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 il processo operativo adottato da DNS Informatica SAS per la gestione efficace e tempestiva degli incidenti di sicurezza informatica, in conformità ai requisiti di ISO/IEC 27001 (clausole 6.1, 7.5, 8.1, 9.1, 10.1) e integrando le best practice di ISO 9001 per il miglioramento continuo e la gestione della qualità (clausole 8.5, 9.2, 10.2). L'obiettivo è garantire la tutela della riservatezza, integrità e disponibilità delle informazioni gestite, minimizzando impatti operativi e reputazionali per l'azienda e i suoi clienti nel settore ICT-IT consultancy and solutions.

1. Ambito e Applicabilità

La procedura si applica a tutti gli incidenti di sicurezza informatica che coinvolgono le infrastrutture IT, i servizi cloud, le soluzioni di cybersecurity, nonché i sistemi di gestione e hosting gestiti da DNS Informatica SAS presso la sede operativa di via Pietro Micca 3, Trecate (NO). Sono inclusi incidenti rilevati internamente o segnalati da clienti, fornitori o terze parti, in linea con il contesto aziendale e i rischi identificati nel Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

2. Definizioni e Classificazione degli Incidenti

Un incidente di sicurezza informatica è qualsiasi evento che compromette o minaccia la riservatezza, integrità o disponibilità delle informazioni o dei sistemi IT. Gli incidenti sono classificati in base alla gravità e impatto, considerando:

• Incidente di basso impatto: anomalie o tentativi di accesso non autorizzato senza compromissione effettiva.

• Incidente di medio impatto: compromissione parziale di dati o servizi con impatto limitato su clienti o processi interni.

• Incidente di alto impatto: violazioni significative che compromettono dati sensibili, infrastrutture critiche o comportano interruzioni di servizio rilevanti.

3. Ruoli e Responsabilità

Ruolo |

Responsabilità |

Riferimento ISO |

Responsabile Sicurezza Informazioni (RSI) |

Coordinamento della gestione incidenti, valutazione impatti, attivazione delle contromisure e comunicazione interna ed esterna. |

ISO/IEC 27001: 7.5, 8.1, 9.1 |

Team Tecnico ICT |

Analisi tecnica, contenimento, mitigazione e ripristino dei sistemi coinvolti nell'incidente. |

ISO/IEC 27001: 8.1, 9.1 |

Direzione Aziendale |

Supporto decisionale, allocazione risorse e approvazione delle azioni correttive e preventive. |

ISO 9001: 5.1, 10.2 |

Tutti i Dipendenti |

Segnalazione tempestiva di anomalie o sospetti incidenti secondo le modalità definite. |

ISO/IEC 27001: 7.2 |

4. Processo Operativo di Gestione Incidenti

Il processo di gestione incidenti si articola nelle seguenti fasi, integrate nel sistema di gestione documentale e di monitoraggio della qualità:

• Rilevazione e Segnalazione: Ogni dipendente o sistema automatizzato può rilevare un potenziale incidente. La segnalazione deve essere inoltrata immediatamente al RSI tramite il modulo di registrazione incidenti dedicato.

• Registrazione e Classificazione: Il RSI registra l'incidente nel registro ufficiale, assegnando priorità e categoria in base all'impatto e alla probabilità di danno.

• Analisi e Contenimento: Il team tecnico effettua un'analisi approfondita per identificare la causa, estensione e possibili vulnerabilità sfruttate, attivando misure di contenimento per limitare la diffusione o aggravamento.

• Mitigazione e Ripristino: Vengono implementate azioni correttive per eliminare la causa dell'incidente e ripristinare i servizi e dati compromessi, garantendo la continuità operativa.

• Comunicazione e Reporting: Il RSI informa la direzione e, se necessario, i clienti o autorità competenti, nel rispetto delle normative vigenti e della politica aziendale sulla privacy e sicurezza.

• Verifica e Chiusura: Dopo il ripristino, si verifica l'efficacia delle azioni intraprese e si formalizza la chiusura dell'incidente nel registro, con evidenza documentale.

• Analisi Post-Incidente e Miglioramento: Si conducono analisi approfondite per identificare opportunità di miglioramento, aggiornamento delle procedure e formazione del personale.

IsoPilot inserirà qui automaticamente il 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 la conformità ai requisiti normativi e di sistema:

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

• Registro Incidenti di Sicurezza: Archivio digitale centralizzato contenente tutte le segnalazioni, analisi, azioni e chiusure.

• Report di Analisi e Azioni Correttive: Documentazione tecnica dettagliata delle attività svolte e delle misure adottate.

• Verbali di Riesame e Miglioramento: Evidenze delle riunioni di valutazione post-incidente e delle decisioni di miglioramento.

6. Indicatori di Prestazione e Audit

Per monitorare l'efficacia della procedura, DNS Informatica SAS ha definito indicatori chiave di prestazione (KPI) quali:

• Tempo medio di rilevazione e segnalazione dell'incidente.

• Tempo medio di contenimento e mitigazione.

• Numero di incidenti ricorrenti o non risolti al primo intervento.

• Percentuale di incidenti comunicati tempestivamente alla direzione e, se applicabile, alle autorità competenti.

Questi indicatori sono oggetto di verifica durante gli audit interni del SGSI e del Sistema di Gestione per la Qualità, con particolare attenzione alla conformità ai requisiti di ISO/IEC 27001 (clausole 9.2, 9.3) e ISO 9001 (clausole 9.2, 10.2). Le nonconformità rilevate sono gestite tramite azioni correttive documentate.

7. Interfacce e Collaborazioni Esterne

La procedura prevede interfacce operative con fornitori di servizi ICT, partner di sicurezza e clienti, in particolare per la gestione di incidenti che coinvolgano infrastrutture condivise o servizi in outsourcing. Le responsabilità e modalità di intervento sono definite nei contratti e accordi di servizio, in linea con la clausola 8.4 di ISO/IEC 27001. La collaborazione tempestiva e trasparente è essenziale per la mitigazione efficace degli incidenti.

8. Formazione e Consapevolezza

Per garantire la prontezza operativa, DNS Informatica SAS organizza periodicamente sessioni di formazione specifica per il personale coinvolto nella gestione degli incidenti, con aggiornamenti sulle minacce emergenti e sulle procedure interne. La formazione è documentata e valutata per assicurare il mantenimento delle competenze richieste, in conformità con la clausola 7.2 di ISO/IEC 27001.

9. Riesame e Miglioramento Continuo

Il Responsabile Sicurezza Informazioni, in collaborazione con la Direzione, conduce regolarmente il riesame del processo di gestione incidenti, analizzando indicatori, registrazioni e feedback per identificare opportunità di miglioramento. Le azioni correttive e preventive sono pianificate e monitorate secondo il ciclo PDCA previsto da ISO 9001 e ISO/IEC 27001, garantendo l'evoluzione continua del sistema di gestione.

La presente procedura è soggetta a revisione periodica e aggiornamento controllato, con versionamento documentale conforme al sistema di gestione documentale aziendale, assicurando la disponibilità della versione vigente a tutto il personale interessato.