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 presente registro costituisce uno strumento operativo fondamentale per la gestione sistematica dei rischi relativi alla sicurezza delle informazioni in NUBYSS.R.L., in conformità ai requisiti di ISO/IEC 27001 (clausole 6.1 e 8.1) e integrato con il sistema di gestione per la qualità ISO 9001 (clausole 6.1 e 9.1). Il registro supporta la pianificazione, l'attuazione e il monitoraggio delle misure di sicurezza, garantendo la protezione della riservatezza, integrità e disponibilità delle informazioni trattate nei processi aziendali di sviluppo software, consulenza tecnologica e assistenza tecnica.

1. Scopo e campo di applicazione

Il registro rischi sicurezza informazioni documenta l'identificazione, la valutazione, il trattamento e il monitoraggio dei rischi associati alle informazioni gestite da NUBYSS.R.L., con particolare attenzione ai dati e sistemi coinvolti nelle attività di programmazione informatica e digitalizzazione dei processi aziendali. Include rischi tecnici, organizzativi e di processo, riferiti sia alla sede operativa di Romentino (NO) sia alla sede legale di Milano (MI).

2. Responsabilità e ruoli

La responsabilità primaria per la gestione del registro rischi è attribuita al Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (ISMS Manager), nominato tra i referenti aziendali (Martinelli Giancarlo e Racca Marco). L'ISMS Manager coordina le attività di identificazione e valutazione dei rischi, coinvolgendo i responsabili di processo e il personale tecnico, e garantisce l'aggiornamento periodico del registro in relazione a modifiche organizzative, tecnologiche o normative.

3. Metodologia di identificazione e valutazione dei rischi

L'analisi dei rischi si basa su una valutazione qualitativa e quantitativa, considerando la probabilità di accadimento e l'impatto potenziale su riservatezza, integrità e disponibilità delle informazioni. Vengono presi in esame fattori interni quali vulnerabilità dei sistemi software sviluppati, configurazioni di rete, competenze del personale, nonché fattori esterni come minacce informatiche e compliance normativa. La metodologia è allineata ai criteri definiti nel contesto aziendale e documentata nel piano di trattamento dei rischi.

4. Struttura del registro rischi

Identificativo rischio |

Descrizione rischio |

Fonte minaccia |

Vulnerabilità |

Impatto |

Probabilità |

Livello rischio |

Misure di controllo |

Responsabile |

Data valutazione |

Stato trattamento |

R001 |

Accesso non autorizzato a dati clienti |

Minaccia interna/esterna |

Controlli accesso insufficienti |

Alto |

Medio |

Alto |

Implementazione autenticazione multifattore, formazione personale |

ISMS Manager |

01/06/2026 |

In corso |

5. Interfacce con altri processi e documenti

Il registro rischi è strettamente integrato con il processo di gestione delle non conformità e azioni correttive (ISO 9001 clausola 10.2), con il piano di trattamento dei rischi (ISO/IEC 27001 clausola 6.1.3) e con le attività di audit interno (clausola 9.2). Le evidenze di monitoraggio e revisione del registro sono documentate e conservate come parte della documentazione di sistema, garantendo tracciabilità e trasparenza nelle decisioni di gestione del rischio.

Inoltre, il registro supporta la valutazione periodica del contesto organizzativo e delle parti interessate (clausola 4.1 e 4.2 ISO 9001 e ISO/IEC 27001), permettendo di aggiornare tempestivamente le strategie di sicurezza in risposta a cambiamenti tecnologici o di mercato.

6. Evidenze e indicatori di efficacia

Per verificare l'efficacia delle misure di controllo e la corretta gestione dei rischi, sono definiti indicatori specifici quali il numero di incidenti di sicurezza registrati, il tempo medio di risposta agli eventi, la percentuale di personale formato e la frequenza di aggiornamento del registro. Tali indicatori sono oggetto di monitoraggio continuo e riportati nei rapporti di audit interno e nelle riesaminazioni della direzione (clausola 9.3).

7. Conservazione e controllo del registro

Il registro rischi è conservato in formato elettronico all'interno del sistema documentale aziendale, con accesso controllato e versionamento conforme alla procedura di gestione della documentazione (ISO 9001 clausola 7.5). Ogni modifica è tracciata con data, autore e motivazione, garantendo la disponibilità dell'informazione aggiornata a tutti i soggetti coinvolti nel sistema di gestione.

8. Audit e verifiche

Durante le attività di audit interno ed esterno, il registro rischi rappresenta un elemento chiave per la valutazione della conformità e dell'efficacia del sistema di gestione della sicurezza delle informazioni. Gli auditor verificano la completezza, l'aggiornamento e la coerenza delle valutazioni di rischio, nonché l'adeguatezza delle azioni di trattamento intraprese, in linea con i requisiti normativi e le politiche aziendali.

9. Aggiornamento e miglioramento continuo

Il registro rischi è soggetto a revisione almeno annuale o in seguito a eventi significativi quali incidenti di sicurezza, modifiche organizzative o tecnologiche, o aggiornamenti normativi. Il processo di aggiornamento è coordinato dall'ISMS Manager e coinvolge i responsabili di processo per garantire un miglioramento continuo della gestione del rischio, in conformità con la clausola 10 di ISO 9001 e ISO/IEC 27001.

La documentazione aggiornata del registro rischi contribuisce a consolidare la cultura della sicurezza in NUBYS S.R.L., supportando la protezione delle informazioni critiche e la resilienza operativa dell'azienda nel settore della programmazione informatica.

[Diagramma del processo di gestione del registro rischi sicurezza informazioni: identificazione, valutazione, trattamento, monitoraggio e revisione.]