W18D4 – Pratica

Epic Education Srl

Annualized Loss Expectancy
CIA terremoto sul datacenter

Simone Giordano

11/11/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Annualized Loss Expectancy

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

Dati:

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Esercizio

Per calcolare la perdita annuale **Annualized Loss Expectancy (ALE)**, bisogna calcolare la **Single Loss Expectancy (SLE)**, moltiplicando l'**Asset Value (AV)** per l'**Exposed Factor (EF)**. Una vota ottenuto il valore di SLE otteniamo la perdita annuale ALE, moltiplicando SLE per ARO.

Ricapitolando:

SLE = AV x EF
ALE = SLE x ARO

Asset	Valore (AV)	Evento	ARO/anno	EF	SLE	ALE
Edificio secondario	150.000 €	Inondazione	0,02	40%	60.000 €	**1.200 €**
Datacenter	100.000 €	Terremoto	0,033	95%	95.000 €	**3.135 €**
Edificio primario	350.000 €	Incendio	0,05	60%	210.000 €	**10.500 €**
Edificio secondario	150.000 €	Incendio	0,05	50%	75.000 €	**3.750 €**

CIA terremoto sul datacenter

esercizio extra

Traccia

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

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.

Esercizio

Asset	Valore (AV)	Evento	ARO/anno	EF	SLE	ALE
Edificio primario	35.000 €	Inondazione	0,02	55%	19.250 €	**385 €**
Edificio primario	35.000 €	Terremoto	0,033	80%	28.000 €	**924 €**

Terremoto sull'asset "Data center"

Confidenzialità, Integrità e Disponibilità dei dati

Confidenzialità significa che i dati possono essere visti solo da chi è autorizzato. Anche durante o dopo il terremoto nessuno deve poter accedere a informazioni sensibili approfittando del caos.

Integrità significa che i dati non devono essere alterati in modo non autorizzato. Un sisma può danneggiare infrastrutture e causare corruzione dei dati, quindi è fondamentale garantire che ciò che era memorizzato resti esatto e utilizzabile.

Disponibilità significa che i dati devono essere accessibili quando servono. Il terremoto può mettere fuori uso server, connettività o alimentazione, quindi è importante mantenere i servizi attivi o rapidamente recuperabili.

Potenziali minacce alla Confidenzialità, Integrità e Disponibilità

Confidenzialità
- Accesso fisico non autorizzato al datacenter danneggiato.
- Furto di supporti di memoria o server durante e dopo l'evacuazione.

Integrità
- Corruzione dei dati per danni fisici ai dischi.
- Manipolazioni dovute a guasti elettrici, sbalzi di tensione o shock hardware.

Disponibilità

- Interruzione dell'alimentazione elettrica.
- Danni strutturali al datacenter che contengono i dati.

Contromisure per proteggere i dati

Confidenzialità

- Crittografia dei dati.
- Controlli di accesso forti, badge, biometria, sorveglianza fisica.
- Segmentazione per proteggere anche la rete di emergenza.

Integrità

- Backup regolari.
- Replica dei dati in siti geografici distinti.
- Alimentazione protetta con UPS e protezioni da sbalzi elettrici.

Disponibilità

- Ridondanza dei sistemi e failover automatico verso un sito secondario.
- Data center geograficamente distribuiti (strategia di disaster recovery).
- Sistemi di alimentazione d'emergenza (generatori, UPS)
- Piano di Disaster Recovery chiaramente definito, testato e aggiornato.