i cui destinatari sono esterni all'Ente e tutti i documenti informatici, ad eccezione di quelli espressamente esclusi dalla normativa vigente (TUDA, art. 53, comma 5) e altri documenti informatici già soggetti a registrazione particolare. Ugualmente sono esclusi gli atti relativi alle operazioni attinenti al censimento della popolazione o di altri censimenti particolari, i certificati di malattia, i DURC e la corrispondenza interna che, pur essendo parte della gestione di un procedimento amministrativo, non ha contenuto probatorio, i certificati anagrafici e di stato civile oltre ad estratti conto e comunicazioni di bonifici bancari.

## **Art. 30 Interoperabilità e cooperazione applicativa**

1. Per quanto riguarda le registrazioni effettuate sul sistema di gestione informatica dei documenti che sono necessarie per l'aggiornamento di altre banche dati o, viceversa, ci sia la necessità di registrare su di esso i documenti prodotti e gestiti con altri sistemi dell'Amministrazione, si ricorre di norma ai meccanismi dell'interoperabilità e della cooperazione applicativa, che permettono l'interscambio automatico di dati e documenti tra software di produttori diversi.
2. Per le finalità di cui al comma 1, il sistema di protocollo informatico dell'Amministrazione implementa i meccanismi dell'interoperabilità e cooperazione applicativa basati su soluzioni tecnologiche e modelli standard conformi alle linee guida dettate dall'AGID.

### **Art. 31 Il registro giornaliero di protocollo**

Il registro giornaliero di protocollo è prodotto in maniera automatica dal software di gestione documentale entro il giorno lavorativo seguente, mediante la generazione o il raggruppamento delle informazioni registrate secondo una struttura logica predeterminata e memorizzato in forma statica, immutabile e integra.

Il registro giornaliero è trasmesso al sistema di conservazione entro la giornata lavorativa successiva alla produzione.

### **Art. 32 Annullamento o modifica delle registrazioni di protocollo**

1. Le registrazioni di protocollo possono essere annullate su autorizzazione del Responsabile della gestione documentale e con apposito documento autorizzativo.
2. Le registrazioni annullate rimangono memorizzate nella base di dati e sono evidenziate dal sistema di gestione informatica dei documenti con un simbolo o una dicitura.
3. Non si annulla mai un documento informatico trasmesso con PEC in quanto il destinatario è già in possesso del documento stesso, con l'eccezione del caso in cui sia errato proprio l'indirizzo PEC del destinatario. Si può procedere con la redazione di un nuovo documento che annulla e sostituisce il precedente (in questo caso è necessario citare il riferimento del protocollo), è protocollato e inviato via PEC.
4. L'operazione di modifica di una registrazione di protocollo è eseguita con le seguenti modalità:
  - 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 riportando, a seconda dei casi, un segno o una dicitura in posizione sempre visibile e tale, comunque, da consentire la loro lettura unitamente alla data, all'identificativo dell'operatore e agli estremi del provvedimento di autorizzazione.

### **Art. 33 Riservatezza delle registrazioni di protocollo**

1. Ad ogni documento, all'atto della sua registrazione nel sistema di gestione informatica dei documenti, è assegnato un livello di riservatezza, che consente di stabilire quali utenti o gruppi di utenti possono avere accesso ad esso.
2. La visualizzazione delle informazioni nel sistema segue la logica dell'organizzazione e dei ruoli; pertanto, ciascun utente può accedere solamente ai documenti che ha prodotto o che gli sono stati assegnati direttamente, e a quelli dell'unità organizzativa cui appartiene.
3. I documenti a cui è stato assegnato un certo livello di riservatezza "PRIVACY" non vengono mai visualizzati agli utenti non autorizzati, neanche a fronte di una ricerca globale nell'archivio o una ricerca *full text*. Il sistema filtra l'accesso non soltanto al contenuto del documento ma anche ai dati della registrazione. Si tratta di tipologie di documenti per le quali sono previste particolari forme di riservatezza e di accesso controllato al protocollo unico secondo la normativa vigente relativamente a dati sensibili e giudiziari in esso contenuti.
4. Il Responsabile della gestione documentale individua, in collaborazione con Responsabile della *privacy*, le tipologie documentarie soggette a *privacy* e per ognuna di esse definisce le modalità di trattamento. Il documento risultante, denominato *policy* per la riservatezza dei dati e dei documenti gestiti nel sistema di protocollo informatico, è riportato nel sito web del Comune all'indirizzo

