POL Politica di sicurezza delle informazioni

Nome della società	JEF SRL
Data di entrata in vigore	03/10/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	03/10/2025	-- N/D --	Salvatore La Porta	Luca Postacchini

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 stabilisce gli obiettivi strategici e i principi fondamentali per la gestione della sicurezza delle informazioni all'interno di JEF SRL. Il suo scopo è proteggere gli asset informativi dell'organizzazione e dei suoi clienti da ogni tipo di minaccia, garantendo la riservatezza, l'integrità e la disponibilità dei dati. Questo documento si applica a tutti i dipendenti, processi, attività e risorse tecnologiche che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità con gli standard di riferimento.

Riferimenti Normativi

- ISO/IEC 27001
- ISO/IEC 27017
- Regolamento Generale sulla Protezione dei Dati (GDPR)

Termini e Definizioni

- **Riservatezza** : Proprietà secondo cui le informazioni non vengono rese disponibili o divulgate a persone, entità o processi non autorizzati.
- **Integrità** : Proprietà di salvaguardare l'accuratezza e la completezza degli asset.
- **Disponibilità** : Proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** : Un insieme di politiche, procedure, linee guida e risorse associate, gestite collettivamente da un'organizzazione, per proteggere i suoi asset informativi.

Ruoli e Responsabilità

- **Top Management** : Supervisiona l'implementazione e il miglioramento continuo del SGSI, garantisce che tutto il personale sia consapevole e rispetti le politiche di sicurezza, approva il budget per le iniziative di sicurezza e gestisce gli incidenti rilevanti per assicurare la continuità operativa.
- **Organo di governo** : Assicura l'istituzione e il mantenimento di un SGSI efficace, assegna le risorse necessarie per la mitigazione dei rischi, approva le politiche e gli obiettivi di sicurezza e promuove una cultura della sicurezza all'interno dell'organizzazione.
- **Responsabile del sistema di gestione (RSGSI)** : Guida l'implementazione e il mantenimento del SGSI, conduce le valutazioni dei rischi, supervisiona lo sviluppo e l'applicazione delle politiche di sicurezza e coordina gli audit per garantire il miglioramento continuo.

- **Responsabile digitalizzazione e informatizzazione (sviluppo IT)** : Definisce e applica pratiche di sviluppo sicuro, supervisiona la sicurezza delle applicazioni cloud e dei servizi di hosting in conformità con la norma ISO 27017, ed è responsabile della gestione degli incidenti di sicurezza relativi ai sistemi e alle applicazioni IT.

Obiettivi di sicurezza delle informazioni

Il Top Management di JEF SRL si impegna a proteggere gli asset informativi dell'organizzazione e dei suoi clienti da tutte le minacce, interne o esterne, deliberate o accidentali. La presente politica stabilisce gli obiettivi strategici per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità con gli standard ISO/IEC 27001 e ISO/IEC 27017.

Gli obiettivi primari sono:

- **Garantire la Riservatezza, Integrità e Disponibilità (RID)** delle informazioni gestite, prevenendo accessi non autorizzati, modifiche improprie o indisponibilità dei servizi.
- **Assicurare la Conformità** a tutti i requisiti legali, normativi (incluso il GDPR), e contrattuali applicabili alle attività di JEF SRL.
- **Stabilire un quadro di riferimento per la gestione del rischio** informatico, che consenta di identificare, valutare e trattare i rischi in modo sistematico e coerente con gli obiettivi di business, come definito nella "PRO Procedura di gestione dei rischi".
- **Promuovere una cultura della sicurezza** in tutta l'organizzazione, in cui ogni membro del personale comprende il proprio ruolo e le proprie responsabilità nella protezione degli asset informativi.
- **Perseguire il miglioramento continuo** dell'efficacia del SGSI attraverso la definizione e il monitoraggio di obiettivi misurabili, come descritto nella procedura "PRO Obiettivi e pianificazione per il loro raggiungimento".

L'Organo di governo e il Top Management devono approvare la presente politica e garantire l'allocazione delle risorse necessarie per la sua attuazione. Il Responsabile del sistema di gestione (RSGSI) ha la responsabilità di implementare, mantenere e supervisionare il SGSI.

