Sistema di gestione per la sicurezza delle informazioni

Politica della sicurezza delle informazioni

Redatto da	Revisionato da	Approvato da
Daniele Cerbarano	Emanuela Selogni	Monica Sordi
Data 4/07/2025	Data 4/07/2025	Data 28/07/2025
Firma	Firma	Firma

Note di revisione		
Motivo revisione	Numero	Data
Prima Emissione	0	12/06/2024
Revisione Politica SGI short	1	4/07/2025

Politica per la Sicurezza delle Informazioni – Sintesi

Introduzione

GMM considera la **sicurezza delle informazioni** un elemento strategico e imprescindibile per il raggiungimento dei propri obiettivi di business, soprattutto in un contesto altamente digitalizzato, normato e orientato all'innovazione tecnologica. La protezione dei dati è essenziale per garantire la continuità operativa, la fiducia di clienti e partner, e la conformità ai requisiti legali e contrattuali.

In coerenza con i requisiti della norma **ISO/IEC 27001**, la Società ha adottato un **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** finalizzato a proteggere tutte le informazioni aziendali – digitali, cartacee, vocali – da minacce interne ed esterne.

Principi fondamentali

La politica si fonda sul rispetto del principio **RID**, ovvero:

- **Riservatezza**: garantire che le informazioni siano accessibili solo a soggetti autorizzati;
- **Integrità**: garantire che le informazioni siano accurate e non modificate in modo non autorizzato;
- **Disponibilità**: garantire che le informazioni siano accessibili nel momento in cui sono necessarie.

In aggiunta, GMM si impegna a garantire la **conformità normativa**, inclusa la protezione dei dati personali secondo il Regolamento (UE) 2016/679 (GDPR).

Obiettivi

Attraverso la presente politica, la Società intende:

- Migliorare il governo della sicurezza informatica;
- Prevenire la perdita di dati critici e capitale informativo;
- Promuovere la consapevolezza interna sul rischio ICT;
- Garantire un vantaggio competitivo attraverso una gestione sicura ed efficiente dei sistemi informativi;
- Rispondere efficacemente agli incidenti informatici e garantirne il tracciamento;
- Integrare la sicurezza delle informazioni nei processi di sviluppo, manutenzione e innovazione tecnologica.

Ambito di applicazione

La politica si applica a:

- Tutto il personale interno ed esterno (dipendenti, collaboratori, fornitori);
- Tutti i dati trattati da GMM o in sua gestione;

- Tutti i sistemi informatici, infrastrutture e applicazioni aziendali, comprese le attività in cloud e in outsourcing.

Approccio organizzativo e metodologico

Il SGSI è sviluppato secondo il ciclo di miglioramento continuo **Plan-Do-Check-Act (PDCA)**. Vengono definite e mantenute procedure per:

- Analisi e trattamento dei rischi ICT;
- Gestione degli accessi logici secondo i principi del "privilegio minimo" e del "bisogno di sapere";
- Classificazione, etichettatura e protezione delle informazioni;
- Gestione degli asset informatici e delle vulnerabilità;
- Controllo degli accessi fisici e sicurezza dei locali;
- Gestione della continuità operativa e risposta agli incidenti di sicurezza.

Ruoli e responsabilità

Le responsabilità sono chiaramente definite a tutti i livelli organizzativi:

- **Consiglio di Amministrazione**: approva la strategia e la politica della sicurezza;
- **Amministratore Delegato**: supervisiona l'applicazione della politica;
- **Information Security & IT Compliance**: definisce le regole di sicurezza, analizza i rischi, gestisce gli incidenti e assicura la compliance normativa;
- **IT**: gestisce l'infrastruttura tecnologica e monitora la sicurezza dei sistemi;
- **Tutti i dipendenti**: sono responsabili della protezione delle informazioni secondo le regole aziendali.

Impegni della Direzione

La Direzione di GMM si impegna a:

- Fornire le risorse necessarie per mantenere efficace il SGSI;
- Garantire la diffusione della cultura della sicurezza tra tutto il personale;
- Monitorare e migliorare continuamente le misure tecniche e organizzative;
- Assicurare che la sicurezza sia integrata in ogni processo aziendale, incluse le attività di sviluppo software, gestione delle terze parti e continuità operativa.