[https://www.comune.casalgrande.re.it/wpcontent/uploads/2022/08/Privacypolicy\\_ComuneCasalgrande.pdf](https://www.comune.casalgrande.re.it/wpcontent/uploads/2022/08/Privacypolicy_ComuneCasalgrande.pdf) e nel “Documento programmatico della sicurezza” adottato da questo ente con deliberazione del Consiglio Comunale n. 214 in data 29 dicembre 2005 oltre al Regolamento sull'utilizzo delle risorse informatiche riportato al seguente indirizzo: <https://www.tresinarosecchia.it/wp-content/uploads/2022/09/Regolamento-utilizzo-risorse-informatiche.pdf>

### **Art. 34 Registro di emergenza**

1. Il Responsabile della gestione documentale 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 di gestione informatica dei documenti, allegato 8 “Registro di emergenza”.
2. In condizione di emergenza si applicano le seguenti modalità di registrazione e di recupero dei dati:
  - a) 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 di gestione informatica dei documenti;
  - b) qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il Responsabile della gestione documentale 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;
  - c) per ogni giornata di registrazione di emergenza è riportato sul registro il numero totale di operazioni effettuate;
  - d) 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;
  - e) le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema di gestione informatica dei documenti, 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. Ciascun protocollatore è dotato degli strumenti necessari per provvedere alla protocollazione anche in condizione di emergenza e tutte le unità dovranno rivolgersi all'Ufficio Protocollo e Archivio per svolgere le operazioni di protocollazione (Iterno/Arrivo/Partenza).

## **PARTE IV**

### **FLUSSI DI LAVORAZIONE DEI DOCUMENTI**

#### **Art. 35 Consegna dei documenti**

Al termine delle operazioni di registrazione al protocollo e fascicolazione, i documenti pervenuti all'amministrazione in formato analogico o informatico vengono consegnati nel più breve tempo possibile ai destinatari interni competenti.

#### **Articolo 36 Smistamento ed assegnazione dei documenti**

I documenti protocollati in arrivo vengono smistati alle unità competenti e assegnati ai singoli componenti delle stesse. I destinatari ricevono in scrivania virtuale la notifica di avvenuto smistamento e/o assegnazione di documento, comprensiva dei dati essenziali del documento e della data di avvenuto smistamento. La notifica è di per sé link al documento e ai metadati di protocollo. Le funzioni di smistamento e assegnazione dei documenti si avvalgono della struttura organizzativa dell'Ente.

1. I dati di flusso (smistamento, assegnazione, presa in carico/rifiuto e archiviazione) sono accessibili direttamente accedendo alla maschera di protocollo di ciascun documento.
2. Lo smistamento e l'assegnazione su scrivania virtuale per competenza attribuiscono al ricevente una competenza di modifica dei dati archivistici del documento e la possibilità di effettuare ulteriori smistamenti per competenza.
3. L'unità che attiva lo smistamento mantiene anche successivamente i diritti di reperimento e visualizzazione sul documento smistato.

### **Articolo 37 Presa in carico dei documenti**

I documenti notificati in scrivania virtuale possono essere presi in carico dall'ufficio, attraverso uno dei suoi componenti, o dal singolo componente destinatario in assegnazione, dopo valutazione della pertinenza del documento rispetto ai procedimenti trattati.

La presa in carico attesta l'effettiva assunzione di responsabilità sul documento da parte del destinatario ricevente.

Al momento della presa in carico, il ricevente può conservare il documento in scrivania virtuale, può smistarlo e assegnarlo a sua volta, oppure può archiviarlo all'interno dell'area documentale.

Il Sistema di gestione informatica dei documenti tiene traccia del flusso dei passaggi del documento all'interno dell'Ente, memorizzando, per ciascuno di essi, l'identificativo dell'utente che effettua l'intervento, la data e l'ora di esecuzione.

A seguito della presa in carico, l'ufficio ricevente può associare il documento ad un proprio fascicolo, utilizzando le funzionalità della classificazione e fascicolazione secondarie.

Con la funzione "Rifiuta smistamento" il destinatario di uno smistamento/assegnazione può restituire, con obbligo di motivazione, il documento ricevuto impropriamente.

Nel caso di mancata gestione di presa in carico o rifiuto di un documento da parte dell'ufficio destinatario nell'arco di sessanta giorni dalla notifica del documento in scrivania virtuale, il Sistema attiva la presa in carico automatica a carico dell'ufficio destinatario.

