2023

Politica
per la sicurezza delle informazioni

Ente Autonomo Volturno

Politica
per la sicurezza delle informazioni
di Ente Autonomo Volturno

Indice

1 Introduzione e obiettivi

Un *sistema di gestione della sicurezza delle informazioni* (o SGSI) può essere definito come l'insieme di elementi interrelati e interagenti di un'organizzazione per stabilire politiche, obiettivi e processi al fine di garantire la *sicurezza delle informazioni*, ossia la preservazione delle proprietà di *riservatezza*, *integrità* e *disponibilità*.

L'*Ente Autonomo Volturno srl* ha sviluppato e implementato un sistema di gestione della sicurezza delle informazioni conforme ai requisiti prescritti dallo standard internazionale ISO/IEC 27001:2013 allo scopo di soddisfare i seguenti obiettivi per la sicurezza delle informazioni:

a) dimostrare l'impegno dell'organizzazione nel garantire la conformità alle normative e agli standard internazionali in materia di sicurezza delle informazioni;

b) dimostrare alle parti interessate il valore della sicurezza delle informazioni per l'organizzazione e la capacità di soddisfare i propri requisiti relativi alla sicurezza delle informazioni;

c) rendere il personale consapevole dei benefici derivanti dal miglioramento delle prestazioni relative alla sicurezza delle informazioni

d) identificare, valutare e trattare i rischi relativi alla sicurezza delle informazioni incluse nel campo di applicazione del SGSI;

e) garantire la tutela delle informazioni aziendali e dei dati personali, riducendo sicché al minimo la verosimiglianza e l'impatto di eventuali minacce per la loro riservatezza, integrità e disponibilità.

f) ricercare attivamente opportunità per migliorare continuamente i servizi e i processi di sicurezza delle informazioni.

2 Campo d'applicazione del sistema di gestione per la sicurezza delle informazioni

Il *campo di applicazione* del sistema di gestione della sicurezza delle informazioni, secondo lo standard ISO/IEC 27001:2013, par. 4.3, deve essere disponibile come insieme di informazioni documentate. Il campo di applicazione del SGSI di EAV srl è il seguente:

Progettazione ed erogazione del servizio di trasporto pubblico ferroviario, automobilistico e funivia di Monte Faito.

3 Principi generali

Per garantire la conformità agli obiettivi di sicurezza delle informazioni, EAV ha definito un sistema di gestione della sicurezza delle informazioni che si basa sui seguenti principi generali:

a) *Gestione della sicurezza delle informazioni:* assicurare l'identificazione dei ruoli e l'attribuzione delle responsabilità per la sicurezza delle informazioni, nonché l'istituzione di processi organizzativi per garantire la corretta applicazione del presente documento.

b) *Monitoraggio, misurazione, analisi e valutazione del SGSI*: misurare l'efficacia del SGSI di EAV e la sua capacità di adempiere ai principi della presente Politica e agli obiettivi del SGSI, in particolare tramite:

    1. Audit interni;
    2. Riesame della direzione.

c) *Gestione dei rischi relativi alla sicurezza delle informazioni:* assicurare la definizione e l'applicazione di un processo di valutazione dei rischi relativi alla sicurezza delle informazioni che includa criteri e metodologie per l'identificazione, l'analisi, la ponderazione dei rischi per la sicurezza delle informazioni, nonché per l'accettazione del rischio.

d) *Classificazione e protezione del patrimonio informativo aziendale*: assicurare che le informazioni ricevano un adeguato livello di protezione in linea con la loro importanza per l'organizzazione, sviluppando e attuando un appropriato insieme di regole per il trattamento e l'etichettatura delle

informazioni, che siano in formato cartaceo oppure elettronico.

e) *Controllo degli accessi logici ai sistemi informativi: assicurare* la coerenza dei diritti di accesso definiti ai sistemi informativi secondo i principi della "necessità di conoscere" (cd. *need to know*) e del "minimo privilegio" (cd. *least privilege*), garantendo allo stesso tempo il rispetto della “segregazione dei ruoli” (cd. *segregation of duties*).

f) *Controllo dell'accesso fisico alle aree e apparecchiature:* prevenire l’accesso fisico non autorizzato, danni e disturbi al patrimonio informativo aziendale, limitando l'accesso agli edifici, ai locali e alle apparecchiature aziendali solo ai soggetti autorizzati.

g) *Sicurezza dei sistemi informativi aziendali:* garantire l'adozione di misure di sicurezza logiche, fisiche e organizzative al fine di proteggere in modo efficace i sistemi informativi aziendali.

h) *Sviluppo di software sicuro:* assicurare che la sicurezza delle informazioni sia progettata e implementata nell'ambito del ciclo di sviluppo del software.

