W18D1 PRATICA EXTRA - TULLI ROBERTO
SECURITY OPERATION: AZIONI PREVENTIVE

ROMA 09/11/2025

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).

SVOLGIMENTO:

1) Che cos'è la **Business Continuity (BC)** e che cos'è il **Disaster Recovery (DR)**

Business Continuity (BC)
La Business Continuity è l'insieme di processi, procedure e risorse necessari per mantenere operative le funzioni aziendali essenziali durante e dopo un evento che causa interruzione (es. incendio, blackout, attacco informatico). L'obiettivo è limitare l'impatto sul business e continuare a fornire i servizi critici.

Elementi principali della BC:

- Analisi dei processi critici (quali funzioni non possono fermarsi).
- Valutazione dei rischi e delle priorità.
- Piani organizzativi e procedure operative alternative.
- Comunicazione interna ed esterna (dipendenti, clienti, fornitori).
- Test e esercitazioni periodiche.

Disaster Recovery (DR)
Il Disaster Recovery è una parte (specializzata) della Business Continuity focalizzata principalmente sul ripristino delle risorse tecnologiche (sistemi IT, dati, reti) dopo un disastro. Si occupa del "come riportare online" server, applicazioni e dati.

Elementi principali del DR:

- Backup dei dati e procedure di ripristino.
- Procedure per il ripristino di server, database e applicazioni.

- Test di recovery regolari.

Aspetto / Caratteristica	Business Continuity (BC)	Disaster Recovery (DR)
Scopo	Garantire la continuità delle funzioni aziendali	Ripristinare l'infrastruttura IT e i dati dopo un evento
Ambito	Tutta l'organizzazione (persone, processi, sedi, IT)	Principalmente infrastruttura IT e dati
Orizzonte temporale	Immediato e a medio-lungo termine (continuità operativa)	Focalizzato sul breve termine: ripristino tecnico
Attività principali	Procedure operative alternative, comunicazione, ruoli	Backup, ripristino server, replica dati, test di recovery
Metriche chiave	RTO processo, Priorità di servizio, impatto operativo	RTO (Recovery Time Objective), RPO (Recovery Point Objective)
Responsabilità tipiche	Management, Business Continuity Manager	IT, responsabile DR, team sysadmin
Testing	Esercitazioni integrate (prove con personale e processi)	Test tecnici di ripristino e restore dei dati
Esempio di azione	Ridistribuire attività su altra sede o lavoro remoto	Ripristinare database dal backup o avviare server in DR site

Spiegazione veloce di RTO e RPO:

- **RTO (Recovery Time Objective):** tempo massimo accettabile per ripristinare un servizio/processo.
- **RPO (Recovery Point Objective):** quantità massima di dati che si può tollerare perdere (es. backup ogni 4 ore → RPO = 4 ore).

---

3) ICT readiness for business continuity (IRBC — ISO/IEC 27031): concetto semplice

Cosa significa IRBC (ICT readiness for business continuity)?
IRBC è un insieme di attività e controlli mirati a rendere l’ICT (sistemi informativi, reti, dati) pronto a sostenere la continuità del business. L’ISO/IEC 27031 è lo standard che fornisce linee guida su come progettare e gestire questa “prontezza” tecnologica.

Obiettivo principale:

- Assicurare che le risorse ICT siano disponibili e funzionanti quando sono necessarie per sostenere le attività critiche dell’azienda.

Principali aree coperte dall’IRBC (semplice):

1. **Valutazione dei requisiti ICT**: capire quali sistemi e dati sono critici per l’azienda.
2. **Architettura e progettazione**: definire ridondanze, backup e siti di recovery.
3. **Procedure operative**: documentare come operare in caso di interruzione.
4. **Gestione terze parti**: accordi con fornitori e cloud provider per continuità.
5. **Test e manutenzione**: verifiche periodiche delle soluzioni di recovery.
6. **Comunicazione e formazione**: persone pronte a eseguire i piani.

Tabella: Componenti chiave di IRBC

Componente IRBC	Cosa include
Identificazione requisiti ICT	Elenco dei sistemi/dati essenziali e loro priorità
Progettazione infrastruttura	Ridondanza, siti secondari, replica dati, separazione geografica
Backup e restore	Politiche di backup, frequenza, test di restore
Monitoraggio e disponibilità	Controlli per rilevare problemi e reagire rapidamente
Sicurezza e accesso	Controlli di accesso, cifratura dei backup, protezione dati
Comunicazione con stakeholder	Piani di contatto per informare personale, clienti e fornitori
Test e esercitazioni	Esercizi regolari che valutano la capacità di recovery
Gestione fornitori	SLA, contratti che garantiscono supporto in emergenza

Come implementare IRBC / ISO 27031: passi pratici

1. **Inventario dei servizi critici**
    - Elencare applicazioni, server, database e processi aziendali critici.
    - Per ogni elemento definire RTO e RPO.
2. **Valutazione del rischio e impatto**
    - Valutare che cosa potrebbe interrompere quei servizi e che impatto avrebbero (persone, fatturato, reputazione).
3. **Progettare soluzioni tecnologiche**
    - Decidere backup, repliche, siti secondari, cloud o on-premise.
    - Prevedere meccanismi di ridondanza e accesso sicuro.
4. **Definire responsabilità e procedure**
    - Chi fa cosa durante l'incidente (nomina responsabili).

- Scrivere procedure passo-passo di recovery e di comunicazione.

5. **Testare regolarmente**
    - Eseguire test di restore, esercitazioni con il personale e simulazioni.
    - Correggere le lacune emerse.
6. **Manutenere e aggiornare**
    - Aggiornare piani e infrastrutture quando cambiano processi o tecnologie.
7. **Coinvolgere terze parti**
    - Assicurare che i fornitori rispettino gli SLA e che abbiano piani di continuità.