### **Articolo 38 Classificazione dei documenti**

Tutti i documenti prodotti e ricevuti dall'Amministrazione, indipendentemente dal supporto sul quale sono formati, sono classificati in base al titolario riportato nell'allegato n. 4 per garantire il reperimento certo e veloce.

I documenti sono classificati a cura degli operatori che li registrano nel sistema di gestione informatica dei documenti avvalendosi del titolario, o piano di classificazione nazionale, strutturato sulla base delle funzioni dell'ente.

L'aggiornamento del titolario di classificazione dell'archivio compete al Responsabile della gestione documentale di concerto con i Responsabili delle UOR sulla base delle mutate esigenze normative ed in riferimento ai cambiamenti dell'organigramma dell'Ente. In questo caso, essi sono adottati a partire dal 1° gennaio dell'anno successivo a quello di approvazione.

Il titolario vigente è pubblicato nel sito web istituzionale, nella sezione "Amministrazione trasparente".

È garantita la storicizzazione delle variazioni del titolario di classificazione e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i vincoli tra le unità archivistiche, le unità documentarie e la struttura del titolario vigente al momento della loro produzione.

La sostituzione delle voci del titolario comporta l'impossibilità di aprire nuovi fascicoli nelle voci eliminate. Rimane possibile, invece, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

### **Art. 39 Fascicolazione dei documenti e tipologie di fascicoli**

Gli atti, i documenti e i dati di procedimento e di processo, registrati al protocollo informatico o semplicemente acquisiti al Sistema, vengono raccolti in fascicoli informatici attraverso l'attività di

fascicolazione, intesa come attività sostanziale alla tenuta dell'Archivio, funzionale all'esercizio del diritto di accesso e alla efficiente gestione del procedimento amministrativo. Il fascicolo è l'unità di base dell'archivio. Ogni fascicolo conserva documenti che afferiscono a un medesimo affare, attività o procedimento amministrativo e sono classificati in maniera omogenea. La classificazione viene apposta (o associata) in base al contenuto e secondo il grado divisionale attribuito dal titolare (o piano di classificazione), salvo alcune eccezioni, come il fascicolo di persona.

All'interno di ciascun fascicolo i documenti sono inseriti secondo l'ordine cronologico di registrazione (ordine di sedimentazione), in maniera tale che l'inserzione a fascicolo individui subito il documento più recente. L'ordine di sedimentazione è rispettato anche all'interno dei sottofascicoli. L'obbligo di fascicolatura dei documenti riguarda sia i documenti contraddistinti dalla segnatura di protocollo sia i documenti istruttori e transitori non protocollati.

La corretta tenuta del fascicolo garantisce sia la sedimentazione che l'esercizio del diritto di accesso. Sono presenti cinque tipologie di fascicolo:

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

#### **Art. 40 Formazione, implementazione, gestione ed elenco minimo di metadati descrittivi**

Per ogni procedimento, affare e attività, il Comune di Casalgrande ha l'obbligo di conservare in un fascicolo gli atti, i documenti e i dati da chiunque formati su supporto informatico; Ogni fascicolo deve essere contraddistinto dai seguenti elementi, atti a determinarne l'identificazione all'interno del sistema documentale:

- amministrazione titolare del procedimento;
- altre amministrazioni partecipanti;
- nominativo del responsabile del procedimento;
- oggetto del fascicolo;
- elenco dei documenti contenuti;
- indice di classificazione (titolo, classe, etc.);
- numero del fascicolo, identificativo di una catena numerica relativamente alla classe e al titolo di riferimento dell'anno di creazione;
- data di apertura e di chiusura del fascicolo.

1. I fascicoli possono essere organizzati in sottofascicoli e inserti, i quali sono numerati progressivamente nell'ambito delle unità archivistiche che li contengono.
2. Il fascicolo contiene i documenti relativi ad un procedimento
3. Ad ogni fascicolo, può essere assegnato un livello di riservatezza. È possibile che un utente abbia accesso ad un fascicolo ma non possa vedere tutti i documenti in esso contenuti perché ad alcuni di essi è stato

attribuito un livello riservatezza superiore a quello assegnato al fascicolo.

#### **Art. 41 Fascicoli ibridi o misti**

Nel caso di fascicoli ibridi o misti, contenenti documenti formati su supporti diversi (digitale e analogico), la camicia cartacea per la conservazione esclusiva degli originali cartacei deve riportare la classifica e il numero del fascicolo digitale. Tale attività sarà svolta dall'UOR di riferimento.

