

1. Procedura backup e ripristino

Procedura backup e ripristino

La presente procedura definisce le modalità operative adottate da GMK SISTEMI S.R.L. per garantire la corretta esecuzione delle attività di backup e ripristino dei dati aziendali, in conformità ai requisiti delle norme ISO 9001 (clausole 7.5, 8.5.3) e ISO/IEC 27001 (clausole 8.3, 8.4, 9.1). L'obiettivo è assicurare la disponibilità, integrità e riservatezza delle informazioni critiche, minimizzando rischi di perdita o compromissione dei dati nell'ambito delle attività di commercio all'ingrosso, assistenza tecnica e sviluppo software.

1. Ambito e campo di applicazione

La procedura si applica a tutti i sistemi informativi, server, postazioni di lavoro e dispositivi di memorizzazione utilizzati da GMK SISTEMI S.R.L. per la gestione dei dati aziendali, inclusi i dati relativi al sito web aziendale, software sviluppati internamente, documentazione tecnica e amministrativa. Sono inclusi anche i dati gestiti da fornitori esterni in outsourcing, ove applicabile.

2. Responsabilità

- **Responsabile IT:** pianifica, esegue e verifica le attività di backup e ripristino, mantiene la documentazione aggiornata e coordina le azioni di miglioramento.
- **Responsabile Qualità:** monitora la conformità della procedura rispetto ai requisiti ISO 9001 e supporta le attività di audit interne ed esterne.
- **Responsabile Sicurezza delle Informazioni:** garantisce l'adeguatezza delle misure di sicurezza adottate in conformità a ISO/IEC 27001, inclusi i controlli di accesso e la protezione dei dati di backup.
- **Tutti i dipendenti:** devono segnalare tempestivamente eventuali anomalie o incidenti relativi alla perdita o compromissione dei dati.

3. Modalità operative

Le attività di backup sono pianificate con cadenza regolare, definita in base alla criticità dei dati e alla frequenza di aggiornamento, con almeno un backup completo settimanale e backup incrementali giornalieri. I supporti di memorizzazione utilizzati sono protetti da accessi non autorizzati e conservati in luoghi sicuri, preferibilmente in formato digitale e con ridondanza geografica per garantire la continuità operativa.

Il processo di ripristino viene testato periodicamente, almeno una volta ogni sei mesi, per verificare l'efficacia delle procedure e la corretta integrità dei dati recuperati. Le prove di ripristino sono documentate e analizzate per identificare eventuali criticità e implementare azioni correttive.

4. Controlli e indicatori di prestazione

Indicatore |

Descrizione |

Frequenza di monitoraggio |

Responsabile |

Percentuale backup completati con successo |

Misura la riuscita delle operazioni di backup pianificate |

Mensile |

Responsabile IT |

Tempo medio di ripristino dati |

Valuta l'efficienza del processo di ripristino in caso di incidente |

Semestrale (in occasione dei test) |

Responsabile IT |

Numero di incidenti legati alla perdita dati |

Conta gli eventi di perdita o compromissione dati rilevati |

Continuo |

Responsabile Sicurezza delle Informazioni |

5. Documentazione e registrazioni

Tutte le attività di backup e ripristino sono tracciate mediante registri digitali, che includono data, ora, tipologia di backup, esito dell'operazione e nominativo dell'operatore. Le prove di ripristino sono documentate con report dettagliati contenenti tempi di esecuzione, eventuali anomalie riscontrate e azioni correttive adottate. Questi documenti costituiscono evidenza oggettiva per le verifiche interne e per gli audit di certificazione.

6. Gestione dei rischi e miglioramento continuo

In linea con la politica di gestione del rischio di GMK SISTEMI S.R.L., i processi di backup e ripristino sono soggetti a valutazioni periodiche per identificare vulnerabilità e minacce quali guasti hardware, errori umani o attacchi informatici. Le misure di mitigazione includono l'adozione di tecnologie aggiornate, la formazione del personale e la revisione delle procedure in base ai risultati degli audit e delle analisi degli incidenti.

7. Interfacce con altri processi aziendali

La procedura di backup e ripristino interagisce strettamente con i processi di gestione della sicurezza delle informazioni, manutenzione IT, gestione della qualità e formazione del personale. La collaborazione tra i responsabili di tali processi è fondamentale per garantire la coerenza delle misure adottate e il rispetto dei requisiti normativi e contrattuali.

Placeholder per diagrammi di processo integrato backup e ripristino con interfacce ai processi di sicurezza, qualità e manutenzione IT.

8. Verifiche e audit

Le attività di backup e ripristino sono oggetto di verifica durante gli audit interni programmati, con particolare attenzione alla conformità procedurale, all'efficacia delle misure di sicurezza e alla completezza della documentazione. Eventuali non conformità rilevate sono gestite tramite il sistema di gestione delle non conformità, con azioni correttive e preventive documentate e monitorate.

La partecipazione attiva del Responsabile IT e del Responsabile Sicurezza delle Informazioni è essenziale per fornire evidenze oggettive e facilitare il miglioramento continuo del sistema di gestione.