Principi fondamentali di sicurezza delle informazioni

Gestione e Revisione della Politica

La presente politica è il documento di vertice del SGSI. Il Top Management deve approvarla formalmente. Il Responsabile del sistema di gestione (RSGSI) deve assicurare che sia pubblicata, comunicata a tutto il personale e alle parti interessate rilevanti e che ne venga compreso il contenuto. La politica deve essere riesaminata almeno una volta all'anno, o a seguito di cambiamenti significativi, nell'ambito del processo descritto nella "PRO Gestione riesame della direzione", per garantirne la continua idoneità, adeguatezza ed efficacia.

Responsabilità Condivisa per la Sicurezza

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge l'intera organizzazione. Sebbene il Top Management detenga la responsabilità ultima, ogni individuo è tenuto a contribuire attivamente alla protezione degli asset informativi. Le responsabilità specifiche sono formalmente definite e assegnate nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e integrate nei mansionari aziendali.

Sicurezza nell'Uso e nella Fornitura di Servizi Cloud

JEF SRL, agendo sia come cliente sia come fornitore di servizi cloud, adotta principi specifici per la gestione della sicurezza in tali ambienti, come dettagliato nella "POL Politica di sicurezza del cloud".

- **JEF SRL come Cliente di Servizi Cloud** : Nell'utilizzo di servizi cloud esterni (es. AWS, Aruba), il Responsabile digitalizzazione e informatizzazione (sviluppo it) deve valutare e gestire i rischi derivanti, considerando l'accesso del fornitore ai dati, l'isolamento in ambienti multi-tenant e la localizzazione geografica dei dati.
- **JEF SRL come Fornitore di Servizi Cloud** : Nella fornitura di servizi di hosting e applicazioni cloud, il Responsabile digitalizzazione e informatizzazione (sviluppo it) deve implementare controlli robusti per garantire l'isolamento tra i clienti, applicare un'autenticazione forte per l'accesso amministrativo, gestire in modo sicuro il ciclo di vita degli account dei clienti e proteggere l'infrastruttura di virtualizzazione, in accordo con la "PRO Procedura di sviluppo sicuro".

Uso Accettabile delle Risorse

Tutto il personale deve utilizzare le informazioni e le risorse aziendali, inclusi sistemi, reti e dispositivi, esclusivamente per scopi lavorativi autorizzati e in modo responsabile. Le regole per l'uso accettabile sono stabilite nel "Codice di condotta" e nella "POL Politica di sicurezza operativa".

Protezione degli Asset Aziendali

Tutti gli asset informativi devono essere protetti in base al loro valore e alla loro classificazione.

- **Classificazione delle Informazioni** : Le informazioni devono essere classificate in base alla loro sensibilità, criticità e ai requisiti legali, come stabilito nella "POL Politica di classificazione ed etichettatura delle informazioni".
- **Asset Fuori Sede** : Gli asset aziendali utilizzati al di fuori delle sedi fisiche, come i laptop per il lavoro da remoto, devono essere protetti da furto, perdita, danno e accesso non autorizzato. L'assegnazione di tali beni è formalmente tracciata tramite il "MOD Modulo di assegnazione dei beni".
- **Scrivania Pulita e Schermo Pulito** : Il personale deve assicurare che documenti cartacei e supporti di memorizzazione contenenti informazioni sensibili non siano lasciati

incustoditi. Le postazioni di lavoro devono essere bloccate quando non presidiate e configurate per l'attivazione automatica del blocco schermo dopo un breve periodo di inattività.

Sicurezza nel Lavoro da Remoto e sui Dispositivi Mobili

L'accesso remoto alle risorse aziendali è consentito solo attraverso canali sicuri e autorizzati, come la VPN aziendale. Il personale che opera in modalità di lavoro da remoto deve utilizzare esclusivamente dispositivi forniti e configurati dall'azienda, dotati di controlli di sicurezza adeguati come antivirus e firewall, che non devono essere disattivati o modificati. Ulteriori dettagli sono specificati nella "POL Politica di sicurezza operativa".

Segnalazione e Gestione degli Eventi di Sicurezza

Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni, debolezza o incidente sospetto, utilizzando i canali definiti. Il Responsabile del sistema di gestione (RSGSI) deve garantire che ogni segnalazione sia gestita secondo la "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni" e registrata nel "MOD Registro degli incidenti di sicurezza delle informazioni".

Archiviazione e Aggiornamenti

Questo documento è gestito in formato controllato all'interno del sistema documentale aziendale. Viene riesaminato con cadenza almeno annuale, e ogni qualvolta si verifichino cambiamenti significativi, dal Responsabile del sistema di gestione (RSGSI) per garantirne la continua idoneità. Ogni aggiornamento è approvato dal Top Management.

Documenti di Riferimento

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