

POL Politica di sicurezza delle informazioni

Nome della società	EXA Consulting
Data di entrata in vigore	07/05/2025

Storia della versione

Versione	Data	Descrizione	Autore	Approvato da
1	07/05/2025	-- N / D --	Marta Santi	Giuseppe Settanni

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
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Governance e Impegno della Direzione
- Responsabilità per la Sicurezza
- Uso Accettabile delle Risorse
- Protezione degli Asset
- Segnalazione degli Eventi di Sicurezza
- Archiviazione e aggiornamenti
- Documenti di riferimento

Campo di applicazione

La presente politica definisce i principi, gli obiettivi e le responsabilità per la gestione della sicurezza delle informazioni all'interno di EXA Consulting. Il suo scopo è proteggere il patrimonio informativo aziendale da ogni minaccia, interna o esterna, intenzionale o accidentale, al fine di garantire la continuità operativa, minimizzare i rischi e assicurare la conformità ai requisiti legali, normativi e contrattuali. Questo documento si applica a tutte le informazioni gestite da EXA Consulting, indipendentemente dal formato, e a tutto il personale, ai collaboratori e alle terze parti che hanno accesso agli asset informativi dell'organizzazione.

Riferimenti normativi

- **ISO/IEC 27001:2022:** Sicurezza delle informazioni, cybersecurity e protezione della privacy — Sistemi di gestione per la sicurezza delle informazioni - Requisiti.
- **Regolamento (UE) 2016/679 (GDPR):** Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- **D.Lgs. 30 giugno 2003, n. 196:** Codice in materia di protezione dei dati personali e successive modifiche e integrazioni.

Termini e definizioni

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

Ruoli e responsabilità

- **Top Management:** Detiene la responsabilità ultima per l'efficacia del Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Assicura la disponibilità delle risorse necessarie, approva le politiche di sicurezza, promuove una cultura orientata alla protezione dei dati e supervisiona la gestione dei rischi e la conformità normativa.
- **Responsabile del sistema di gestione integrato (RSGI):** Ha la responsabilità di implementare, gestire e mantenere il SGSI in conformità con la presente politica. Supervisiona l'applicazione dei controlli di sicurezza, coordina le attività di valutazione dei rischi, gestisce la documentazione del sistema e funge da punto di contatto principale per la segnalazione e la gestione degli incidenti di sicurezza.

Obiettivi di sicurezza delle informazioni

EXA Consulting si impegna a proteggere il proprio patrimonio informativo per garantire la continuità del business, minimizzare i rischi e massimizzare le opportunità, in linea con la propria missione di partner per pubbliche amministrazioni e imprese. Gli obiettivi strategici del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), conformi allo standard ISO/IEC 27001, sono:

- **Riservatezza:** Garantire che le informazioni siano accessibili solo al personale autorizzato e protette da divulgazioni indebite. La protezione dei dati dei clienti e dei segreti commerciali è un fattore critico per mantenere la fiducia del mercato.
- **Integrità:** Salvaguardare l'accuratezza, la completezza e la validità delle informazioni e dei metodi di elaborazione, per assicurare che le decisioni si basino su dati affidabili e non alterati.
- **Disponibilità:** Assicurare che il personale autorizzato abbia accesso alle informazioni e alle risorse associate quando necessario, proteggendo i processi operativi da interruzioni impreviste.
- **Conformità:** Rispettare tutti i requisiti legali, normativi e contrattuali applicabili alla sicurezza delle informazioni e alla protezione dei dati personali.
- **Miglioramento Continuo:** Valutare e migliorare costantemente l'efficacia del SGSI attraverso il monitoraggio delle prestazioni, la gestione dei rischi e il riesame periodico.

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

Principi fondamentali di sicurezza delle informazioni

Governance e Impegno della Direzione

Il Top Management di EXA Consulting dimostra leadership e impegno attivo verso la sicurezza delle informazioni, assicurando che la presente politica e gli obiettivi di sicurezza siano compatibili con gli indirizzi strategici dell'organizzazione.

Il Top Management approva formalmente la presente politica e le politiche specifiche ad essa collegate.

Il Responsabile del sistema di gestione integrato (RSGI) deve garantire che questa politica sia comunicata a tutto il personale e alle parti interessate rilevanti, mantenuta come informazione documentata e riesaminata a intervalli pianificati o a seguito di cambiamenti significativi, in accordo con le procedure "PRO Procedura di gestione delle informazioni documentate" e "PRO Gestione riesame della direzione".

