EPICODE

ESERCIZIO W18D1 - EXTRA

SECURITY OPERATION

Azioni preventive

Mungiovì Fabio

TASK

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).

ESECUZIONE

1. Business Continuity (BC) e Disaster Recovery (DR)

Immaginiamo un'azienda come un organismo vivente.
La **Business Continuity (BC),** o Continuità Operativa, è come il sistema immunitario di questo organismo.
Si tratta di un approccio olistico, che non si concentra solo sull'IT, ma su tutti gli aspetti dell'azienda.
Il suo obiettivo è garantire che l'azienda possa continuare a funzionare, anche di fronte a interruzioni gravi.
Non importa se è un'alluvione, un incendio, un attacco informatico o una pandemia, la BC si preoccupa di come l'azienda possa continuare a fornire i suoi prodotti o servizi essenziali ai clienti.
Pensiamo a tutte le funzioni vitali dell'azienda: produzione, vendite, servizio clienti, finanze, risorse umane, e come ognuna di queste può essere mantenuta attiva o ripristinata rapidamente.
È un processo continuo che include l'identificazione dei rischi, la pianificazione per mitigarli, la risposta agli incidenti e il recupero.

Il **Disaster Recovery (DR),** o Ripristino d'Emergenza, è invece una parte specifica della Business Continuity.
Se la BC è il sistema immunitario, il DR è come il "kit di pronto soccorso" per la parte tecnologica dell'azienda, quindi per i sistemi informatici e le infrastrutture IT.
Il suo focus è specifico sul ripristino di hardware, software, dati e reti dopo un disastro che ha colpito l'infrastruttura tecnologica.
Se un server crolla o un data center viene distrutto, il DR si occupa di come riportare online i sistemi IT nel minor tempo possibile.
È un piano molto più tecnico e dettagliato, che stabilisce procedure precise per il backup dei dati, il ripristino dei server, la configurazione delle reti e il funzionamento di siti di recupero alternativi.

Per fare un paragone semplice: la Business Continuity si chiede "Come possiamo continuare a lavorare se succede qualcosa di brutto?", mentre il Disaster Recovery si chiede "Come facciamo a rimettere in piedi i nostri computer e i nostri dati se si rompono?".
La prima è una strategia più ampia, la seconda è una tattica IT essenziale all'interno di quella strategia.

2. Tabella Comparativa tra BC e DR

Caratteristica	Business Continuity (BC)	Disaster Recovery (DR)
Ambito	Riguarda l'intera organizzazione	Specifico, si concentra sulle infrastrutture e sui sistemi IT
Obiettivo Principale	Mantenere le funzioni aziendali critiche operative e la capacità di erogare servizi essenziali durante e dopo un'interruzione.	Ripristinare l'ambiente IT dopo un disastro o un'interruzione, per supportare la ripresa delle operazioni.
Natura	Strategica e operativa. Si concentra sul "come continuare a fare business".	Tattica e tecnica. Si concentra sul "come ripristinare la tecnologia".
Focus	Continuità dei processi aziendali e servizi.	Ripristino dei sistemi informativi e dei dati.
Responsabilità	Tipicamente della direzione aziendale, coinvolgendo tutti i reparti.	Principalmente del dipartimento IT, con input dagli stakeholder aziendali.
Esempio di Piano	Include piani per il personale, le comunicazioni di crisi, la gestione dei fornitori, le procedure operative di emergenza.	Include piani per il backup e ripristino dei dati, il failover dei server, l'attivazione di siti di DR, la connettività di rete.
Quando si Attiva	Quando si verifica un evento che minaccia le operazioni aziendali (disastro naturale, interruzione di fornitura, attacco informatico).	Quando l'infrastruttura IT è compromessa o distrutta.

3. Comprendere il Concetto di ICT Readiness for Business Continuity (IRBC - ISO/IEC 27031)

L'**ICT readiness for business continuity (IRBC),** secondo la norma ISO/IEC 27031, è un concetto che si concentra sulla preparazione dell'Information and Communication Technology (ICT) per supportare la Business Continuity.
In altre parole, è una guida che ci dice cosa dobbiamo fare a livello tecnologico per assicurarci che la nostra infrastruttura IT sia pronta a rispondere a qualsiasi interruzione e a sostenere la ripresa delle attività aziendali.

Pensiamo all'ICT come al sistema nervoso dell'azienda, se il sistema nervoso si blocca, tutto il corpo ne risente.
La ISO/IEC 27031 non è un sostituto della ISO 22301 (che è la norma sulla Business Continuity a livello generale), ma piuttosto un suo complemento.
Essa fornisce delle linee guida specifiche per l'aspetto tecnologico, spiegando come pianificare, implementare, operare, monitorare, revisionare, mantenere e migliorare la "prontezza" dell'ICT.

Questa norma ci aiuta a:

- **Identificare le esigenze di BC legate all'ICT**:
  capire quali sono i requisiti tecnologici per supportare i processi aziendali critici.
- **Pianificare la capacità dell'ICT**:
  assicurarsi che l'infrastruttura IT possa sostenere le operazioni in caso di emergenza, magari avendo server di riserva o data center alternativi.
- **Garantire la disponibilità delle informazioni:**
  implementare misure per proteggere i dati e renderli accessibili quando servono, anche dopo un incidente.
- **Definire procedure di ripristino:**
  stabilire come e quando ripristinare i sistemi e i dati IT.
- **Testare regolarmente**:
  fare delle simulazioni per verificare che i piani funzionino davvero.

In sintesi, la ISO/IEC 27031 assicura che il lato tecnologico dell'azienda sia robusto, resiliente e ben preparato a supportare gli sforzi di continuità operativa, integrandosi perfettamente con il piano di Business Continuity più ampio.