ALLEGATO 7

PIANO DI SICUREZZA DEL SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI

Al fine di garantire la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni, il Comune di Reggello adotta, ai sensi del par. 3.9 delle LLGG, il seguente piano di sicurezza del sistema di gestione informatica dei documenti.

Il piano di sicurezza, basato sui risultati dell'analisi dei rischi a cui sono esposti i dati e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'Amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno del Comune di Reggello;
- le modalità di accesso al sistema di protocollo e gestione documentale;
- le misure di sicurezza operative adottate sotto il profilo organizzativo, procedurale e tecnico;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

L'attuazione del piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dal Comune di Reggello siano resi disponibili, autentici e integri e riservati;
- i dati personali, i dati sensibili e quelli giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il Comune di Reggello ha adottato le misure tecniche e organizzative atte a garantire la protezione logica e fisica di documenti, informazioni e dati in possesso dell'Amministrazione previste nel piano di sicurezza dell'Unione dei Comuni del Valdarno e della Valdisieve, come di seguito specificate:

- protezione periferica della Intranet dell'Amministrazione;
- protezione dei sistemi di accesso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazione;
- modifica periodica delle credenziali di accesso. Le credenziali di accesso sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime;
- piano di continuità del servizio con particolare riferimento, sia all'esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo in caso di disastro;
- conservazione, a cura dei servizi informatici, delle copie di riserva dei dati e dei documenti, in locali diversi e lontani da quelli in cui è installato il sistema di elaborazione di esercizio;
- gestione delle situazioni di emergenza informatica attraverso risorse qualificate;
- impiego e manutenzione di un adeguato sistema antivirus;
- uso di codici identificativi (o altre soluzioni) dei dati sensibili e giudiziari contenuti in elenchi, registri o banche dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli intellegibili a chi non è autorizzato ad accedervi;
- impiego di idonee misure di sicurezza anche nel caso di supporti analogici contenenti banche dati sensibili e giudiziari;
- archiviazione giornaliera, in modo non modificabile, delle copie del registro di protocollo.

Il sistema è costituito dall'utilizzo di:

- applicativi in cloud
- applicativi on premise

Le misure tecniche e organizzative atte a garantire la protezione logica e fisica degli applicativi in cloud sono predisposte dal fornitore del servizio.

Componente logica della sicurezza del Sistema

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
Tale componente, nell'ambito del sistema di protocollo informatico e di gestione documentale, è stata realizzata attraverso:

- identificazione e autenticazione utente;
- profilazione degli accessi (ACL);
- politica antivirus;
- firma digitale;

All'interno della suite sono presenti una serie di applicazioni e procedure che vengono rese disponibili contemporaneamente (distribuite) a più soggetti tramite rete.
Agli utenti generici non è consentito interrogare direttamente il database e nemmeno accedere direttamente alle cartelle di sistema ai server fisici e virtualizzati.
Le precedenti operazioni sono possibili ai soli soggetti autorizzati ed appartenenti all'Ufficio Ced per le sole attività sistemistiche di amministrazione, aggiornamento e manutenzione delle componenti di sistema.
Nessun sistema, componente, servizio ed interfaccia inerente al sistema è direttamente accessibile e fruibile tramite rete pubblica.

I documenti informatici, una volta registrati sul Sistema di Gestione Informatica dei Documenti, risultano immodificabili e non eliminabili; l'accesso ad essi, da parte degli utenti interni all'AOO, avviene soltanto attraverso il Sistema medesimo, previa procedura di identificazione informatica e nel rispetto dei profili di autorizzazione di ciascun utente.
Il Sistema consente l'effettuazione di qualsiasi operazione su di esso o sui dati, documenti, fascicoli e aggregazioni documentali in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività.
Il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni (log di sistema) sono protette al fine di non consentire modifiche non autorizzate. I dati registrati nei file di log sono raccolti, memorizzati e conservati dal sistema informatico in conformità alla normativa vigente. Le informazioni contenute nei file di log possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione di tali file per un periodo più lungo di quanto disposto dalla legge.
Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione di sistemi di sicurezza perimetrale (firewall con doppia autenticazione) mantenuti regolarmente aggiornati ogni qualvolta venga rilasciato un aggiornamento dal fornitore. E' inoltre adottato un sistema di protezione degli endpoint e della rete, basato su analisi tramite Intelligenza Artificiale con gestione centralizzata in cloud.
Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dall'AOO e il Sistema di Gestione Informatica dei Documenti vengono tenuti costantemente aggiornati, per mezzo dell'installazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Gestione delle registrazioni di protocollo di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo, che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.
Le registrazioni di sicurezza possono essere costituite:

- dai log di sistema generati dal sistema operativo;
- dalle registrazioni di utilizzo del gestore del SGID;

Le registrazioni di sicurezza sono soggette almeno ad una delle seguenti misure:

- scrittura su database in modalità sincrona (scrittura logica che coincide con scrittura fisica sul disco);
- copie di backup realizzate su server con sistemi RAID5;
- conservazione di una copia di sicurezza dei backup in locali diversi, come previsto dalla normativa.

