Thorsoft Srl

Pubblico

POL Politica di sicurezza delle informazioni

Nome della società	Thorsoft Srl
Data di entrata in vigore	04/04/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	04/04/2025	-- N / D --	Mattia Mirenda	Mattia Mirenda

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

Indice

Campo di applicazione

Questa politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi tecnologici e le sedi dell'organizzazione. Coinvolge tutto il personale, collaboratori a contratto e terze parti che hanno accesso alle informazioni o ai sistemi aziendali, indipendentemente dalla loro ubicazione geografica.

Riferimenti normativi

- **ISO 27001:2022:** Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO 27002:2022:** Linee guida per i controlli di sicurezza delle informazioni.
- **Regolamento (UE) 2016/679 (GDPR):** Protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Termini e definizioni

- **Sicurezza delle Informazioni:** La tutela della Riservatezza, Integrità e Disponibilità delle informazioni.
- **Riservatezza:** La proprietà per cui le informazioni non vengono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità:** La proprietà di salvaguardare l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione.
- **Disponibilità:** La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **SGSI (Sistema di Gestione della Sicurezza delle Informazioni):** L'approccio sistematico dell'organizzazione per gestire le informazioni sensibili in modo che rimangano sicure.

Ruoli e responsabilità

Responsabile SGSI:

- Supervisionare la conformità complessiva della politica.

Collaboratori / Terze parti:

- Comprendere e applicare la presente politica e i principi e le linee guida ivi contenute.
- Segnalare immediatamente qualsiasi anomalia o violazione della presente politica.

Obiettivi di sicurezza delle informazioni

La dedizione dell’organizzazione alla sicurezza delle informazioni non è un'attività fine a sé stessa, ma un pilastro strategico che si traduce in una serie di obiettivi chiari e misurabili, i quali guidano ogni decisione in materia. Il primo e fondamentale obiettivo è garantire una solida conformità normativa, nel pieno rispetto delle leggi, dei regolamenti e degli obblighi

contrattuali, assicurando che le pratiche di sicurezza siano sempre allineate ai più recenti requisiti legali.

Al di là della conformità, lo scopo primario dell'organizzazione è la protezione proattiva degli asset informativi. Infatti, si lavora costantemente per salvaguardare attivamente le informazioni che vengono affidate all'organizzazione dai propri clienti e la proprietà intellettuale dell'organizzazione stessa, proteggendole con determinazione da ogni minaccia, sia essa interna o esterna. Questo impegno si estende all'obiettivo di garantire la resilienza operativa; non ci si limita a prevenire gli incidenti, ma ci si prepara a rispondervi. L'organizzazione vuole essere in grado di mantenere la continuità delle operazioni critiche e di ripristinare i servizi in modo rapido ed efficace, minimizzando l'impatto sul business e sui clienti.

L'organizzazione riconosce che la tecnologia da sola non è sufficiente. Pertanto, un obiettivo cruciale è la promozione di una pervasiva cultura della sicurezza, in cui ogni cllaboratore non solo sia a conoscenza delle policy, ma comprenda profondamente il valore del proprio ruolo nella protezione delle informazioni. Infine, tutte le iniziative dell'organizzazione sono guidate da un approccio maturo alla gestione del rischio, che permette di identificare, valutare e trattare le minacce in modo intelligente e prioritario, assicurando che le risorse siano sempre investite dove possono generare il massimo valore per la sicurezza delle informazioni.

Principi fondamentali di sicurezza delle informazioni

La strategia di sicurezza delle informazioni dell'organizzazione non si basa su un singolo controllo, ma su un insieme di principi interconnessi che formano il fondamento del Sistema di Gestione adottato.

Il pilastro su cui si regge l'intera struttura è il principio della responsabilità condivisa. La sicurezza delle informazioni non è un compito relegato ad un singolo reparto, ma un dovere che appartiene a ogni persona all'interno dell'organizzazione. Per questo, si promuove una cultura in cui ogni collaoratore è consapevole del proprio ruolo e si sente tenuto a segnalare tempestivamente qualsiasi incidente, debolezza o anomalia di sicurezza nota o sospetta.

Questa responsabilità diffusa è guidata da un approccio proattivo basato sulla gestione del rischio. Le decisioni prese dall'organizzazione in materia di sicurezza delle informazioni non sono arbitrarie, ma derivano da un'analisi formale delle minacce e delle vulnerabilità, che consente di implementare controlli proporzionati ed efficaci. Uno dei principali frutti di questo approccio è il principio del controllo degli accessi, secondo cui l'accesso alle informazioni e ai sistemi viene concesso seguendo le logiche di "minimo privilegio" e "necessità di sapere" (need-to-know), assicurando che ogni utente disponga solo delle autorizzazioni indispensabili per svolgere le proprie mansioni.

I controlli, a loro volta, non sono elementi isolati. Il principio della sicurezza integrata (security-by-design) garantisce che la sicurezza sia una componente nativa e non un'aggiunta tardiva, venendo considerata fin dalla fase di progettazione di nuovi processi, sistemi o servizi. Infine, l'organizzazione applica una strategia di difesa in profondità, implementando più livelli di controlli di sicurezza (tecnologici, fisici e procedurali). In questo

modo, se una barriera dovesse fallire, altre sarebbero pronte a intervenire, creando una protezione stratificata e resiliente per i nostri asset più preziosi.

Archiviazione e aggiornamento

Questa politica è un documento controllato e sarà riesaminata con cadenza annuale, o a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia o nel contesto delle minacce, sotto la supervisione del Responsabile SGSI.

Documenti di riferimento

- *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni*
- *POL Politica del sistema di gestione*
- *POL Politica di classificazione ed etichettatura delle informazioni*
- *POL Politica di sicurezza operativa*