



Città di Castelnuovo di Garfagnana

Provincia di Lucca

Via Vallisneri, 1 – 55032 Castelnuovo di Garfagnana (LU)

P.I. 00204360465

Tel. 0583-6448304 Fax. 0583-644133

Manuale di Gestione Documentale

Allegato 8 – Piano per la sicurezza informatica

Sommario

Premessa	3
Elementi di rischio	3
Sicurezza della rete di accesso	3
Accesso degli utenti interni	4
Trattamento di dati personali, particolari o giudiziari.....	4
Trattamento senza strumenti elettronici	4
Formazione dei documenti informatici	4
Sicurezza delle registrazioni di protocollo	4
Sicurezza logica e gestione dei documenti.....	5
Backup e ripristino dei dati.....	5
Trasmissione e interscambio dei documenti.....	5
Conservazione dei documenti	5
Disaster recovery e continuità operativa	5
Accesso di utenti esterni	5
Formazione del personale	5
Monitoraggio periodico	6

Premessa

Il presente **Piano di Sicurezza** è adottato dal **Comune di Castelnuovo di Garfagnana** ai sensi delle **Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici**, del **Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.)** e della normativa in materia di **protezione dei dati personali** (Regolamento (UE) 2016/679 – GDPR, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018).

Scopo del presente Piano è garantire che:

- i documenti e le informazioni trattati dal Comune siano **disponibili, integri e riservati**;
- i **dati personali**, comuni, particolari e giudiziari, siano **custoditi e trattati** in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, nonché di accesso non autorizzato o trattamento non consentito o non conforme alle finalità per le quali sono stati raccolti.

I requisiti minimi di sicurezza dei sistemi di protocollo informatico cui il presente Piano si conforma sono quelli stabiliti dall'**articolo 7 del DPCM 3 dicembre 2013**.

Il Piano di Sicurezza, in relazione ai rischi cui sono esposti i dati e i documenti trattati, definisce:

- le **politiche generali e specifiche di sicurezza** adottate dal Comune;
- le **modalità di accesso** al Sistema di Gestione Informatica dei Documenti;
- gli **interventi organizzativi, procedurali e tecnici**, con particolare riferimento alle **misure minime di sicurezza ICT** definite da AgID;
- le **attività di formazione del personale**;
- le **modalità di monitoraggio periodico** dell'efficacia e dell'efficienza delle misure di sicurezza adottate.

Il Piano è soggetto a **revisione** in presenza di nuove disposizioni normative, evoluzioni tecnologiche o mutamenti organizzativi significativi.

Elementi di rischio

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con strumenti digitali sono riconducibili a:

- **accesso non autorizzato** ai sistemi o ai documenti e dati contenuti;
- **cancellazione o manomissione** di dati e documenti;
- **perdita** di informazioni digitali;
- **trattamento illecito o non conforme** alla normativa vigente in materia di protezione dei dati personali.

Per prevenire tali rischi, il Comune di Castelnuovo di Garfagnana adotta misure tecniche e organizzative in linea con le **Linee Guida AgID**, il **GDPR** e le **Misure minime di sicurezza ICT**.

Sicurezza della rete di accesso

Il **Sistema di Gestione Informatica dei Documenti (SGID)** del Comune opera su una piattaforma **in cloud**, fornita da soggetto qualificato e conforme ai requisiti di **sicurezza, affidabilità e riservatezza dei dati** stabiliti

da AgID per i servizi cloud della Pubblica Amministrazione. L'accesso al sistema avviene esclusivamente tramite connessioni sicure, mediante protocolli di comunicazione cifrati (HTTPS/TLS), e attraverso credenziali di autenticazione personali e non trasferibili.

Accesso degli utenti interni

L'accesso degli utenti interni avviene mediante **autenticazione individuale** con credenziali composte da **User-ID e Password**. Le abilitazioni e i profili di accesso sono definiti in base ai **ruoli e alle responsabilità** di ciascun operatore, come riportato nell'Allegato n. 6 del Manuale di Gestione Documentale.

Le password devono:

- essere lunghe almeno **otto caratteri** alfanumerici;
- essere **modificate al primo accesso** e successivamente ogni **sei mesi** (ogni **tre mesi** se si trattano dati particolari o giudiziari);
- non contenere riferimenti riconducibili all'utente;
- essere custodite con la massima riservatezza.

