Traccia:
In questo esercizio, ipotizzeremo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia. Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»

ALE=AROxSLE

ARO

terremoto 1 volta ogni 30anni = 0.0333
incendio 1 volta ogni 20 anni= 0,05
inondazione 1 ogni 50 anni = 0,02

Inondazione sull'asset «edificio secondario»

valore= 150.000€
EF = 40%= 0,04

SLE (valore asset x EF) =60.000€
ALE= 1.200€

Terremoto sull'asset «datacenter»

valore =100.000€
EF 95%=0,95

SLE=95.000€
ALE=3166,67€

Incendio sull'asset «edificio primario»

valore=350.000€
EF 60%=0.60

SLE=210.000€
ALE=10.500€

Incendio sull’asset «edificio secondario»

valore=150.000€
EF= 50%=0.05

SLE=75.000€
ALE=3.750€

Estendere l’esercizio precedente andando a valutare:
- Inondazione sull’asset «edificio primario»;
- Terremoto sull’asset «edificio primario».

Inondazione sull’asset «edificio primario»

valore=350.000€
EF= 55%=0.55

SLE=192.500€
ALE=3.850€

Terremoto sull’asset «edificio primario».

valore= 350.000€
EF= 80%=0,80

SLE=280.000€
ALE=9.324€

FACOLTATIVO

Successivamente, scegli uno scenario tra quelli proposti e definisci:
- cosa si intende per Confidenzialità, Integrità e Disponibilità dei dati;
- potenziali minacce alla Confidenzialità, Integrità e Disponibilità dei dati;
- contromisure per proteggere i dati da queste minacce.

Scenario scelto: Terremoto sul datacenter

Il datacenter è una parte essenziale per qualsiasi azienda, poiché ospita i server e i sistemi che gestiscono i dati critici. Un terremoto potrebbe causare seri danni al datacenter, con un impatto importante sulla **Confidenzialità, Integrità e Disponibilità** dei dati, cioè sui principi fondamentali della sicurezza delle informazioni.

Cosa significano Confidenzialità, Integrità e Disponibilità?

- **Confidenzialità:** La confidenzialità significa tenere i dati al sicuro da occhi indiscreti. Solo le persone autorizzate dovrebbero avere accesso alle informazioni, soprattutto quando si tratta di dati sensibili come informazioni sui clienti o progetti aziendali.
- **Integrità:** L'integrità riguarda il mantenimento dei dati così come sono stati creati o memorizzati, senza che vengano alterati o corrotti. Un esempio potrebbe essere garantire che nessuno modifichi i dati finanziari di un'azienda per errore o intenzionalmente.
- **Disponibilità:** La disponibilità significa che i dati devono essere accessibili quando servono. Se un terremoto interrompe l'accesso ai server, le persone che hanno bisogno di quei dati per lavorare potrebbero trovarsi bloccate.

Possibili minacce per la Confidenzialità, Integrità e Disponibilità dei dati in caso di terremoto

- **Confidenzialità:**
    - Se il terremoto danneggia i sistemi di sicurezza o il controllo degli accessi, potrebbe esserci il rischio che persone non autorizzate accedano ai dati del datacenter.
    - Il caos dopo il disastro potrebbe portare a furti di hardware, come server o dischi rigidi, contenenti dati sensibili.
- **Integrità:**
    - Il danno fisico ai server o agli hard disk potrebbe corrompere i dati, rendendoli inutilizzabili o imprecisi.
    - Se qualcuno accede al datacenter in modo non controllato durante l'emergenza, potrebbe modificare o cancellare informazioni importanti.
- **Disponibilità:**
    - Un terremoto potrebbe danneggiare la rete elettrica o i cavi di connessione, rendendo impossibile accedere ai sistemi e ai dati per giorni o settimane.
    - Se i server del datacenter vengono danneggiati, i dati potrebbero non essere disponibili fino a quando non vengono riparati o sostituiti.

Come proteggere i dati da queste minacce?

- **Per la Confidenzialità:**
  - **Crittografia:** Criptare i dati significa renderli illeggibili a chi non ha le chiavi per decrittarli. Questo garantisce che, anche se qualcuno riuscisse ad accedere ai server, non potrebbe leggere le informazioni senza le autorizzazioni corrette.
  - **Accesso controllato:** Bisogna rafforzare il controllo su chi può accedere ai dati, utilizzando sistemi di autenticazione forti, come l'autenticazione a più fattori (ad esempio, password + codice sul telefono).
  - **Sicurezza fisica:** Avere misure di sicurezza fisica come videocamere e guardie aiuta a proteggere il datacenter da accessi non autorizzati, specialmente in situazioni di emergenza.
- **Per l'Integrità:**
  - **Backup:** È fondamentale fare copie regolari dei dati (backup), magari in un luogo fisicamente lontano, così che se qualcosa va storto, sia possibile ripristinare una versione recente e integra dei dati.
  - **Controllo delle versioni:** Usare sistemi che tengano traccia di tutte le modifiche ai dati permette di tornare indietro a versioni precedenti in caso di problemi, evitando che modifiche non autorizzate o errori compromettano le informazioni.
  - **Strumenti di verifica:** Strumenti che controllano automaticamente se i dati sono stati corrotti possono individuare problemi di integrità e segnalare subito.
- **Per la Disponibilità:**
  - **Piano di emergenza:** Avere un piano di disaster recovery (recupero dai disastri) significa essere preparati con strategie su come ripristinare i sistemi e i dati dopo un evento come un terremoto.
  - **Ridondanza:** Distribuire i dati in diversi luoghi (ad esempio, in datacenter remoti o nel cloud) assicura che, anche se il datacenter principale è danneggiato, i dati siano comunque accessibili.
  - **Alimentazione di riserva:** Avere generatori di emergenza e batterie di riserva per mantenere i server accesi è essenziale per evitare interruzioni improvvise.