Politica per la Sicurezza delle Informazioni

La Politica della Sicurezza delle Informazioni di Daikin Applied Europe intende fornire un quadro di riferimento per le persone dell'organizzazione e le parti interessate in merito agli obiettivi della sicurezza delle informazioni.
Questo si traduce nella salvaguardia dei parametri di:
Riservatezza: le informazioni non devono essere accessibili a soggetti non autorizzati;
Integrità: le informazioni non devono essere modificate da soggetti non autorizzati, non devono essere corrotte e devono essere affidabili;
Disponibilità: le informazioni devono essere accessibili ai soggetti autorizzati nei tempi previsti.

Per garantire che tali parametri siano rispettati, l'organizzazione si impegna a rendere disponibili le risorse necessarie al soddisfacimento dei **requisiti applicabili** previsti dalla norma ISO/IEC 27001, affinché siano seguite ed implementate le procedure operative definite dal Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), le politiche e tutti i controlli applicabili al perimetro come definito dalla **SOA** – (Statement Of Applicability).

In particolare, il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) di Daikin Applied Europe ha il fine di garantire:

- la piena conoscenza e la valutazione della criticità delle informazioni gestite, mediante opportuna attività di **analisi del rischio**;
- **l'accesso logico** sicuro alle informazioni sotto il principio del "Need to know";
- piena **consapevolezza** di tutti i soggetti coinvolti nei processi relativi alla sicurezza delle informazioni;
- che **l'organizzazione e le terze parti** eventualmente coinvolte collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza, in accordo con procedure e politiche del SGSI;
- il **riconoscimento tempestivo** di eventi, anomalie e vulnerabilità affinché la loro corretta gestione garantisca la protezione delle informazioni e la minimizzazione degli impatti sui processi aziendali e sulle parti interessate.
- che **l'accesso fisico** ai locali e alle aree avvenga esclusivamente da parte di personale autorizzato;
- il rispetto dei requisiti di legge e degli impegni di sicurezza stabiliti nei contratti con le parti interessate;
- la **continuità dei processi** aziendali attraverso la definizione e applicazione di idonei Piani di Continuità Operativa che comprendano adeguati Piani di Disaster Recovery;
- che il personale e le terze parti coinvolte nei trattamenti siano opportunamente **formate** in materia di sicurezza delle informazioni, maturando la necessaria consapevolezza per la corretta gestione dei dati e delle informazioni.
- che i **fornitori** siano opportunamente verificati, secondo quanto applicabile, attraverso clausole contrattuali, audit, attività di monitoraggio, condivisione di piani e di azioni di miglioramento;
- che nella fase **progettuale, nella realizzazione dei prodotti e nella fase di erogazione dei servizi,** siano considerati opportunamente i requisiti di sicurezza sin dalla loro progettazione secondo il principio di Security & data Protection by design.
- che gli **eventi** ed **incidenti** inerenti la sicurezza delle informazioni siano tempestivamente identificati, analizzati, valutati e trattati al fine di prevenire o ridurne gli impatti, bilanciandoli con il rischio d'impresa, la sua sostenibilità e la sua predisposizione all'innovazione;

- che ogni opportunità di **miglioramento** sia individuata e analizzata affinché possa essere colta;
- che i **trattamenti dei dati personali**, avvenga nel rispetto del Regolamento Europeo sulla Protezione dei Dati Personali (GDPR) 679/2016.

L'organizzazione ha definito una metodologia di **valutazione del rischio** basata sulle linee guida della ISO/IEC 27005 e sono stati individuati gli opportuni **obiettivi** (KPI) e relativi parametri di monitoraggio per la gestione delle performance del SGSI.

Il sistema di gestione della sicurezza delle informazioni viene costantemente monitorato e aggiornato per assicurare il suo **continuo miglioramento** anche con l'ausilio di audit periodici ai quali tutte le parti interessate sono sottoposti periodicamente, al fine di mantenere alto il livello di consapevolezza sul tema della sicurezza delle informazioni.

La presente politica è condivisa e resa disponibile con l'organizzazione e tutte le parti interessate attraverso il sistema intranet e specifici canali di **comunicazione**.

L'organizzazione ha definito inoltre precise **responsabilità** per la definizione e la gestione del SGSI, in particolare prevedendo un ruolo specifico assegnato al Responsabile della Sicurezza delle Informazioni (Security Manager).

In generale, in tema di informazioni Daikin Applied Europe si prefigge tra gli obiettivi primari:

- affrontare i crescenti rischi legati alla responsabilità civile o legale dell'organizzazione e della dirigenza a seguito di informazioni inesatte o all'assenza della dovuta cura nella loro protezione o alla non conformità con la normativa cogente;
- garantire la conformità delle politiche;
- aumentare la prevedibilità e ridurre l'incertezza delle operazioni aziendali portando il rischio a livelli definibili e accettabili;
- fornire un livello di garanzia che le decisioni critiche non si basino su informazioni errate;
- fornire una solida base per una gestione efficiente ed efficace del rischio, miglioramento dei processi, risposta rapida agli incidenti e gestione della continuità;
- migliorare la fiducia nelle relazioni con i clienti e partner;
- proteggere la reputazione dell'organizzazione;
- consentire modi nuovi e migliori per elaborare le transazioni elettroniche;
- assegnare le responsabilità per la salvaguardia delle informazioni nello svolgimento delle attività commerciali, dei processi di recupero delle attività aziendali e in risposta alla normativa;
- una gestione efficace ed efficiente delle risorse dedicate alla sicurezza delle informazioni.

In sintesi, l'implementazione di una strategia della sicurezza delle informazioni efficace può aggiungere valore all'organizzazione riducendo le perdite che derivano da eventi relativi alla sicurezza delle informazioni e fornendo assicurazione che incidenti e violazioni della sicurezza non siano catastrofici.

La presente Politica per la Sicurezza delle Informazioni è periodicamente rivista, da parte della Direzione, per assicurarne il continuo aggiornamento in coerenza con l'evoluzione del contesto nel quale opera Daikin Applied Europe S.p.A.

Ariccia, 09/01/2024

Francesco Aruta
Information Security Representative

Claudio Capozio
Chief Executive Officer
Daikin Applied Europe S.p.A