Disaster Recovery plan

Il **Disaster Recovery Plan (DRP)** è un documento formale che descrive l'insieme di strategie, azioni e strumenti tecnologici necessari per ripristinare il corretto funzionamento dell'infrastruttura IT, dei sistemi informatici e il recupero dei dati dopo il verificarsi di un'emergenza o di un evento imprevisto all'interno dell'azienda.

SCOPO

Un DRP ha l'obiettivo di mettere in condizione l'azienda di risolvere più rapidamente possibile le criticità derivanti da una perdita di dati o da un'interruzione delle attività IT, e di ripristinare le funzionalità dei sistemi per garantire la business continuity.

ANALISI DEI RISCHI

La redazione di un DRP comporta un'analisi dei processi aziendali e delle esigenze di business continuity. Prima di generare un documento DRP dettagliato, infatti, spesso le aziende eseguono una **Business Impact Analysis (BIA)** e una **Risk Analysis (RA)** e stabiliscono gli obiettivi di ripristino.

LE CINQUE FASI DI IMPLEMENTAZIONE DI UN PROGETTO DI DRP

1 - Studio di fattibilità e stima di RPO e RTO

2 - Definizione della soluzione più adeguata

3 - Implementazione della soluzione

4 - Test periodico di disaster recovery

5 - MANUTENZIONE COSTANTE DEI SISTEMI

Primo step

Studio di fattibilità

Lo studio di fattibilità preliminare serve a identificare i rischi ed a effettuare una prima valutazione con l'individuazione dei target

Rpo

Recovery Point Objective

identifica la quantità massima di dati che si possono perdere a seguito dell'arresto.

★★★★★

Rto

Recovery Time Objective

tempo che intercorre tra l'interruzione e il momento del ripristino

★★★★★

Secondo step

Piano di disaster recovery

Una solida politica di **backup** potrebbe non esere sufficiente ai fini del ripristino dei dati ma comunque è già un buon punto di partenza

INFRASTUTTURA FISICA

INFRASTUTTURA VIRTUALE

IN CLOUD COME SERVIZIO(DRaaS).

Terzo step

Implementazione della soluzione

Scenario	Ransomware rilevato su uno o più computer/server
Cause possibili	Malware
Dati a rischio	Dati LIMS: registrazione campioni e relative informazioni, risultati delle prove e rapporti di prova emessi
Impatto	Perdita o danneggiamento di dati
Prevenzione	✓ Proteggere la sicurezza e-mail per evitare tentativi di phishing. ✓ .....
Piano di azione	✓ Scollegare l'hardware interessato rimuovendo il cavo di rete. ✓ Non pagare mai il riscatto richiesto. ....
Contatti chiave	Nome cognome e numero di telefono SoftwareHouse

Esempio

Piano di Disaster Recovery in caso di attacco Ransomware

ANALISI DEI RISCHI IN UN LABORATORIO DI PROVA

ISO 17025 Paragrafo 8.5.2 – Perdita di dati

QUARTO STEP: TEST PERIODICI DI DISASTER RECOVERY

I test periodici, a cadenza programmata, fanno parte integrante del piano e sono utili a verificare:

- ✓ l'efficacia della soluzione di Disaster Recovery
- ✓ il suo corretto funzionamento
- ✓ il rispetto dei valori di RTO/RPO
- ✓ la conferma dell'effettiva compliance rispetto agli SLA (Service Level Agreement) contrattualizzati.

QUINTO STEP

Manutenzione costante dei sistemi

La responsabilità di decidere quali rischi e opportunità sia necessario affrontare è del laboratorio

ISO 17025 – PUNTO 8.5.2

Il laboratorio deve pianificare:

a) Azioni per affrontare rischi e opportunità;

b) Le modalità per:

- integrare e attuare le azioni nel proprio sistema di gestione;
- Valutare l’efficacia di tali azioni.

BUSINESS CONTINUITY

il Disaster Recovery solitamente è compreso all’interno di un più ampio piano di continuità operativa e può essere considerato come uno degli elementi che costituiscono la Business Continuity