ALLEGATO 06

TRACCIA B

Quesito 1 – Storage, backup e continuità operativa:

Dopo un'analisi dei rischi, l'Amministrazione decide di rivedere la protezione dei dati di VM e condivisioni di rete ospitate presso uno o più fornitori cloud, su servizi IaaS, PaaS, SaaS o storage generico.

Questo vale in particolare per lo scenario di un attacco ransomware che colpisca contemporaneamente i sistemi di produzione e i backup tradizionali.

Il candidato progetti una soluzione di storage, backup e disaster recovery, descrivendo:

1. la classificazione dei sistemi per criticità e i relativi obiettivi di RPO e RTO, anche con una tabella di esempio;
2. l'architettura di backup: strumenti, frequenze, Retention, applicazione della regola 3-2-1 o 3-2-1-1-0, copie immutabili o air-gapped, cifratura;
3. le differenze tecniche tra snapshot, replica e backup, e il ruolo di ciascuno nella soluzione proposta;
4. Come organizzerebbe il ripristino dei servizi in un sito o cloud alternativo, garantendo l'accesso dalle sedi anche in caso di guasto a un collegamento? Non sono richiesti calcoli.
5. le procedure di verifica periodica (test di restore, esercitazioni DR) e i ruoli organizzativi coinvolti.

Quesito 2:

Quali sono le differenze tra backup, Business Continuity e Disaster Recovery in termini di finalità?

Quesito 3:

Descrivi la differenza tra RTO e RPO nell'ambito Business Continuity/Disaster Recovery e Backup in generale.

Quesito 4:

Come dimensionerebbe i collegamenti WAN e le reti locali necessari per replica e ripristino, tenendo conto di quantità dei dati, finestra disponibile, latenza, banda effettiva, traffico ordinario e priorità dei servizi?

TRACCIA NON SVOLTA

NB