1. Procedura gestione incidenti di sicurezza informatica

Mappa di processo - Procedura gestione incidenti di sicurezza informatica

Diagramma di processo: Input -> Responsabile processo -> Controlli operativi -> Output -> KPI e miglioramento.

Procedura gestione incidenti di sicurezza informatica

La presente procedura definisce le modalità operative adottate da GMK SISTEMI S.R.L. per la gestione tempestiva, efficace e documentata degli incidenti di sicurezza informatica, in conformità ai requisiti di ISO/IEC 27001 (clausole 6, 7, 8 e 10) e integrando le buone pratiche di gestione della qualità secondo ISO 9001 (clausole 8.5 e 10). L'obiettivo è garantire la protezione della riservatezza, integrità e disponibilità delle informazioni trattate, minimizzando impatti operativi e reputazionali nel contesto del commercio all'ingrosso e dei servizi informatici erogati dall'azienda.

1. Ambito e campo di applicazione

La procedura si applica a tutti i sistemi informatici, applicazioni, infrastrutture di rete e dati gestiti da GMK SISTEMI S.R.L., inclusi quelli utilizzati per la progettazione software, assistenza tecnica e formazione del personale. Sono inclusi gli incidenti rilevati internamente o segnalati da terze parti, con particolare attenzione agli eventi che possono compromettere la continuità operativa o la conformità normativa.

2. Definizioni e classificazione degli incidenti

Un incidente di sicurezza informatica è qualsiasi evento che comprometta o possa compromettere la sicurezza delle informazioni o dei sistemi aziendali. Gli incidenti sono classificati in base alla gravità e all'impatto potenziale, secondo la seguente scala:

• Critico: compromissione grave con impatto diretto su servizi essenziali o dati sensibili.

• Alto: evento che può causare interruzioni significative o perdita di dati non critici.

• Medio: anomalie o tentativi di accesso non autorizzato senza impatti immediati.

• Basso: eventi di natura informativa o tentativi bloccati senza conseguenze.

3. Ruoli e responsabilità

La responsabilità primaria della gestione degli incidenti è assegnata al Responsabile della Sicurezza delle Informazioni (RSI), che coordina l'identificazione, la valutazione, la risposta e la comunicazione degli eventi. Il personale tecnico e amministrativo è tenuto a segnalare tempestivamente qualsiasi anomalia o sospetto incidente al RSI. La Direzione Aziendale garantisce le risorse necessarie per l'attuazione della procedura e la formazione continua del personale.

4. Processo operativo di gestione degli incidenti

La gestione degli incidenti si articola nelle seguenti fasi:

• Rilevazione e segnalazione: ogni dipendente o sistema automatizzato può identificare un potenziale incidente e deve comunicarlo immediatamente al RSI tramite il modulo di segnalazione dedicato.

• Registrazione: l'incidente viene documentato nel registro incidenti con data, ora, descrizione, classificazione e soggetto segnalante.

• Valutazione e prioritizzazione: il RSI valuta la gravità e l'impatto, definendo le azioni di contenimento e mitigazione.

• Risposta e risoluzione: vengono attivate le misure tecniche e organizzative per isolare, correggere e prevenire la diffusione dell'incidente.

• Comunicazione: se necessario, si informa la Direzione e gli stakeholder coinvolti, rispettando la riservatezza e le normative vigenti.

• Analisi post-incidente: si esegue una revisione per identificare cause radice, migliorare controlli e aggiornare procedure.

5. Documentazione e registrazioni

Tutte le attività correlate agli incidenti sono tracciate mediante documenti controllati, inclusi:

• Modulo di segnalazione incidente (formato digitale controllato);

• Registro degli incidenti di sicurezza informatica;

• Report di analisi e azioni correttive;

• Verbali di riunioni di revisione post-incidente.

Questi documenti sono conservati secondo le politiche aziendali di gestione documentale, garantendo integrità, accessibilità e riservatezza, in linea con le clausole 7.5 di ISO 9001 e 7.5 di ISO/IEC 27001.

6. Indicatori di performance e monitoraggio

Per valutare l'efficacia della procedura, GMK SISTEMI S.R.L. monitora i seguenti indicatori:

Indicatore |

Descrizione |

Obiettivo |

Frequenza di monitoraggio |

Tempo medio di risposta |

Durata media tra la segnalazione e l'avvio delle azioni di contenimento |

< 2 ore |

Mensile |

Numero di incidenti risolti |

Percentuale di incidenti chiusi con successo entro i tempi stabiliti |

> 95% |

Trimestrale |

Incidenti ricorrenti |

Frequenza di incidenti simili ripetuti nello stesso periodo |

Riduzione continua |

Annuale |

7. Audit e miglioramento continuo

La procedura è soggetta a verifiche interne periodiche integrate negli audit del sistema di gestione qualità e sicurezza delle informazioni, come previsto dalle clausole 9 di ISO 9001 e 9 di ISO/IEC 27001. Gli audit valutano la conformità, l'efficacia delle azioni intraprese e l'adeguatezza delle risorse. Le non conformità rilevate generano azioni correttive documentate e monitorate per garantire il miglioramento continuo del processo.

8. Interfacce con altri processi aziendali

La gestione degli incidenti interagisce strettamente con i processi di gestione del rischio, manutenzione IT, formazione del personale e comunicazione interna. La collaborazione tra i responsabili di processo assicura un approccio integrato e coerente, in linea con la politica aziendale e gli obiettivi di sicurezza e qualità.

9. Riferimenti normativi e regolamentari

La procedura tiene conto delle disposizioni vigenti in materia di protezione dei dati personali e sicurezza informatica, tra cui il Regolamento UE 2016/679 (GDPR) e il Decreto Legislativo 196/2003 aggiornato, oltre a eventuali normative specifiche applicabili al settore ICT e al commercio all'ingrosso.

10. Formazione e consapevolezza

GMK SISTEMI S.R.L. assicura che tutto il personale coinvolto riceva formazione specifica sulla gestione degli incidenti di sicurezza informatica, con aggiornamenti periodici e simulazioni pratiche. La formazione è documentata e valutata per garantire la preparazione operativa e la sensibilizzazione continua, requisito fondamentale per la conformità ISO 9001 e ISO/IEC 27001.