POL Politica di sicurezza delle informazioni

Nome della società	Gep Informatica
Data di entrata in vigore	14/05/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	14/05/2025	-- N / D --	Giulia Borghi	Davide Villa

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

La presente politica definisce i principi e gli obiettivi strategici per la gestione della sicurezza delle informazioni in Gep Informatica. Il suo scopo è proteggere gli asset informativi aziendali, quelli dei clienti e delle altre parti interessate, al fine di assicurare la continuità del business, minimizzare i rischi e massimizzare le opportunità. Questo documento si applica a tutto il personale, ai processi e alle tecnologie coinvolte nella progettazione, sviluppo, implementazione e supporto di soluzioni software per la logistica.

Riferimenti Normativi

- UNI CEI EN ISO/IEC 27001:2024 - Sistemi di gestione per la sicurezza delle informazioni — Requisiti.
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (Regolamento Generale sulla Protezione dei Dati - GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Termini e Definizioni

- **Riservatezza**: La proprietà che le informazioni non siano rese disponibili o divulgate a persone, entità o processi non autorizzati.
- **Integrità**: La proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

Ruoli e Responsabilità

- **Direttore generale**: Approva la politica di sicurezza delle informazioni e garantisce la disponibilità delle risorse necessarie per la sua efficace implementazione, supervisionando il rischio informatico e la conformità normativa.
- **C.d.A.**: Definisce la visione strategica complessiva per la sicurezza delle informazioni, allineandola agli obiettivi aziendali.
- **Ufficio legale**: Supervisiona la conformità della politica e della sua applicazione ai requisiti legali, statutari e normativi vigenti.
- **Responsabile SGI**: Gestisce, pubblica e revisiona la politica di sicurezza. Coordina il processo di valutazione e trattamento del rischio, gestisce gli incidenti di sicurezza e supervisiona l'implementazione dei controlli per garantire la conformità allo standard ISO/IEC 27001 e ISO/IEC 9001.
- **Responsabile personale e comunicazione**: Assicura che la politica sia comunicata a tutto il personale e alle parti interessate rilevanti, garantendone la comprensione e promuovendo la formazione in materia di sicurezza.
- **CTO**: Implementa e gestisce i controlli tecnici necessari per far rispettare le politiche di sicurezza, inclusa la protezione delle postazioni di lavoro e l'uso accettabile delle risorse aziendali.

Obiettivi di sicurezza delle informazioni

Gep Informatica si impegna a proteggere i propri asset informativi, quelli dei clienti e delle parti interessate per garantire la continuità del business, minimizzare i rischi e massimizzare le opportunità. La sicurezza delle informazioni è un fattore strategico per il successo dell'azienda, essenziale per la progettazione, lo sviluppo, l'implementazione e il supporto di soluzioni software per la logistica.

Il Direttore Generale e il C.d.A., in linea con gli indirizzi strategici definiti nella "POL Politica del sistema di gestione", stabiliscono i seguenti obiettivi generali per la sicurezza delle informazioni:

- **Riservatezza**: Assicurare che le informazioni, inclusa la proprietà intellettuale e i dati dei clienti, siano accessibili solo al personale autorizzato. La protezione delle informazioni è un obbligo per tutto il personale, come dettagliato nella "POL Politica di classificazione ed etichettatura delle informazioni".
- **Integrità**: Mantenere l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione, proteggendo gli asset da modifiche, cancellazioni o corruzioni non autorizzate durante l'intero ciclo di vita.
- **Disponibilità**: Garantire che il personale autorizzato abbia accesso alle informazioni e agli asset associati quando necessario, in conformità con gli accordi contrattuali e le esigenze operative.
- **Conformità**: Rispettare tutti i requisiti legali, statutari, normativi e contrattuali applicabili alla sicurezza delle informazioni, con la supervisione dell'Ufficio legale e del Responsabile del SGI.
- **Miglioramento Continuo**: Promuovere una cultura della sicurezza e migliorare continuamente l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) attraverso riesami periodici e l'analisi delle performance.

Il raggiungimento di tali obiettivi è pianificato, monitorato e misurato secondo quanto stabilito nella procedura "PRO Obiettivi e pianificazione per il loro raggiungimento".