Il fascicolo ibrido è composto da documenti formati su due supporti, quello cartaceo e quello informatico, afferenti ad un affare o procedimento amministrativo che dà origine a due unità archivistiche di conservazione differenti; l'unitarietà del fascicolo è garantita dall'indicazione della classe e del numero di fascicolo sul documento oppure sul fascicolo. Tale attività sarà svolta dall'UOR di riferimento. La gestione in ingresso dei documenti analogici è disciplinata seguendo le procedure indicate precedentemente riguardo alla gestione dei documenti analogici; l'ufficio protocollo, pertanto, si occuperà della riproduzione digitale dei documenti che sarà inserita nel protocollo solo dopo aver concluso l'attività di protocollazione e classifica e di apposizione dell'etichetta con barcode prodotta dal gestionale.

L'attività di protocollazione prevederà, inoltre, l'annotazione "Documento analogico" nel sistema di Gestione documentale per i documenti analogici in entrata e in uscita.

#### **Art. 42 Tenuta degli archivi correnti, dei fascicoli e delle serie documentarie**

I dirigenti sono responsabili della formazione e della tenuta degli archivi correnti dei rispettivi settori e adottano le procedure e gli strumenti stabiliti dal presente Manuale e dal Regolamento generale del Servizio Archivio del Comune.

Ai funzionari, o a loro delegato, spetta la responsabilità della formazione e della tenuta dei fascicoli e dei singoli documenti delle pratiche di loro competenza, fino al momento del loro versamento nell'Archivio di deposito, a chiusura del procedimento.

A conclusione del procedimento, la segreteria provvede alla chiusura del fascicolo all'interno del Sistema di gestione informatica dei documenti, modificandone lo stato, da "aperto" (archivio corrente) a "chiuso" (archivio di deposito). I fascicoli rimangono consultabili all'interno del Sistema di gestione informatica dei documenti.

La chiusura del fascicolo prelude al suo versamento all'Archivio di deposito che, di norma, avviene a distanza di cinque anni dalla chiusura della pratica.

### **PARTE V** **SICUREZZA DEI SISTEMI E DEI DOCUMENTI INFORMATICI**

#### **Art. 43 Misure di sicurezza nella formazione e gestione dei documenti**

1. Il sistema di gestione informatica dei documenti dell'Amministrazione è attivato su tutte le stazioni di lavoro delle UOR che compongono l'Area Organizzativa Omogenea.
2. Il controllo degli accessi è realizzato assegnando a ciascun utente le credenziali di identificazione (User ID e Password) la cui gestione in termini di sicurezza e riservatezza è garantita dal Responsabile del Servizio sistemi informativi dell'Amministrazione e che ne determinano all'interno dell'amministrazione la corrispondente autenticazione dell'utente al sistema.
3. Il sistema di protocollo informatico gestisce diversi tipi di accesso, dalla consultazione alla possibilità di eseguire tutte le operazioni inerenti alla gestione documentale.
4. Le abilitazioni all'accesso alle funzionalità del sistema di protocollo informatico sono attribuite agli utenti dal Responsabile della gestione documentale in base al loro ruolo, ai compiti assegnati e alla struttura di appartenenza.
5. Nell'allegato n. 3, per ciascun utente del sistema di protocollo informatico, sono riportati i dati identificativi e le abilitazioni concesse dal Responsabile della gestione documentale.



6. L'accesso per via telematica al sistema di gestione informatica dei documenti da parte di utenti esterni all'AOO è consentito solo con strumenti tecnologici che permettano l'autenticazione "forte" (*strong authentication*) dei soggetti richiedenti, rappresentati:

- dalla carta d'identità elettronica (CIE) o documento digitale unificato (DDU);
- dalla carta nazionale dei servizi (CNS);
- dall'identità digitale gestita nell'ambito dello SPID (Sistema pubblico per la gestione dell'identità digitale)

Le misure di sicurezza informatica sono di carattere tecnico ed organizzativo e hanno l'obiettivo di garantire l'integrità, la disponibilità e la riservatezza dei dati e delle informazioni trattate.

