Piano di Sicurezza del Sistema di Gestione Informatica dei Documenti (SGID)

Premesso che

- il Comune gestisce un significativo flusso documentale informatico e analogico, distribuito tra più settori e servizi;
- il Sistema di Gestione Informatica dei Documenti (SGID) costituisce infrastruttura essenziale per l'azione amministrativa, la trasparenza, l'efficienza e la tutela dei diritti dei cittadini;
- la sicurezza del patrimonio documentale rappresenta un presupposto fondamentale per la continuità amministrativa e la legittimità dell'azione dell'Ente;

Visto

- il Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005 e s.m.i.);
- le Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- il Regolamento (UE) 2016/679 (GDPR) e la normativa nazionale in materia di protezione dei dati personali;
- la normativa vigente in materia di sicurezza informatica e organizzativa nella Pubblica Amministrazione;

Considerato che

- il Comune ha adottato il Manuale di Gestione Documentale;
- il Piano di Sicurezza del Sistema di Gestione Informatica dei Documenti ne costituisce allegato tecnico-operativo;

Art. 1 – Oggetto e finalità

1. Il presente Piano di Sicurezza disciplina l'insieme delle misure organizzative, procedurali e tecnologiche adottate dal Comune per la protezione del Sistema di Gestione Informatica dei Documenti.
2. Le misure sono finalizzate a garantire riservatezza, integrità, disponibilità, autenticità, tracciabilità e reperibilità dei documenti amministrativi.

Art. 2 – Ambito di applicazione

1. Il Piano si applica a tutti i documenti informatici e, per quanto compatibile, ai documenti analogici gestiti dal Comune.
2. Esso riguarda l'intero ciclo di vita del documento: formazione, protocollazione, classificazione, fascicolazione, gestione, archiviazione e conservazione.
3. Le disposizioni si applicano a tutto il personale dell'Ente, nonché a collaboratori e fornitori esterni che operano sul SGID.

Art. 3 – Principi di sicurezza

1. Il Comune ispira la gestione documentale ai seguenti principi:
    a) riservatezza dei dati e dei documenti;

b) integrità delle informazioni;
c) disponibilità continua dei servizi documentali;
d) autenticità e affidabilità dei documenti;
e) tracciabilità delle operazioni.

Art. 4 – Ruoli e responsabilità

1. Il Responsabile della Gestione Documentale definisce le politiche di sicurezza documentale e vigila sull'applicazione del presente Piano.
2. Il Responsabile della Transizione Digitale coordina gli aspetti tecnologici e organizzativi del SGID.
3. Gli Amministratori di sistema assicurano la corretta gestione tecnica delle infrastrutture e l'applicazione delle misure di sicurezza.
4. Gli utenti sono responsabili dell'utilizzo corretto del SGID nel rispetto delle autorizzazioni assegnate.

Art. 5 – Gestione degli accessi

1. L'accesso al SGID è consentito esclusivamente a utenti identificati e autorizzati.
2. Le credenziali di accesso sono personali e non cedibili.
3. I profili di autorizzazione sono attribuiti in base alle funzioni e ai settori di appartenenza.
4. In caso di cessazione del rapporto di lavoro o cambio di mansioni, le autorizzazioni sono tempestivamente aggiornate o revocate.

Art. 6 – Sicurezza logica e applicativa

1. Il Sistema di Gestione Informatica dei Documenti dell'Ente è gestito tramite una soluzione software dedicata allo SGID, adottata in modalità cloud.
2. La soluzione è erogata tramite infrastruttura **cloud SaaS qualificata** e utilizza **software accreditato/qualificato da AgID**, in conformità alla normativa vigente per le Pubbliche Amministrazioni.
3. Il servizio cloud adottato è conforme al **Regolamento (UE) 2016/679 (GDPR)** e garantisce la gestione dei dati personali e documentali nel pieno rispetto delle disposizioni europee e nazionali in materia di protezione dei dati.
4. Il fornitore del servizio assicura adeguate misure di sicurezza logica, organizzativa e fisica, inclusi:
    a) protezione dei dati da accessi non autorizzati;
    b) disponibilità e resilienza dei sistemi;
    c) continuità operativa e disaster recovery.
5. Il Comune verifica periodicamente il mantenimento dei requisiti di qualificazione e conformità della soluzione adottata.

Art. 7 – Protezione dei dati e dei documenti

1. I documenti e i dati sono protetti da accessi non autorizzati, perdita o alterazione.
2. Le copie e le esportazioni dei documenti sono consentite esclusivamente secondo le autorizzazioni.

Art. 8 – Tracciamento e controlli

1. Tutte le operazioni rilevanti sul SGID sono registrate in appositi log.
2. I log sono conservati per il tempo stabilito da normativa.

Art. 9 – Gestione degli incidenti di sicurezza

1. Gli incidenti di sicurezza sono tempestivamente segnalati secondo le procedure interne.

Art. 10 – Formazione del personale

1. Il Comune promuove la formazione continua del personale sull'uso corretto del SGID.
2. Sono realizzate attività di sensibilizzazione sui temi della sicurezza documentale e informatica.

Art. 11 – Verifiche e aggiornamento

1. Il presente Piano è oggetto di verifica periodica.
2. È aggiornato in caso di modifiche normative, organizzative o tecnologiche rilevanti.

Art. 12 – Entrata in vigore

1. Il presente Piano di Sicurezza entra in vigore dalla data di approvazione ed è vincolante per tutti i soggetti coinvolti nella gestione documentale del Comune.