Tutto il personale è tenuto a prendere visione e confermare la comprensione dei principi qui enunciati.

Responsabilità per la Sicurezza

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge tutto il personale di EXA Consulting. Le responsabilità specifiche sono formalmente definite e assegnate nel documento "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni" e integrate nel mansionario aziendale.

- Il Top Management detiene la responsabilità ultima per l'efficacia del SGSI e per l'allocazione delle risorse necessarie.
- Il Responsabile del sistema di gestione integrato (RSGI) ha la responsabilità di supervisionare l'implementazione e il funzionamento dei controlli di sicurezza.
- Tutto il personale, inclusi consulenti e collaboratori, deve rispettare le politiche e le procedure di sicurezza e contribuire attivamente alla protezione degli asset informativi.

Uso Accettabile delle Risorse

Tutti gli asset informativi, i sistemi e le reti di EXA Consulting devono essere utilizzati esclusivamente per scopi aziendali autorizzati e in modo responsabile.

- L'accesso alle informazioni è regolato dal principio del minimo privilegio e della necessità operativa ("need-to-know"). Le autorizzazioni sono documentate nel "Registro degli utenti autorizzati all'uso delle informazioni".
- È vietato utilizzare le risorse aziendali per attività illegali, non etiche o non autorizzate.
- Il personale deve aderire alle regole di comportamento definite nel "Codice di condotta" e nelle policy specifiche, come la "POL Politica di classificazione ed etichettatura delle informazioni".

Protezione degli Asset

Tutti gli asset informativi, sia fisici che digitali, devono essere protetti in base alla loro classificazione e al loro valore per l'organizzazione.

- **Scrivania Pulita e Schermo Pulito:** Il personale deve assicurare che le informazioni sensibili su supporto cartaceo o su supporti di memorizzazione rimovibili non siano lasciate incustodite in aree accessibili. Le postazioni di lavoro devono essere bloccate quando non presidiate e i dispositivi devono essere configurati per il blocco automatico dello schermo dopo un breve periodo di inattività (5 minuti se collegati alla rete elettrica, 3 minuti se a batteria). Ulteriori dettagli sono specificati nella "PRO Procedura di sicurezza fisica e ambientale".
- **Sicurezza degli Asset Fuori Sede:** Gli asset utilizzati al di fuori delle sedi aziendali, come laptop e dispositivi mobili, devono essere protetti con un livello di sicurezza equivalente a quello garantito in ufficio. Il personale che opera in modalità di lavoro da remoto deve seguire scrupolosamente le direttive aziendali, che includono l'uso di connessioni sicure (VPN con autenticazione a più fattori), la protezione delle reti Wi-Fi domestiche e il mantenimento di software di sicurezza (antivirus e firewall) sempre attivi e aggiornati. È severamente vietato disattivare o alterare i controlli di sicurezza installati sui dispositivi aziendali. La gestione di tali asset è normata dalla "PRO Procedura di configurazione, gestione e smaltimento degli asset".

Segnalazione degli Eventi di Sicurezza

Tutto il personale ha il dovere di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni osservato o sospetto, incluse debolezze, minacce o violazioni delle policy.

- Le segnalazioni devono essere effettuate attraverso i canali designati e comunicate al Responsabile del sistema di gestione integrato (RSGI).
- La gestione degli eventi e la risposta agli incidenti sono disciplinate dalla "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni" e dalla "PRO Procedura di gestione dei rilievi ed eventi", al fine di contenere i danni e facilitare il ripristino.

Archiviazione e aggiornamenti

La presente politica è un documento controllato, gestito all'interno del Sistema di Gestione della Sicurezza delle Informazioni. Viene riesaminata con cadenza almeno annuale e aggiornata ogni qualvolta si verificano cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, sotto la supervisione del Responsabile del sistema di gestione integrato (RSGI) e con l'approvazione del Top Management.

Documenti di riferimento

- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di gestione delle informazioni documentate
- PRO Gestione riesame della direzione
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- Registro degli utenti autorizzati all'uso delle informazioni
- Codice di condotta
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di sicurezza fisica e ambientale
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rilievi ed eventi