i) *Sicurezza delle informazioni nei rapporti con i fornitori:* assicurare la protezione degli asset e delle informazioni aziendali introducendo i requisiti relativi alla sicurezza delle informazioni all’interno degli accordi con i fornitori, servendosi, all’uopo, anche di annessi contrattuali *ad hoc*.

j) *Gestione degli eventi relativi alla sicurezza delle informazioni:* assicurare che gli eventi e gli incidenti relativi alla sicurezza delle informazioni siano correttamente riconosciuti e adeguatamente gestiti attraverso efficaci sistemi di prevenzione, comunicazione e risposta, al fine di minimizzare l'impatto sul business.

k) *Continuità operativa:* stabilire misure per la continuità operativa, con particolare attenzione alla continuità della sicurezza delle informazioni, in situazioni avverse.

l) *Gestione della conformità ai requisiti cogenti e contrattuali:* definire misure appropriate per garantire la conformità a discipline normative e/o standard internazionali in materia di sicurezza delle informazioni, con riguardo precipuo alla protezione dei dati personali (Reg. UE 679/2016 – GDPR).

Per la realizzazione dei surriferiti principi e degli obiettivi di sicurezza delle informazioni, EAV ha definito e si impegna a mantenere aggiornato un complesso di politiche e procedure. Tali politiche e procedure rappresentano l'insieme delle regole organizzative che guidano l'attuazione dei meccanismi di protezione delle diverse tipologie di informazioni e degli asset organizzativi, secondo la loro classificazione.

4 Impegno della direzione

La direzione aziendale intende dimostrare la leadership e l’impegno necessari per raggiungere gli obiettivi del SGSI aziendale, assumendosi la responsabilità della sua efficacia ed effettività ed assicurando che:

a) la presente politica per la sicurezza delle informazioni sia comunicata all’interno dell’organizzazione e sia disponibile per le parti interessate;
b) gli obiettivi di sicurezza delle informazioni siano compatibili con gli indirizzi strategici dell’Ente Autonomo Volturno srl;
c) i requisiti del SGSI siano integrati nei processi aziendali;
d) il SGSI aziendale disponga di risorse adeguate;
e) l’importanza di un'efficace gestione della sicurezza delle informazioni e della conformità ai requisiti del SGSI sia comunicata in maniera appropriata;
f) il SGSI aziendale consegua i risultati previsti;
g) il personale sia incoraggiato a contribuire all'efficacia del sistema di gestione;
h) il miglioramento continuo sia promosso attivamente;
i) sia fornito il sostegno necessario agli altri ruoli gestionali pertinenti.

5 Attività necessarie per garantire la sicurezza delle informazioni

Ente Autonomo Volturno srl si impegna a:

a) definire e attuare politiche e procedure per garantire la conformità dei processi aziendali agli standard internazionali in materia di sicurezza delle informazioni;

b) definire i requisiti di sicurezza per i processi aziendali e per i sistemi di supporto;

c) assicurare che il sistema di gestione della sicurezza delle informazioni sia parte integrante dei processi e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli;

d) effettuare a intervalli pianificati, ovvero quando sono proposti o si verificano cambiamenti significativi, le attività di valutazione dei rischi relativi alla sicurezza delle informazioni, come prescritto dallo standard internazionale ISO/IEC 27001, par. 6.1.2 e 8.2;

e) determinare i controlli di sicurezza necessari per proteggere le informazioni, gli strumenti deputati all'elaborazione e conservazione delle informazioni, gli edifici e le aree da minacce ambientali, accessi non autorizzati e attacchi dannosi, promuovendo al contempo il miglioramento continuo dell'efficacia dei controlli già esistenti;

f) definire e mantenere i contatti necessari con le autorità competenti e i gruppi specialistici;

g) definire il *piano di trattamento dei* rischi e la *dichiarazione di applicabilità (cd.* SOA o *statement of applicability*), all'esito del processo di valutazione dei rischi relativi alla sicurezza delle informazioni;

h) determinare le competenze necessarie in materia di sicurezza delle informazioni per l'intero capitale umano, assicurando che il personale soddisfi i requisiti di competenza previsti ed erogando, ove necessario, le opportune attività formative per acquisire siffatte competenze;

i) creare, rendere disponibili ed aggiornare periodicamente le *informazioni documentate* richieste dallo standard ISO/IEC 27001 e quelle ritenute necessarie per l'efficacia del SGSI (par. 7.5);

j) condurre audit interni, riesami e monitoraggi a intervalli periodici, al fine di garantire il corretto funzionamento del SGSI e la conformità ai requisiti prescritti dagli standard internazionali in materia (e, segnatamente, lo standard ISO/IEC 27001).

k) garantire che tutte le attività di trattamento dei dati personali siano conformi agli obblighi cogenti e/o contrattuali, in particolare alla disciplina insita nel Regolamento generale sulla protezione dei dati (Reg UE 679/2016 – GDPR).