Le credenziali non utilizzate da oltre sei mesi vengono automaticamente **disattivate**. Tutti gli accessi vengono **tracciati e registrati** ai fini di controllo e sicurezza.

Trattamento di dati personali, particolari o giudiziari

L'accesso ai dati personali, particolari o giudiziari è consentito solo a personale **autorizzato e profilato**. La verifica dei profili di autorizzazione avviene **annualmente**. Gli incaricati devono evitare di lasciare incustodita la postazione di lavoro e sono tenuti a custodire le proprie credenziali in busta chiusa presso il **Responsabile della Protezione dei Dati (RPD)** o il **Responsabile del trattamento**.

Trattamento senza strumenti elettronici

Per i trattamenti su supporto cartaceo, l'accesso ai documenti contenenti dati personali è consentito solo a personale autorizzato. Gli archivi sono collocati in **locali ad accesso controllato**, e le persone ammesse sono identificate e registrate.

Formazione dei documenti informatici

I documenti informatici del Comune sono prodotti in formati conformi a quanto previsto dall'Allegato numero 3 del Manuale di Gestione Documentale. La **firma digitale** viene apposta su documenti in formati che garantiscono **leggibilità, integrità, immutabilità e interoperabilità** (es. PDF/A).

Sicurezza delle registrazioni di protocollo

Ogni registrazione di protocollo è associata all'identificativo univoco dell'autore e alla data e ora dell'operazione.

Le modifiche e gli annullamenti sono registrati tramite **log di sistema non alterabili** e autorizzati dal **Responsabile della Gestione Documentale**. Al termine di ogni giornata lavorativa, viene generato il **registro giornaliero di protocollo digitale**, trasferito alla struttura di **conservazione accreditata** entro la giornata lavorativa successiva.

Sicurezza logica e gestione dei documenti

Il sistema garantisce la **tracciabilità di tutte le operazioni**, l'immodificabilità dei documenti e la protezione da accessi non autorizzati. Sono attivi **software antivirus e firewall**, aggiornati periodicamente. Il sistema operativo e l'applicativo cloud sono mantenuti **costantemente aggiornati** con le ultime versioni di sicurezza rilasciate dal fornitore.

Backup e ripristino dei dati

Il **backup** dei dati avviene su base **giornaliera, settimanale e mensile**.

I supporti contenenti dati di backup sono **crittografati e custoditi in ambiente sicuro**, con accesso limitato al personale autorizzato. Il **piano di ripristino (disaster recovery)** garantisce il recupero dei dati entro i tempi massimi previsti dai livelli di servizio.

Trasmissione e interscambio dei documenti

La trasmissione dei documenti informatici avviene esclusivamente attraverso il **Sistema di Gestione Informatica dei Documenti** o mediante **posta elettronica certificata (PEC)**. Le informazioni relative alla **segnatura di protocollo** sono strutturate secondo gli **schemi XML** previsti dalle **Linee Guida AgID (Allegato 6)**.

Conservazione dei documenti

I documenti informatici sono trasferiti in conservazione tramite pacchetti di versamento **conformi alle** regole tecniche AgID. **Il Comune si avvale di un conservatore accreditato, in grado di assicurare la conservazione a norma dei documenti informatici e dei relativi metadati.**

Disaster recovery e continuità operativa

In conformità all'art. 50-bis del D.Lgs. 82/2005, il Comune di Castelnuovo di Garfagnana adotta un Piano di Continuità Operativa e di Disaster Recovery, volto a garantire la continuità dei servizi essenziali e il tempestivo ripristino dell'operatività.

Accesso di utenti esterni

L'accesso ai documenti da parte di utenti esterni avviene nel rispetto della **Legge 241/1990** e del **Regolamento (UE) 2016/679 (GDPR)**. Durante la consultazione, vengono adottate misure per assicurare la **tutela della riservatezza** (es. posizionamento del monitor, schermatura di dati non pertinenti).

Formazione del personale

Il Comune predispone un **piano formativo periodico** rivolto al personale coinvolto nella gestione documentale, comprendente:

- l'utilizzo del sistema gestionale in cloud;
- la protocollazione e fascicolazione dei documenti informatici;
- la gestione e conservazione digitale;
- gli aggiornamenti normativi in materia di sicurezza e privacy.

Monitoraggio periodico

Il **Responsabile della Gestione Documentale** effettua verifiche periodiche sul corretto funzionamento del sistema, anche tramite controlli a campione, documentando le attività e proponendo eventuali azioni correttive.