#### **Art. 44 Misure tecniche di sicurezza informatica dei sistemi**

- **Misure di sicurezza fisica:** controllo degli accessi ai luoghi fisici in cui sono custoditi dati e sistemi, accesso mediante badge opportunamente abilitato;
- **Misure di sicurezza logica:** sicurezza del canale di comunicazione (es. https), architettura applicativa multi-layer;
- **Sistemi di identity management e di sicurezza:** sistemi di gestione degli account aziendali centralizzati, sistemi antivirus e sistemi di patch management per il costante aggiornamento dei sistemi operativi e di tutte le componenti applicative;
- **Politiche di backup e recovery:** produzione di copie di backup dei dati e dei documenti con frequenza giornaliera. Simulazioni trimestrali di recupero dati e sistemi.
- **Sistemi e soluzioni applicative in modalità Cloud della PA.**

#### **Art. 45 Misure di sicurezza del sistema informativo integrato di gestione documentale**

Il Sistema informativo integrato di gestione documentale rispetta le disposizioni in materia di sicurezza informatica stabilite dalla normativa vigente e le disposizioni in materia di protezione dei dati personali.

In particolare garantisce:

- l'univoca identificazione ed autenticazione degli utenti (credenziali utente con cambio password trimestrale);
- l'accesso alle sole risorse di competenza, sulla base di specifici profili abilitativi (rif. Allegato 3);
- il tracciamento permanente, su file di log, di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore;
- la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato;
- il reperimento delle informazioni riguardanti i documenti registrati;
- la formazione del registro giornaliero di protocollo e la sua trasmissione entro la giornata lavorativa successiva ai sistemi di conservazione documentale, a garanzia dell'integrità dello stesso.

#### **Art. 46 Misure di sicurezza del sistema informativo integrato di gestione documentale**

Le applicazioni utilizzate per la formazione dei documenti informatici gestiscono:

- l'identificabilità dell'Ente e del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi della normativa vigente;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati (sistemi informativi Gestionali);
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno dell'Ente, con altre AOO e con soggetti esterni.

I documenti informatici prodotti dall'Ente sono convertiti in formato pdf/A, prima della loro

sottoscrizione con firma digitale, al fine di garantire la leggibilità mediante altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento. Quando è prevista la sottoscrizione del documento amministrativo informatico, per attribuire in modo certo la titolarità del documento, la sua integrità, la sua riservatezza e la validazione temporale, il documento è sottoscritto con firma digitale.

#### **Art. 47 Misure di sicurezza informatica di carattere organizzativo-gestione dei profili abilitativi**

Sulla base delle richieste formali pervenute dai responsabili degli Uffici al Responsabile della Gestione documentale, mediante sistema informativo di gestione delle richieste di abilitazione agli applicativi, si procede all'assegnazione di un profilo abilitativo associato all'account indicato nella richiesta.

### **PARTE VI – GESTIONE DELL'ARCHIVIO DI DEPOSITO E STORICO**

#### **Art. 48 Archivio di deposito**

L'Archivio di deposito conserva in forma temporanea i documenti dell'Ente relativi ad affari e procedimenti amministrativi conclusi nell'ultimo quarantennio. In questo arco temporale, si svolgono le periodiche operazioni di selezione dei materiali ai fini dello scarto degli atti inutili e della conservazione illimitata dei restanti documenti destinati all'Archivio storico.

All'interno dell'Archivio di deposito l'ordinamento delle serie trasferite avviene nel rispetto del principio dell'ordine originario e dell'organizzazione assunta da fascicoli e serie all'interno dell'Archivio corrente.

#### **Art. 49 Trasferimento dei documenti all'Archivio di deposito (fascicoli analogici o ibridi)**

Il Responsabile della gestione documentale opera affinché sia garantita regolare periodicità nel trasferimento, dagli archivi correnti dei servizi all'Archivio di deposito, di fascicoli riconducibili a pratiche concluse, non più necessarie allo svolgimento delle attività correnti. La disposizione di versamento, che sancisce il passaggio di responsabilità sulle unità archivistiche versate, avviene in collaborazione con il dirigente responsabile.

Le liste di versamento vengono predisposte anche nel caso di versamento di atti destinati allo scarto.

In preparazione del trasferimento, il responsabile d'ufficio esegue lo scarto di duplicati, appunti, buste e documenti non protocollati giudicati superflui, e controlla che il fascicolo contenga tutti i documenti protocollati che lo compongono, evidenziando le eventuali lacune sulla stampa dell'elenco dei documenti, da inserire all'interno del fascicolo.

Sulla base di valutazioni di natura logistica, il Responsabile della gestione documentale individua la più idonea dislocazione dei materiali destinati all'incameramento.

#### **Art. 50. Sistema di conservazione dei documenti informatici**

Il Comune di Casalgrande, per la conservazione dei documenti informatici e degli altri oggetti della conservazione, si avvale di un conservatore esterno ai sensi dell'art. 44, comma 1-quater, CAD.