Backup e ripristino dell'accesso ai dati

Il backup dei dati contenuti nel SGID avviene con cadenza giornaliera. Il tempo di ripristino dei dati dipende dalla consistenza degli stessi ma avviene sempre nel rispetto dei tempi previsti dalla vigente normativa in materia.
Le copie di dati eseguite in locale sono custodite, sotto chiave, al fine di evitare accessi non autorizzati e trattamenti non consentiti.
Supporti riscrivibili, eventualmente utilizzati dall'Ente, contenenti dati sensibili o giudiziari, possono venire cancellati e riutilizzati esclusivamente nel caso in cui le informazioni in essi contenute non siano intelligibili e in alcun modo ricostruibili.
Qualora dati sensibili e giudiziari vengano memorizzati su supporti rimovibili non riscrivibili, una volta che sia cessato lo scopo per cui tali dati sono stati memorizzati, i supporti vengono distrutti.

Trasmissione e interscambio dei documenti

Il Comune di Reggello predilige l'utilizzo di tecnologie di trasmissione sicure. In riferimento alla modalità di scambio dei documenti, le modalità previste per la trasmissione hanno il seguente livello di sicurezza:

Posta elettronica Certificata - livello di sicurezza: elevato
Canali Web-Istanze online - livello di sicurezza: elevato
Interoperabilità - livello di sicurezza: elevato
Posta elettronica ordinaria - livello di sicurezza: basso

Conservazione dei documenti

I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore accreditato dall'AgID, che svolge tale attività in conformità a quanto sancito nelle LLGG. Il trasferimento in conservazione avviene mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nello stesso manuale di conservazione e nella normativa vigente.

Accesso di utenti esterni

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e s.m.i., dal D. Lgs. 196/03 e s.m.i. e dal Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016.

Qualora l'utente esterno decida di esercitare il proprio diritto di accesso, la consultazione deve avvenire in modo che siano resi visibili soltanto dati o notizie che riguardino il soggetto interessato ed adottando gli opportuni accorgimenti (ad es. il posizionamento del monitor) volti ad evitare la diffusione di informazioni di carattere personale.

Piani formativi del personale

Ai fini di una corretta gestione dell'intero ciclo dei documenti informatici, dalla formazione degli stessi fino alla loro trasmissione al sistema di conservazione, l'Ente predispone le apposite attività formative per il personale, con particolare riferimento ai seguenti temi:

- utilizzo applicativi software per la gestione dei documenti informatici;
- utilizzo del Sistema di Gestione Informatica dei Documenti;
- politiche e aspetti organizzativi previsti nel manuale di gestione;
- legislazione e tematiche relative al documento informatico, alla gestione documentale e alla
- conservazione digitale a norma;
- fascicolazione dei documenti informatici;
- gestione dei fascicoli informatici;
- aggiornamento sui temi suddetti.

Monitoraggio periodico del funzionamento del Sistema

Il Responsabile della Gestione Documentale effettua periodiche verifiche sul corretto funzionamento del Sistema di Gestione Informatica dei Documenti, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale. I log di sistema sono comunque conservati e protetti in modo da consentire successive verifiche che dovessero risultare necessarie sullo svolgimento di tutte le operazioni rilevanti al fine della sicurezza dei dati, effettuate sul sistema.

Componente fisica della sicurezza

Si garantisce la sicurezza fisica degli accessi ai luoghi in cui sono custodite le risorse del sistema informatico attraverso locali dotati di:

- porte chiuse a chiave;
- impianti elettrici dedicati;
- sistemi di condizionamento per il raffreddamento delle apparecchiature;
- continuità elettrica è garantita da gruppi di continuità dedicati per i sistemi informatici;
- estintori;
- controllo dell'attuazione del piano di verifica periodica dell'efficacia dei sistemi di sorveglianza e degli estintori;

Trattamento dei dati personali, sensibili o giudiziari senza l'ausilio di strumenti elettronici

Analogamente al trattamento dei medesimi dati svolto per mezzo di strumenti elettronici, sarà verificato il sussistere delle condizioni per l'accesso e il trattamento dei suddetti dati, da parte di ciascun utente o gruppo di utenti, con cadenza almeno annuale.
I documenti, sono controllati e custoditi dagli incaricati del trattamento per tutto il tempo di svolgimento dei relativi compiti; nell'arco di tale periodo gli incaricati medesimi si assicureranno che a tali documenti non accedano persone prive di autorizzazione.
L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solo previa autorizzazione; le persone ammesse sono identificate e registrate.