1. Registro rischi sicurezza informazioni

Mappa di processo - Registro rischi sicurezza informazioni

Diagramma di processo: Contesto -> Identificazione rischi -> Valutazione -> Azione di trattamento -> Verifica efficacia.

Registro rischi sicurezza informazioni

Il registro rischi sicurezza informazioni rappresenta uno strumento fondamentale per GMK SISTEMI S.R.L. al fine di identificare, valutare, monitorare e mitigare i rischi che possono compromettere la riservatezza, integrità e disponibilità delle informazioni gestite nell'ambito delle attività di commercio all'ingrosso, assistenza tecnica, progettazione software e formazione del personale. Questo documento è conforme ai requisiti di ISO/IEC 27001 (clausole 6, 8 e 9) e integra le prescrizioni di ISO 9001 relative alla gestione del rischio e al miglioramento continuo del sistema di gestione per la qualità.

1. Scopo e campo di applicazione

Il registro ha lo scopo di fornire una visione strutturata e aggiornata dei rischi inerenti alla sicurezza delle informazioni, con particolare attenzione ai dati trattati nel sito web aziendale e nei sistemi informatici utilizzati nei processi di GMK SISTEMI S.R.L. Il documento copre tutte le informazioni digitali e cartacee rilevanti per il mantenimento della qualità e della sicurezza, in linea con il campo di applicazione definito nel sistema di gestione.

2. Responsabilità

La responsabilità primaria per la gestione e l'aggiornamento del registro rischi è attribuita al Responsabile della Sicurezza delle Informazioni (RSI), che opera in coordinamento con il Responsabile Qualità e il Responsabile IT. Il RSI garantisce che le valutazioni siano condotte con cadenza periodica e in seguito a modifiche significative nei processi o nell'infrastruttura tecnologica. La Direzione di GMK SISTEMI S.R.L. approva le strategie di trattamento dei rischi e verifica l'efficacia delle azioni correttive e preventive.

3. Metodologia di identificazione e valutazione dei rischi

L'identificazione dei rischi si basa sull'analisi dei processi chiave, delle risorse informative e delle minacce interne ed esterne, con particolare attenzione ai rischi specifici del settore ICT e del commercio all'ingrosso di apparecchiature informatiche. La valutazione considera la probabilità di accadimento e l'impatto potenziale, utilizzando criteri quantitativi e qualitativi definiti nel piano di gestione del rischio. Le valutazioni sono documentate nel registro e aggiornate in seguito a eventi di sicurezza, audit interni o modifiche normative.

4. Trattamento e monitoraggio dei rischi

Per ogni rischio identificato, il registro riporta le misure di controllo adottate o pianificate, quali l'implementazione di controlli di accesso, backup regolari, formazione del personale e aggiornamenti software. Il monitoraggio continuo è assicurato tramite indicatori di performance specifici, come il numero di incidenti di sicurezza rilevati, tempi di risposta e percentuale di conformità alle procedure. Le azioni di mitigazione sono integrate nel piano di miglioramento continuo e verificate durante le attività di audit interne (ISO/IEC 27001 clausola 9).

5. Interfacce con altri processi e documenti

Il registro rischi è strettamente collegato al sistema di gestione della qualità e sicurezza delle informazioni, interfacciandosi con il piano di formazione del personale, il registro delle non conformità, il piano di audit e il sistema di gestione documentale digitale. Le modifiche al registro sono soggette a controllo documentale, con versionamento e tracciabilità delle revisioni, in conformità alle procedure interne e ai requisiti ISO 9001 (clausola 7.5).

[Placeholder per diagramma di processo: Gestione integrata del rischio sicurezza informazioni - identificazione, valutazione, trattamento, monitoraggio e revisione]

6. Evidenze e registrazioni

Tipo di evidenza |

Descrizione |

Responsabile |

Conservazione |

Riferimento ISO |

Registro rischi aggiornato |

Documento contenente l'elenco dei rischi identificati, valutazioni e misure di controllo |

RSI |

Archivio digitale protetto, minimo 5 anni |

ISO/IEC 27001 clausola 6.1.2 |

Report audit interni |

Verifiche periodiche sull'efficacia delle misure di sicurezza e gestione del rischio |

Responsabile Qualità |

Archivio digitale, minimo 3 anni |

ISO 9001 clausola 9.2 |

Registro non conformità e azioni correttive |

Documentazione di eventi di sicurezza e relative azioni di miglioramento |

RSI / Responsabile Qualità |

Archivio digitale, minimo 5 anni |

ISO/IEC 27001 clausola 10 |

7. Indicatori di performance e audit

Per garantire l'efficacia del sistema di gestione della sicurezza delle informazioni, GMK SISTEMI S.R.L. utilizza indicatori quali la frequenza di aggiornamento del registro rischi, il numero di incidenti di sicurezza rilevati, il tempo medio di risoluzione degli eventi e la percentuale di personale formato sulle procedure di sicurezza. Tali indicatori sono oggetto di revisione durante gli audit interni e le riunioni di riesame della direzione, in linea con le clausole 9 e 10 di ISO/IEC 27001 e ISO 9001.

8. Conformità normativa e riferimenti esterni

Le attività di gestione del rischio sicurezza informazioni sono svolte nel rispetto delle normative vigenti in materia di protezione dei dati personali e sicurezza informatica, quali il Regolamento UE 2016/679 (GDPR) e le disposizioni nazionali applicabili. GMK SISTEMI S.R.L. mantiene aggiornato il registro anche in funzione di eventuali evoluzioni legislative e best practice del settore ICT, garantendo così la conformità e la riduzione dei rischi legali e reputazionali.