

Allegato 8

Piano per la sicurezza informatica

Manuale di gestione documentale – Comune di San Giacomo V.se

Allegato 8 – Piano per la sicurezza informatica

I documenti del Comune di San Giacomo V.se vengono gestiti attraverso il sistema di Protocollo e gestione documentale *Egisto* di SISCOM SPA.

Il sistema di gestione informatica dei documenti:

- a) garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- b) assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- c) fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- d) consente il reperimento delle informazioni riguardanti i documenti registrati;
- e) garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

La componente organizzativa della sicurezza consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza nell'ambito delle attività svolte dal sistema informatico *Egisto*. In tale contesto la gestione della sicurezza si realizza sia con specifici interventi tecnici e organizzativi finalizzati a prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, sia con attività di controllo e verifica essenziali ad assicurare l'efficacia nel tempo del sistema informatico.

Conseguentemente vengono adottate le seguenti misure di sicurezza, la cui competenza è posta a carico dei seguenti settori del Comune di San Giacomo V.se:

- Sicurezza Fisica e infrastrutturale: ditta SISCOM SPA (software in cloud);
- Sicurezza logica: _____;
- Sicurezza Organizzativa: _____.

La sicurezza fisica degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informativo è garantita dalle norme di sicurezza di SISCOM SPA, in quanto il *software* *Egisto/Olimpo* è completamente in *cloud*.

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 gestione documentale, si realizza attraverso l'identificazione dell'utente, la profilazione degli accessi, la politica antivirus, firma digitale, monitoraggio delle sessioni di lavoro, disponibilità del software e dell'hardware. Il software e le informazioni gestite risiedono in un sistema centralizzato presso la ditta SISCOM SPA.

L'operatore può accedere unicamente al livello "interfaccia utente" e solamente se dotato di specifiche autorizzazioni di accesso al sistema.

L'interfaccia disponibile viene generata in funzione delle autorizzazioni in possesso dell'utente connesso; funzioni e dati ai quali l'utente non è autorizzato ad accedere non vengono resi disponibili.