Il servizio di conservazione dei documenti informatici dell'ente è stato affidato al Conservatore PARER (Servizio Polo Archivistico Regionale dell'Emilia-Romagna, d'ora in avanti anche solo "Conservatore").

Le attività affidate al Conservatore sono puntualmente indicate nella convenzione per l'affidamento del servizio.

Per la descrizione delle attività del processo di conservazione non definite nel presente Manuale, così come consentito dal par. 4.6 delle Linee Guida, è fatto rinvio al **Manuale di conservazione del Polo Archivistico Regionale - ParER (Allegato 6)**, nonché agli ulteriori documenti tecnici concernenti l'affidamento del servizio di conservazione (**allegato 7 – Schema di convenzione per lo svolgimento della funzione di conservazione dei documenti informatici**).

#### **Art. 51. Responsabile della conservazione**

Il Comune di Casalgrande ha designato un unico soggetto che riveste i ruoli di Responsabile della gestione documentale e Responsabile della conservazione.

È compito del Responsabile assicurare il rispetto della normativa vigente da parte del Conservatore e degli obblighi contrattuali dallo stesso assunti, ivi compreso il rispetto delle misure di sicurezza dei dati trattati. A tal fine, il Responsabile agisce d'intesa con il RPD dell'ente.

Il Responsabile, ferma restando la propria responsabilità, può delegare in tutto o in parte una o più attività di propria competenza relative alla conservazione, affidandole a soggetti interni all'ente dotati di adeguate competenze. Gli atti di delega devono individuare le specifiche attività e funzioni delegate.

#### **Art. 52. Oggetti della conservazione**

Gli oggetti della conservazione sono:

- i documenti informatici formati dal Comune e i rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- i fascicoli informatici e rispettivi metadati (conformi all'allegato 5 alle Linee guida dell'AgID);
- il registro del protocollo informatico;
- gli altri registri e repertori tenuti dall'ente.

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

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

Il Responsabile provvede ad associare a ogni pacchetto di versamento almeno i seguenti metadati:

1. identificativo univoco e persistente del pacchetto di versamento;
2. riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
3. denominazione del soggetto responsabile della produzione del pacchetto;
4. impronta del pacchetto di versamento;
5. numero dei documenti compresi nel pacchetto.

Le specifiche operative e le modalità di descrizione e di versamento delle singole tipologie documentarie oggetto del servizio di conservazione sono dettagliatamente individuate nel Disciplinare tecnico per lo svolgimento della funzione di conservazione dei documenti informatici sottoscritto dal Comune unitamente alla convenzione di affidamento del servizio al Conservatore PARER.

#### **Art. 53. Formati ammessi per la conservazione**

I formati ammessi per la conservazione sono individuati nell'allegato 2 alle Linee guida dell'AgID. Il Responsabile, prima del versamento in conservazione, valuta i casi in cui è opportuno procedere al riversamento del documento in diverso formato, purché conforme ai formati indicati adatti alla

conservazione nell'allegato 2 alle Linee guida. In tal caso, la corrispondenza fra il formato originale e quello di riversamento è garantita dal Responsabile attraverso attestazione di conformità rilasciata secondo le modalità indicate nella Parte Seconda del presente Manuale.

#### **Art. 54 Modalità e tempi di trasmissione dei pacchetti di versamento**

All'inizio di ogni anno ciascuna UOR individua i fascicoli da versare all'archivio di deposito, dandone comunicazione al Responsabile, che provvede alla formazione e alla trasmissione dei pacchetti di versamento, secondo le modalità operative definite nel manuale del Conservatore e nei documenti tecnici sull'affidamento del servizio.

Il Responsabile genera il rapporto di versamento relativo a uno o più pacchetti di versamento e una o più impronte relative all'intero contenuto del pacchetto, secondo le modalità descritte nel manuale del Conservatore.

Prima del versamento in conservazione, il Responsabile verifica che agli oggetti della conservazione siano stati correttamente associati i rispettivi metadati e, se mancanti, richiede al produttore dell'oggetto di provvedere correttamente all'associazione dei metadati.

