

1. Procedura backup e ripristino

Procedura backup e ripristino

La presente procedura definisce le modalità operative per l'esecuzione, la gestione e la verifica delle attività di backup e ripristino dei dati e dei sistemi informatici di DNS Informatica SAS, in conformità ai requisiti della norma ISO 9001 (clausole 8.5.3 e 9.1.1) e ISO/IEC 27001 (clausole 8.3, 8.4, 9.1 e 10.1). L'obiettivo è garantire la disponibilità, integrità e riservatezza delle informazioni gestite, minimizzando i rischi di perdita o compromissione, in linea con il contesto operativo e i processi ICT-IT dell'azienda.

1. Ambito e campo di applicazione

La procedura si applica a tutti i sistemi, infrastrutture e dati critici gestiti da DNS Informatica SAS presso la sede operativa di via Pietro Micca 3, Trecate (NO), inclusi server, dispositivi di rete, ambienti cloud e supporti di memorizzazione locali e remoti. Sono inclusi i dati relativi ai servizi di consulenza ICT, hosting, cybersecurity, VoIP e gestione infrastrutturale erogati ai clienti.

2. Responsabilità e ruoli

- Responsabile ICT (Racca Marco): definisce le politiche di backup, approva la pianificazione e verifica periodicamente l'efficacia del sistema di backup e ripristino.
- Amministratore di sistema: esegue operazioni tecniche di backup e ripristino, mantiene la documentazione aggiornata e segnala eventuali anomalie o incidenti.
- Responsabile Qualità e Sicurezza delle Informazioni: monitora la conformità della procedura ai requisiti ISO 9001 e ISO/IEC 27001, coordina le attività di audit interne e gestisce le non conformità correlate.

3. Pianificazione e frequenza dei backup

I backup devono essere pianificati in base alla criticità dei dati e alla frequenza di aggiornamento, garantendo almeno una copia giornaliera per i dati operativi e una copia settimanale per i dati di archivio. Le copie di backup devono essere conservate in luoghi sicuri, con almeno una copia off-site o in ambiente cloud certificato, per assicurare la continuità operativa in caso di eventi avversi.

4. Metodologia di backup

Le attività di backup si basano su soluzioni tecnologiche certificate e aggiornate, che prevedono backup completi, incrementali e differenziali a seconda delle esigenze specifiche dei sistemi. È obbligatorio l'uso di crittografia per la protezione dei dati durante la memorizzazione e il trasferimento, in conformità con le politiche di sicurezza aziendali e i requisiti di riservatezza ISO/IEC 27001.

5. Procedure di ripristino

Il ripristino dei dati deve essere eseguito tempestivamente in caso di perdita, danneggiamento o compromissione dei sistemi, seguendo un piano di disaster recovery documentato. Le operazioni di ripristino devono essere testate almeno semestralmente per verificarne l'efficacia e la tempestività, con registrazione dettagliata delle attività e degli esiti. Eventuali anomalie devono essere gestite tramite il sistema di gestione delle non conformità.

6. Controlli, monitoraggio e indicatori

Per garantire la conformità e l'efficacia della procedura, sono previsti controlli periodici e audit interni focalizzati su:

- Verifica della corretta esecuzione dei backup secondo la pianificazione;

- Controllo dell'integrità e della disponibilità delle copie di backup;
- Monitoraggio dei tempi di ripristino e rispetto degli SLA definiti;
- Analisi degli incidenti e delle non conformità correlate ai backup e ripristini.

Gli indicatori chiave di prestazione (KPI) includono la percentuale di backup completati con successo, il tempo medio di ripristino (RTO) e il numero di test di ripristino eseguiti con esito positivo.

7. Documentazione e registrazioni

Tutte le attività di backup e ripristino devono essere documentate in appositi registri elettronici, contenenti almenodata, ora, sistema interessato, tipo di backup, esito dell'operazione e responsabile esecutore. La documentazionecostituisce evidenza oggetto di audit e deve essere conservata per un periodo minimo di [inserire periodo conforme alle normative applicabili e alle esigenze aziendali].

8. Gestione delle non conformità e miglioramento

Eventuali malfunzionamentiritardi o errori nelle attività di backup e ripristino devono essere segnalati tempestivamente e gestiti tramite il sistema di gestione delle non conformità. Le azioni correttive e preventive devono essere pianificate e monitorate per evitare il ripetersi degli eventi, contribuendo al miglioramento continuo del sistema di gestione della qualità e della sicurezza delle informazioni.

9. Interfacce con altri processi aziendali

La procedura di backup e ripristino interagisce con i processi di gestione della sicurezza informatica, continuità operativa, gestione incidenti e supporto tecnico. La collaborazione tra i reparti ICT, qualità e sicurezza è fondamentale per garantire un approccio integrato e conforme ai requisiti normativi e contrattuali.

[Placeholder per diagrammadi flusso del processo di backup e ripristino, evidenziando input, output, responsabilità e interfacce con altri processi aziendali.]