mercoledì 6 novembre 2024 19:31

Traccia:

1. Documentarsi su Business Continuity (BC) e Disaster Recovery (DR);

2. Produrre una tabella comparativa che evidenzi le differenze tra BC e DR;

3. Comprendere il concetto di ICT readiness for business continuity (IRBC - ISO/IEC 27031).

La **Business Continuity (BC)**, o continuità operativa, è la capacità di un'azienda di continuare a funzionare anche se accade qualcosa di inaspettato, come un guasto tecnico, un incendio o un disastro naturale. La BC si basa su piani e strategie preventive che permettonno di mantenere attive le funzioni principali dell'azienda, in modo da evitare perdite economiche e proteggere l'immagine dell'azienda.
Ad esempio, immagina una banca: anche in caso di blackout o di problemi tecnici, è fondamentale che i clienti possano continuare a prelevare soldi o a fare operazioni online. Per questo motivo, la banca deve avere strategie e strumenti pronti per garantire che i servizi essenziali non vengano interrotti, o che possano riprendere rapidamente.

Il **Disaster Recovery (DR)**, o recupero da disastro, è una parte della Business Continuity, specificamente dedicata alla gestione e al ripristino dell'infrastruttura IT (computer, server, reti e dati) dopo un disastro o un'interruzione grave.
Ad esempio se un'azienda perde tutti i dati perché i server si danneggiano in un incendio, il disaster recovery è il piano che dice come ripristinare quei dati e riattivare i server il più velocemente possibile. Un piano di DR può includere, il backup regolare dei dati in una posizione sicura o la replica dei server in un'altra sede geografica.

Aspetto	Business Continuity (BC)	Disaster Recovery (DR)
Obiettivo	Assicurare che tutte le attività principali dell'azienda possano continuare	Ripristinare i sistemi IT e i dati dell'azienda
Cosa include	Tutti i processi aziendali, come produzione, gestione clienti, finanza	Solo i sistemi tecnologici e i dati
Quando si attiva	Sempre, anche per piccoli imprevisti	Solo in caso di emergenze gravi che colpiscono la tecnologia
Esempi pratici	Un call center che rimane operativo anche in caso di problemi	Una banca che ripristina i dati in seguito a un crash dei server

La norma **ISO/IEC 27031**, anche conosciuta come ICT Readiness for Business Continuity (IRBC), è una guida che aiuta le aziende a preparare i loro sistemi tecnologici (ICT) per affrontare qualsiasi tipo di emergenza. Pensiamo agli

strumenti ICT come a tutto ciò che riguarda computer, reti, server e software: la "spina dorsale" digitale dell'azienda.
Immagina che un'azienda abbia tutti i dati importanti dei clienti su un server. Cosa accadrebbe se quel server smettesse improvvisamente di funzionare? L'IRBC si occupa proprio di questo: fornire linee guida per garantire che la tecnologia dell'azienda sia preparata per ogni evenienza, e che ci siano strategie in atto per continuare a funzionare anche in caso di problemi.

Principali aspetti coperti dall'IRBC

1. **Analisi dei rischi**: Identificare i possibili rischi per le risorse IT, come attacchi informatici o guasti tecnici, e valutare l'impatto di questi eventi sull'azienda.
2. **Piani di continuità e test**: Creare piani di emergenza per i sistemi ICT e testarli regolarmente per assicurarsi che funzionino davvero in caso di emergenza.
3. **Preparazione delle risorse ICT**: Assicurarsi che tutte le tecnologie di cui l'azienda ha bisogno per lavorare siano pronte ad affrontare situazioni di emergenza.