

# 1. Procedura backup e ripristino

## Procedura Backup e Ripristino

La presente procedura definisce le modalità operative adottate da NUBYS S.R.L. per garantire la protezione, la disponibilità e l'integrità delle informazioni critiche attraverso attività sistematiche di backup e ripristino, in conformità ai requisiti delle norme ISO 9001 (clausole 8.5.3, 9.1.1) e ISO/IEC 27001 (clausole 8.3, 9.1, 10.1). L'obiettivo è assicurare la continuità operativa e la resilienza dei servizi IT erogati nell'ambito delle attività di programmazione informatica e sviluppo software, minimizzando i rischi di perdita dati e interruzione dei processi aziendali.

## 1. Ambito e Campo di Applicazione

La procedura si applica a tutti i sistemi informativi, applicativi, database e infrastrutture IT gestite presso la sede operativa di Via Ticino, 51 - 28068 Romentino (NO), nonché a tutte le risorse digitali utilizzate nei processi di progettazione, sviluppo, manutenzione e assistenza tecnica software. Sono inclusi i dati aziendali, i codici sorgente, le configurazioni di rete, le licenze software e i documenti digitali rilevanti per l'attività.

## 2. Responsabilità

Ruolo |

Responsabilità |

Responsabile IT |

Pianificazione, esecuzione e verifica dei backup; gestione delle procedure di ripristino; monitoraggio degli indicatori di performance; mantenimento della documentazione aggiornata. |

Amministratori di Sistema |

Esecuzione operativa dei backup e ripristini; segnalazione tempestiva di anomalie e non conformità; supporto tecnico alle attività di verifica. |

Direzione |

Approvazione della procedura; allocazione delle risorse necessarie; revisione periodica e audit interni per garantire l'efficacia del sistema di backup. |

## 3. Modalità Operative di Backup

I backup vengono eseguiti con cadenza giornaliera per i dati critici e settimanale per i dati meno sensibili, utilizzando soluzioni software certificate e conformi alle best practice del settore IT. Le copie di sicurezza sono conservate in ambienti protetti, sia on-site che off-site, per garantire la disponibilità anche in caso di eventi disastrosi locali. Il processo prevede la verifica automatica dell'integrità dei file di backup e la registrazione di ogni attività in un registro elettronico dedicato.

- Tipologie di backup: completo, incrementale e differenziale, in funzione della criticità dei dati e della frequenza di aggiornamento.
- Supporti di memorizzazione: server dedicati, cloud certificato, dispositivi di storage esterni con crittografia.

- Protezione dei dati: utilizzo di protocolli sicuri per la trasmissione e conservazione, conformità al GDPR e alle normative vigenti in materia di sicurezza delle informazioni.

#### 4. Procedura di Ripristino

Il ripristino dei dati viene effettuato esclusivamente su autorizzazione del Responsabile IT o della Direzione, previa valutazione dell'impatto e della priorità. Le attività di recupero sono documentate dettagliatamente, includendo la descrizione dell'evento che ha causato la perdita, i tempi di intervento, le risorse coinvolte e l'esito finale. Sono previsti test periodici di ripristino per validare l'efficacia delle copie di backup e garantire la prontezza operativa in caso di emergenza.

#### 5. Monitoraggio e Indicatori di Performance

Per assicurare il continuo miglioramento del sistema di backup e ripristino, vengono monitorati i seguenti indicatori:

- Percentuale di backup completati con successo rispetto al totale pianificato;
- Tempo medio di ripristino dei dati;
- Numero di incidenti legati alla perdita o corruzione dei dati;
- Esito dei test periodici di ripristino.

I risultati vengono analizzati trimestralmente durante le riunioni di riesame della Direzione, con eventuali azioni correttive e preventive documentate e tracciate nel sistema di gestione.

#### 6. Registrazioni e Documentazione

Tutte le attività di backup e ripristino sono registrate nel Registro Backup e Ripristino, che include:

- Data e ora di esecuzione;
- Tipologia di backup effettuato;
- Esito dell'operazione;
- Eventuali anomalie riscontrate e azioni correttive adottate;
- Dettagli degli interventi di ripristino.

La documentazione è conservata in formato digitale e cartaceo, con accesso riservato al personale autorizzato, in linea con le politiche di sicurezza delle informazioni definite nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

#### 7. Interfacce con Altri Processi Aziendali

La procedura di backup e ripristino interagisce strettamente con i processi di gestione della sicurezza informatica, continuità operativa, gestione delle non conformità e formazione del personale. In particolare, la collaborazione con il team di consulenza tecnologica e sviluppo software è fondamentale per identificare i dati critici e aggiornare tempestivamente le strategie di protezione in funzione delle evoluzioni tecnologiche e delle esigenze di business.

Placeholder per diagrammi di flusso del processo di backup e ripristino, inclusivo delle interfacce con i processi di sicurezza, gestione incidenti e formazione.

#### 8. Audit Interni e Verifiche di Conformità

La conformità e l'efficacia della procedura sono oggetto di audit interni programmati secondo il piano di audit del Sistema di Gestione Integrato ISO 9001 e ISO/IEC 27001. Durante le verifiche, si esaminano le registrazioni, si valutano i risultati degli indicatori e si conducono test di ripristino simulati. Le eventuali non conformità rilevate sono gestite tramite il processo di miglioramento continuo, con azioni correttive e preventive documentate e monitorate fino alla loro completa risoluzione.

## **9. Gestione del Rischio**

La procedura integra le attività di analisi e gestione del rischio previste dal SGSI, identificando le minacce potenziali alla disponibilità dei dati (guasti hardware, attacchi informatici, errori umani) e definendo misure di mitigazione adeguate. La revisione periodica del piano di backup tiene conto delle variazioni del contesto tecnologico e organizzativo, garantendo un adeguato livello di protezione coerente con la strategia aziendale e le aspettative dei clienti.

## **10. Formazione e Consapevolezza**

Il personale coinvolto nelle attività di backup e ripristino riceve formazione specifica e aggiornamenti periodici per mantenere elevata la competenza tecnica e la consapevolezza sull'importanza della protezione dei dati. La formazione è documentata e monitorata come parte integrante del sistema di gestione delle risorse umane, in linea con i requisiti ISO 9001 e ISO/IEC 27001.