Principi fondamentali di sicurezza delle informazioni

Impegno della Direzione e Governance

Il Direttore Generale approva la presente politica e si impegna a fornire le risorse necessarie per la sua efficace implementazione. Il Responsabile del SGI è responsabile della gestione, pubblicazione, comunicazione e revisione periodica di questa e di tutte le politiche specifiche del sistema di gestione integrato. La presente politica deve essere riesaminata con cadenza almeno annuale, o a seguito di cambiamenti significativi, come descritto nella "PRO Gestione riesame della direzione". Il Responsabile del personale e comunicazioni deve assicurare che tutto il personale e le parti interessate rilevanti ricevano comunicazione della politica e ne accusino la ricezione e comprensione, come previsto dal "Codice di condotta".

Approccio Basato sul Rischio

Tutte le decisioni in materia di sicurezza delle informazioni devono basarsi su un processo continuo di valutazione e trattamento del rischio. Il Responsabile del SGI ha la responsabilità di coordinare questo processo, assicurando che le misure di controllo siano

proporzionate alle minacce identificate, in accordo con la "PRO Procedura di gestione dei rischi".

Responsabilità Condivisa

La sicurezza delle informazioni è una responsabilità di tutto il personale di GepInformatica, dei collaboratori e delle terze parti. Ogni individuo è tenuto a proteggere gli asset informativi a cui ha accesso. Le responsabilità specifiche sono definite e assegnate formalmente nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e integrate nel mansionario aziendale.

Uso Accettabile delle Risorse

Tutti gli asset aziendali, inclusi hardware, software, informazioni, reti e sistemi, devono essere utilizzati esclusivamente per scopi lavorativi autorizzati e in conformità con le normative vigenti e il "Codice di condotta". È severamente vietato l'uso di tali risorse per attività illegali, inappropriate o che possano compromettere la sicurezza dell'organizzazione. Il CTO deve implementare i controlli tecnici necessari per monitorare e far rispettare tale principio. Le regole di utilizzo sono dettagliate nella "POL Politica di sicurezza operativa".

Sicurezza delle postazioni di lavoro (Clear Desk e Clear Screen)

Tutto il personale è tenuto a proteggere le informazioni sensibili presso la propria postazione di lavoro, sia in sede che in modalità di lavoro agile.

- **Clear Desk**: I documenti cartacei e i supporti di memorizzazione rimovibili contenenti informazioni classificate come riservate o di livello superiore devono essere custoditi in armadi o classificatori chiusi a chiave quando la postazione è incustodita.
- **Clear Screen**: Tutti i dispositivi informatici devono essere configurati con un blocco schermo automatico che si attivi dopo un breve periodo di inattività, richiedendo l'autenticazione per riprendere la sessione. Il CTO ha l'obbligo di implementare tale misura su tutti i dispositivi aziendali.

Sicurezza degli Asset Fuori Sede

Gli asset aziendali utilizzati al di fuori delle sedi di Gep Informatica, inclusi i dispositivi forniti per il lavoro agile, devono essere protetti con la massima diligenza. Il personale che opera da remoto ha la responsabilità di:

- Utilizzare gli strumenti forniti esclusivamente per scopi lavorativi.
- Garantire la protezione fisica dei dispositivi da furto, smarrimento o danneggiamento.
- Adottare misure idonee a prevenire l'accesso non autorizzato a informazioni aziendali, evitando di operare da luoghi pubblici non sicuri.
- Segnalare immediatamente al proprio responsabile e attivare le procedure aziendali in caso di furto, smarrimento o guasto delle attrezzature. Le condizioni specifiche sono definite negli accordi individuali di lavoro agile.

Segnalazione degli Eventi di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento, debolezza o anomalia di sicurezza delle informazioni osservata o sospetta. Le segnalazioni devono essere effettuate attraverso i canali ufficiali e secondo le modalità descritte nella "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni". Il Responsabile del SGI è responsabile della gestione degli incidenti segnalati, che vengono tracciati tramite il "MOD Registro degli incidenti di sicurezza delle informazioni".

Archiviazione e aggiornamenti

Il presente documento è gestito e archiviato secondo le procedure del sistema di gestione documentale aziendale. Viene sottoposto a revisione con cadenza almeno annuale, o ogniqualvolta si verifichino cambiamenti significativi nel contesto aziendale, normativo o tecnologico, sotto la responsabilità del Responsabile del SGI e con l'approvazione del Direttore Generale.

Documenti di riferimento

- Codice di condotta
- POL Politica del sistema di gestione
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Gestione riesame della direzione
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- MOD Registro degli incidenti di sicurezza delle informazioni