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 operativo fondamentale per DNS Informatica SAS, in linea con i requisiti di ISO/IEC 27001 (clausole 6.1 e 8.1) e ISO 9001 (clausola 6.1), finalizzato all'identificazione, valutazione, trattamento e monitoraggio sistematico dei rischi relativi alla sicurezza delle informazioni. Questo registro supporta la gestione integrata della qualità e della sicurezza informatica, garantendo la tutela della riservatezza, integrità e disponibilità dei dati trattati nell'ambito delle attività di consulenza ICT e servizi cloud, hosting e cybersecurity.

1. Scopo e ambito di applicazione

Il registro documenta in modo strutturato e aggiornato tutti i rischi associati ai processi IT e alle infrastrutture gestite da DNS Informatica SAS, inclusi i servizi di system management, VoIP, assistenza remota e valutazioni IT per clienti aziendali e pubblici. L'ambito copre le sedi operative di Romentino e Trecate, considerando le specificità di un'organizzazione di 5 dipendenti operante nel settore ICT (ATECO 62202). Il registro è uno strumento di supporto per il Responsabile della Sicurezza delle Informazioni (RSI) e per il management, integrando le attività di gestione del rischio nel Sistema di Gestione Integrato Qualità-Sicurezza.

2. Metodologia di identificazione e valutazione dei rischi

La valutazione dei rischi si basa su un'analisi approfondita delle minacce, vulnerabilità e impatti potenziali sulle risorse informative critiche, in conformità con la clausola 6.1.2 di ISO/IEC 27001. Vengono considerati fattori quali la natura dei dati trattati, le tecnologie impiegate (es. cloud, hosting, VoIP), e le modalità operative, inclusa la gestione remota. La probabilità e la gravità degli eventi rischiosi sono quantificate attraverso criteri definiti nel piano di trattamento del rischio, con evidenze documentate per garantire la tracciabilità e la ripetibilità del processo.

3. Struttura e contenuti del registro

Codice Rischio |

Descrizione Rischio |

Asset Coinvolto |

Minaccia |

Vulnerabilità |

Impatto |

Probabilità |

Livello di Rischio |

Misure di Controllo |

Responsabile |

Data Revisione |

Stato |

Ogni voce del registro deve essere aggiornata periodicamente, almeno annualmente o in seguito a modifiche significative nei processi o nelle tecnologie, in conformità con la clausola 9.1 di ISO/IEC 27001. Le misure di controllo includono sia azioni preventive che correttive, integrate con le procedure operative e le policy aziendali.

4. Responsabilità e interfacce

Il Responsabile della Sicurezza delle Informazioni (RSI) ha la responsabilità primaria di mantenere e aggiornare il registro, coordinandole attività di valutazione con i responsabili di processo e il management. Il Direttore Tecnico e il Responsabile Qualità collaborano per integrare i risultati nel Sistema di Gestione Integrato. Le interfacce operative coinvolgono il team IT, il personale di assistenza e i fornitori di servizi cloud e hosting, garantendo che le informazioni sui rischi siano condivise e gestite in modo coerente.

5. Evidenze documentali e indicatori di monitoraggio

Il registro rischi costituisce una evidenza documentale obbligatoria per audit interni ed esterni, dimostrando la conformità ai requisiti ISO 9001 (clausola 9.2) e ISO/IEC 27001 (clausola 9.1). Gli indicatori di efficacia includono il numero di rischi identificati, il livello di rischio residuo, il tasso di implementazione delle misure di controllo e la frequenza di aggiornamento del registro. Le non conformità rilevate in sede di audit sono tracciate e gestite tramite il sistema di gestione delle azioni correttive.

6. Integrazione con il processo di gestione del rischio e miglioramento continuo

Il registro rischi è parte integrante del processo di gestione del rischio aziendale, che prevede la pianificazione, attuazione, verifica e riesame delle misure di sicurezza, in linea con la clausola 10 di ISO/IEC 27001. Le revisioni periodiche del registro alimentano il riesame della direzione, contribuendo al miglioramento continuo del Sistema di Gestione Integrato. Eventuali variazioni nel contesto aziendale o normativo sono tempestivamente valutate e incorporate nel registro.

7. Processo di aggiornamento e controllo delle modifiche

Le modifiche al registro rischi sono gestite attraverso un processo documentato di controllo delle modifiche, che prevede l'approvazione formale da parte del RSI e del management. Ogni aggiornamento è registrato con data, descrizione della modifica e responsabile dell'aggiornamento, garantendo la tracciabilità e la trasparenza. Questo processo supporta la conformità ai requisiti di documentazione e controllo previsti da ISO 9001 (clausola 7.5) e ISO/IEC 27001 (clausola 7.5).

8. Audit e verifiche di conformità

Durante gli audit interni ed esterni, il registro rischi viene esaminato per verificare la completezza, l'accuratezza e l'efficacia delle azioni di mitigazione implementate. Gli auditor valutano la coerenza tra i rischi identificati, le misure adottate e i risultati ottenuti, nonché la capacità del registro di supportare la gestione proattiva della sicurezza delle informazioni. Le evidenze raccolte includono report di audit, verbali di riesame della direzione e registrazioni delle azioni correttive.

9. Visualizzazione del processo

Di seguito è rappresentato il processo integrato di gestione e aggiornamento del registro rischi sicurezza informazioni, evidenziando le interazioni tra identificazione, valutazione, trattamento, monitoraggio e riesame, in un contesto di miglioramento continuo e conformità ai requisiti ISO 9001 e ISO/IEC 27001.