Il versamento dei documenti avviene secondo le seguenti tempistiche:

- versamento annuale, per cui ogni anno entro il mese di febbraio sono versati in conservazione tutti i documenti informatici dell'Unione, anche a fascicolo aperto;
- versamento automatizzato a determinate scadenze, che per il registro di protocollo giornaliero avviene entro le 24 ore successive al momento della produzione. Il Responsabile può individuare altre tipologie di versamento automatizzato a determinate scadenze per particolari tipologie di documenti;
- versamento anticipato, nelle particolari ipotesi che richiedono un versamento in conservazione prima del versamento a cadenza annuale (ad esempio, documenti con certificato di firma in scadenza).

#### **Art. 55. Memorizzazione dei dati e dei documenti informatici e salvataggio della memoria informatica**

I dati e i documenti informatici trattati dal Sistema di gestione documentale, vengono archiviati su server cloud qualificato dall'AgID ai sensi della normativa vigente.

La documentazione temporanea e di servizio formata negli anni precedenti alla pubblicazione del presente manuale (che si intende fascicolare e metadattare) viene conservata nel data center dell'Unione Tresinaro Secchia, a cui il Comune ha trasferito la funzione IT.

Le procedure di memorizzazione sono le seguenti:

- a) il salvataggio contestuale all'operatività avviene sui server di rete che ospitano il software di gestione documentale
- b) a cura del Servizio Sistemi Informativi dell'Unione Tresinaro Secchia vengono effettuate copie di backup, con periodicità minima giornaliera, della memoria dell'Amministrazione, riversate a loro volta su supporti di memorizzazione tecnologicamente avanzati e conservati nel Data Center adibito a Disaster Recovery.

#### **Art. 56 Accesso al Sistema di conservazione**

Gli utenti espressamente autorizzati dal Responsabile possono accedere al Sistema tramite credenziali personali rilasciate dal Conservatore e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

## **Art. 57. Selezione e scarto dei documenti**

Periodicamente, secondo quanto previsto nel **Massimario di selezione e scarto** (v. **Allegato 12**) viene effettuata la procedura di selezione della documentazione da proporre allo scarto ed attivato il procedimento amministrativo di scarto documentale, con eventuale invio di proposta alla competente Soprintendenza Archivistica. Le modalità per effettuare le operazioni di selezione e scarto dei documenti informatici sono descritte nel Massimario di selezione e scarto.

## **Art. 58. Misure di sicurezza e monitoraggio dei documenti digitali**

Il Manuale di Conservazione e il Piano della sicurezza del Conservatore descrivono le modalità con cui il fornitore del servizio assicura gli obiettivi di sicurezza richiesti per la conservazione a lungo termine degli archivi, dettagliando i controlli di sicurezza delle diverse componenti del sistema (organizzazione, accessi, infrastruttura, gestione dell'esercizio, gestione dello sviluppo) e le procedure adottate per garantire i *backup* degli archivi e il *Disaster recovery*.

Il Conservatore provvede altresì al periodico monitoraggio al fine di verificare lo stato delle componenti infrastrutturali del sistema e l'integrità degli archivi.

Il Responsabile vigila affinché il Conservatore provveda alla conservazione integrata dei documenti, dei fascicoli e dei metadati associati nelle fasi di gestione e di conservazione. A tal fine, con cadenza almeno annuale, richiede al Conservatore l'esibizione di un campione di documenti o fascicoli.

Nel caso siano riscontrate irregolarità, provvede a sollecitare il Conservatore affinché vi ponga rimedio, anche attraverso gli strumenti contrattuali previsti negli atti di affidamento del servizio.

## GLOSSARIO DEI TERMINI E DEGLI ACRONIMI

TERMINE	DEFINIZIONE
<b>Accesso</b>	Operazione che consente di accedere al Sistema di gestione informatica dei documenti, con declinazioni abilitative diverse, a seconda del ruolo operativo

<b>Affidabilità</b>	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
<b>Aggregazione documentale informatica</b>	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
<b>Archivio</b>	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività
<b>Archivio informatico</b>	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche
<b>Area Organizzativa Omogenea</b>	Insieme di funzioni e uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
<b>Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
<b>Autenticità</b>	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel
<b>TERMINE</b>	<b>DEFINIZIONE</b>
	momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze
<b>Certificazione</b>	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi
<b>Classificazione</b>	Attività di organizzazione di tutti i documenti del soggetto produttore, secondo uno schema costituito da un insieme di voci articolate in modo gerarchico, che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore

