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 NUBYS S.R.L. per la gestione efficace e tempestiva degli incidenti di sicurezza informatica, in conformità ai requisiti di ISO/IEC 27001 (clausole 6.1, 7.5, 8.2, 9.1) e integrando le best practice di ISO 9001 per la gestione della qualità e il miglioramento continuo (clausole 8.7, 10.2). L'obiettivo è garantire la protezione della riservatezza, integrità e disponibilità delle informazioni e dei sistemi IT, minimizzando l'impatto operativo e reputazionale.

1. Ambito e Campo di Applicazione

La procedura si applica a tutte le attività e risorse IT gestite da NUBYS S.R.L., inclusi sistemi software, infrastrutture di rete, servizi cloud e dati trattati nell'ambito dei processi di progettazione, sviluppo, manutenzione e assistenza tecnica. Riguarda tutti i dipendenti, collaboratori e fornitori coinvolti nella gestione e risposta agli incidenti di sicurezza.

2. Definizione di Incidente di Sicurezza Informatica

Per incidente di sicurezza informatica si intende qualsiasi evento che comprometta o possa compromettere la riservatezza, integrità o disponibilità delle informazioni o dei sistemi informatici aziendali. Esempi includono accessi non autorizzati, malware, perdita di dati, interruzioni di servizio e violazioni di policy di sicurezza.

3. Ruoli e Responsabilità

Ruolo |

Responsabilità |

Responsabile Sicurezza delle Informazioni (RSI) |

Coordinamento della gestione degli incidenti, valutazione del rischio, comunicazione con la Direzione e autorità competenti, supervisione delle azioni correttive. |

Team Tecnico IT |

Rilevazione, analisi tecnica e contenimento dell'incidente, raccolta delle evidenze, ripristino dei sistemi e supporto nelle indagini. |

Tutti i Dipendenti |

Segnalazione immediata di qualsiasi sospetto incidente di sicurezza tramite i canali definiti, rispetto delle procedure di sicurezza e collaborazione nelle attività di risposta. |

Direzione Aziendale |

Approvazione delle politiche di sicurezza, allocazione delle risorse necessarie e decisioni strategiche in caso di incidenti gravi. |

4. Processo Operativo di Gestione Incidenti

Il processo di gestione degli incidenti si articola nelle seguenti fasi, in linea con la pianificazione e controllo previsti da ISO/IEC 27001 (clausola 8.2):

• Rilevazione e Segnalazione: Ogni dipendente o sistema automatizzato deve segnalare tempestivamente qualsiasi evento sospetto al Responsabile Sicurezza tramite il modulo di segnalazione incidenti dedicato.

• Classificazione e Prioritizzazione: Il RSI valuta la gravità e l'impatto potenziale dell'incidente, assegnando una priorità di intervento in base alla criticità dei sistemi coinvolti e alla sensibilità dei dati.

• Analisi e Contenimento: Il team tecnico effettua un'analisi approfondita per identificare la causa, l'estensione e le vulnerabilità sfruttate, adottando misure immediate per contenere l'incidente e prevenire ulteriori danni.

• Eradicazione e Ripristino: Vengono rimosse le cause dell'incidente, ripristinati i sistemi e i dati compromessi, garantendo la continuità operativa secondo i piani di disaster recovery e business continuity.

• Comunicazione e Reporting: Tutte le attività e decisioni sono documentate nel registro incidenti. Il RSI informa la Direzione e, se necessario, le autorità competenti rispettando i requisiti normativi applicabili.

• Analisi Post-Incidente e Miglioramento: Si conducono revisioni per identificare le cause profonde, valutare l'efficacia delle contromisure e aggiornare le politiche e procedure di sicurezza per prevenire il ripetersi di eventi analoghi.

Placeholder diagramma di flusso del processo di gestione incidenti.

5. Documentazione e Registrazioni

La gestione degli incidenti è supportata da documenti e registrazioni controllate, fondamentali per garantire la tracciabilità e l'auditabilità del processo, in conformità a ISO 9001 (clausole 7.5 e 8.7) e ISO/IEC 27001 (clausola 7.5):

• Modulo di Segnalazione Incidente: Documento standardizzato per la raccolta delle informazioni iniziali sull'incidente.

• Registro Incidenti di Sicurezza: Archivio centralizzato contenente la descrizione, classificazione, azioni intraprese, responsabili e tempi di risoluzione di ogni incidente.

• Report di Analisi Post-Incidente: Documento di sintesi con valutazioni, lezioni apprese e proposte di miglioramento.

• Comunicazioni Ufficiali: Copie delle comunicazioni interne ed esterne relative all'incidente, incluse eventuali notifiche a clienti o autorità.

6. Indicatori di Prestazione e Verifica

Per monitorare l'efficacia della procedura e favorire il miglioramento continuo, NUBYS S.R.L. utilizza i seguenti indicatori chiave di prestazione (KPI), in linea con le clausole 9.1 e 10.2 di ISO 9001 e ISO/IEC 27001:

• Tempo medio di rilevazione e segnalazione degli incidenti.

• Percentuale di incidenti risolti entro i tempi stabiliti.

• Numero di incidenti ricorrenti o non conformità correlate.

• Valutazione dell'efficacia delle azioni correttive post-incidente.

Questi indicatori sono oggetto di revisione periodica durante le riunioni di riesame della Direzione e degli audit interni, per garantire la conformità e l'adeguatezza del sistema di gestione della sicurezza delle informazioni.

7. Interfacce e Collaborazioni Esterne

La gestione degli incidenti può richiedere l'interazione con fornitori di servizi IT, consulenti esterni, clienti o autorità di controllo. Tali interfacce sono regolate da accordi contrattuali e procedure di comunicazione specifiche, che assicurano la riservatezza e la tempestività delle informazioni scambiate, in coerenza con la politica di sicurezza aziendale e i requisiti normativi vigenti.

8. Audit e Verifiche di Conformità

La procedura di gestione degli incidenti è soggetta a verifiche interne periodiche, integrate nel programma di audit del Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni. Gli audit valutano la corretta applicazione delle fasi operative, la completezza della documentazione, l'efficacia delle azioni correttive e la conformità ai requisiti di ISO 9001 e ISO/IEC 27001. Le evidenze raccolte durante gli audit costituiscono base per il miglioramento continuo e per la gestione dei rischi associati alla sicurezza informatica.

9. Formazione e Consapevolezza

NUBYS S.R.L. garantisce che tutto il personale coinvolto nella gestione degli incidenti riceva formazione specifica e aggiornamenti periodici sulle procedure, sulle tecniche di rilevazione e risposta e sulle normative applicabili. La formazione contribuisce a sviluppare una cultura della sicurezza informatica coerente con gli obiettivi aziendali e i requisiti normativi.

10. Riferimenti Normativi e Standard di Riferimento

- ISO 9001:2015 - Sistemi di gestione per la qualità
- ISO/IEC 27001:2022 - Sistemi di gestione della sicurezza delle informazioni
- Regolamento UE 2016/679 (GDPR) - Protezione dei dati personali (se applicabile)
- Normativa nazionale vigente in materia di sicurezza informatica e protezione dei dati