# Traccia 1

1. Descriva come implementerebbe all’interno di un Ente di Ricerca come l’OGS la seguente Misure di sicurezza di base per i soggetti importanti:
   **ID.RA-01: Le vulnerabilità negli asset sono identificate, confermate e registrate.**

2. Descriva alcune tecniche per aumentare la sicurezza dell’autenticazione ed autorizzazione di utenti, server e servizi.

3. Descriva come implementerebbe all'interno di un Ente di Ricerca la gestione del rischio cyber legato alla catena di approvvigionamento (Supply Chain Risk Management) e ai rapporti con i fornitori di servizi IT.

4. Per i servizi istituzionali che richiedono un funzionamento h24 (come il monitoraggio sismico a supporto della Protezione Civile), descriva i concetti di **RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)** e come strutturerebbe una strategia di Disaster Recovery

# Traccia 2

1. Descriva come implementerebbe all’interno di un Ente di Ricerca come l’OGS la seguente Misure di sicurezza di base per i soggetti importanti:
   **ID.IM-04: I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.**

2. Descriva le metodologie e le soluzioni tecnologiche (architetturali e di endpoint) necessarie per garantire la sicurezza degli accessi remoti e del personale in regime di lavoro agile (smart working).

3. Descriva il ruolo e le componenti principali di un'architettura di monitoraggio continuo della sicurezza (SIEM/SOC), evidenziando come questa possa integrarsi in un Ente pubblico per identificare tempestivamente le minacce.

4. Descriva le tecniche più utili per proteggere gli asset dell’ente da attacchi di tipo ransomware

# Traccia 3

1. Descriva come implementerebbe all'interno di un Ente di Ricerca come l'OGS la seguente Misure di sicurezza di base per i soggetti importanti:
   **PR.AA-05: I permessi, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del minimo privilegio e della separazione dei compiti.**

2. Descriva alcune tecniche per aumentare la sicurezza di una rete LAN aziendale

3. Descriva le strategie di protezione dei dati, con particolare riferimento alle politiche di cifratura (at-rest e in-transit) e alle architetture di backup (es. regola 3-2-1, immutabilità) per garantire la resilienza contro attacchi di tipo Ransomware.

4. Descriva le fasi del processo di Incident Management e la composizione di un Crisis Management Team (CMT) in caso di incidente informatico grave.

Fabiana Brancolini
06.07.2026
08:23:07
GMT+02:00