<b>Conservazione</b>	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
<b>Destinatario</b>	Soggetto o sistema al quale il documento è indirizzato
<b>Documento amministrativo informatico</b>	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
<b>Documento elettronico</b>	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
<b>Documento informatico</b>	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
<b>Esibizione</b>	Operazione che consente di visualizzare un documento conservato
<b>Estratto di documento informatico</b>	Parte del documento tratto dal documento originale
<b>Estratto per riassunto di documento informatico</b>	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici
<b>Estrazione statica dei dati</b>	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
<b>Evidenza informatica</b>	Sequenza finita di bit che può essere elaborata da una procedura informatica
<b>TERMINE</b>	<b>DEFINIZIONE</b>
<b>Fascicolo informatico</b>	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
<b>File</b>	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer
<b>Filesystem</b>	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
<b>Firma elettronica</b>	Vedi articolo 3 del Regolamento eIDAS



<b>Firma elettronica avanzata</b>	Vedi articoli 3 e 26 del Regolamento eIDAS
<b>Firma elettronica qualificata</b>	Vedi articolo 3 del Regolamento eIDAS
<b>Formato del documento informatico</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
<b>Funzioni aggiuntive del protocollo informatico</b>	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
<b>Funzioni minime del protocollo informatico</b>	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
<b>Funzione di hash crittografica</b>	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
<b>Gestione Documentale</b>	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti
<b>hash</b>	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o "digest"
<b>Identificativo univoco</b>	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione
<b>TERMINE</b>	<b>DEFINIZIONE</b>
<b>Impronta crittografica</b>	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
<b>Integrità</b>	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità
<b>Interoperabilità</b>	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi

<b>Leggibilità</b>	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica
<b>Manuale di conservazione</b>	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture
<b>Manuale di gestione documentale</b>	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi
<b>Metadati</b>	Dati associati a un documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017
<b>Oggetto di conservazione</b>	Oggetto digitale versato in un sistema di conservazione
<b>Oggetto digitale</b>	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
<b>Pacchetto di archiviazione</b>	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con
<b>TERMINE</b>	<b>DEFINIZIONE</b>
	le modalità riportate nel manuale di conservazione
<b>Pacchetto di distribuzione</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione
<b>Pacchetto di versamento</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione
<b>Pacchetto informativo</b>	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione
<b>Percorso</b>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso

<b>Piano della sicurezza del sistema di conservazione</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi
<b>Piano della sicurezza del sistema di gestione Informatica dei documenti</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi
<b>Piano di classificazione (Titolario)</b>	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata
<b>Piano di conservazione</b>	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
<b>Piano di organizzazione delle aggregazioni documentali</b>	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
<b>Piano generale della sicurezza</b>	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
<b>Presa in carico</b>	Accettazione da parte dell'unità organizzativa o del
<b>TERMINE</b>	<b>DEFINIZIONE</b>
	singolo componente della stessa di un documento ricevuto in smistamento/assegnazione tramite scrivania virtuale
<b>Processo</b>	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita
<b>Produttore dei PdV</b>	Persona fisica, diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
<b>Protocollo Informatico</b>	Componente software del sistema di "Sistema di Gestione Informatica dei Documenti" che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo.

<b>Rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del Sistema di conservazione dei pacchetti di versamento inviati dal produttore
<b>Registro di protocollo</b>	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso
<b>Registro particolare</b>	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare
<b>Regolamento eIDAS</b>	electronic IDentification Authentication and Signature, Regolamento (UE) No 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
<b>Repertorio</b>	Registro su cui vengono annotati con un numero progressivo specifiche tipologie documentarie (es. contratti, ordinanze, delibere, ecc.) o fascicoli, secondo l'ordine cronologico in cui vengono creati
<b>Responsabile della conservazione</b>	Soggetto che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
<b>Responsabile della gestione documentale</b>	Soggetto responsabile della gestione del Sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445
<b>Responsabile della protezione dei dati</b>	Persona con conoscenza specialistica della normativa e
<b>TERMINE</b>	<b>DEFINIZIONE</b>
	delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679
<b>Riferimento temporale</b>	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC)
<b>Riversamento</b>	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione

<b>Scarto</b>	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale
<b>Serie</b>	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica)
<b>Sigillo elettronico</b>	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi
<b>Sistema di conservazione</b>	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
<b>Sistema di gestione informatica dei documenti</b>	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
<b>Titolare dell'oggetto di conservazione</b>	Soggetto produttore degli oggetti di conservazione
<b>Trasferimento</b>	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente
<b>TUDA</b>	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni
<b>Ufficio</b>	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
<b>TERMINE</b>	<b>DEFINIZIONE</b>
<b>Utente abilitato</b>	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
<b>Versamento</b>	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti.