

Business continuity & disaster recovery

Introduzione

La presente relazione ha lo scopo di valutare l'impatto quantitativo di un determinato disastro su un asset di una compagnia, applicando i concetti teorici di business continuity e disaster recovery. Attraverso l'analisi dei dati forniti, si procederà al calcolo della perdita annuale attesa, al fine di quantificare il rischio associato all'evento in esame.

Calcolo della Perdita Annuale:

Per calcolare la perdita annuale attesa, si utilizzerà la seguente formula:

- **Perdita Annuale:**

$$(SLE) = (AV) \times (EF)$$

$$(ALE) = (SLE) \times (ARO)$$

- **SLE: (Single Loss Expectancy)** Rappresenta il costo stimato di una singola occorrenza del disastro.
- **ARO: (Annualized Rate of Occurrence)** Indica la probabilità che il disastro si verifichi in un anno.
- **AV: (Asset Valute)** indica il Valore del immobile.
- **EF: (Exposure Factor)** indica la ricorrenza di quell'evento.
- **ALE: (Annual Loss Expectancy)** indica la stima del costo finanziario medio che un'organizzazione si aspetta di sostenere a causa di un particolare evento negativo in un anno.

DATI:

-Inondazione sull'asset «edificio secondario»

-Terremoto sull'asset «datacenter»

-Incendio sull'asset «edificio primario»

-Incendio sull'asset «edificio secondario»

-Inondazione sull'asset «edificio primario»

-Inondazione sull'asset «edificio secondario»

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 (EF)	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Calcolo:

1)Inondazione sull’asset «edificio secondario»

$SLE = AV \times EF = 150.000 \times 0,40 = 60.000€$

$ALE = SLE \times ARO = 60.000€ \times 0,02 = 1.200€$

2)Terremoto sull’asset «datacenter»

$SLE = AV \times EF = 100.000€ \times 0,95 = 95.000€$

$ALE = SLE \times ARO = 95.000€ \times 0,03 = 2.850€$

3)Incendio sull'asset «edificio primario»

$$\text{SLE} = \text{AV} \times \text{EF} = 350.000\text{€} \times 0,60 = 210.000\text{€}$$

$$\text{ALE} = \text{SLE} \times \text{ARO} = 210.000\text{€} \times 0,05 = 10.500\text{€}$$

4)Incendio sull'asset «edificio secondario»

$$\text{SLE} = \text{AV} \times \text{EF} = 150.000\text{€} \times 0,50 = 75.000\text{€}$$

$$\text{ALW} = \text{SLE} \times \text{ARO} = 75.000\text{€} \times 0,05 = 3750\text{€}$$

5)Inondazione sull'asset «edificio primario»

$$\text{SLE} = \text{AV} \times \text{EF} = 350.000\text{€} \times 0,55 = 192.500\text{€}$$

$$\text{ALW} = \text{SLE} \times \text{ARO} = 192.500\text{€} \times 0,02 = 3850\text{€}$$

6)Inondazione sull'asset «edificio secondario»

$$\text{SLE} = \text{AV} \times \text{EF} = 150.000\text{€} \times 0,40 = 60000\text{€}$$

$$\text{ALW} = \text{SLE} \times \text{ARO} = 60000\text{€} \times 0,02 = 1200\text{€}$$

Conclusioni

In base ai calcoli effettuati, si può concludere che si devono prendere in considerazione le seguenti misure di sicurezza:

Miglioramento delle misure di prevenzione: Implementare misure preventive per ridurre la probabilità che si verifichi un disastro (es. sistemi antincendio, controlli di sicurezza, manutenzione preventiva).

Potenziamento dei sistemi di backup: Aumentare la frequenza dei backup e implementare soluzioni di backup per garantire la protezione dei dati.

Definizione di un piano di risposta all'emergenza: Elaborare un piano dettagliato che descriva le azioni da intraprendere in caso di disastro, assegnando ruoli e responsabilità a ciascun dipendente.

Test regolari del piano: Effettuare periodicamente dei test del piano di risposta per verificarne l'efficacia e individuare eventuali aree di miglioramento.

Formazione del personale: Fornire al personale la formazione necessaria per affrontare le emergenze e conoscere le procedure da seguire.

Raccomandazioni specifiche :

- **Se il rischio più elevato è legato a un disastro naturale:** Valutare la possibilità di relocare l'asset in una zona meno esposta, stipulare polizze assicurative adeguate o implementare sistemi di monitoraggio ambientale.
- **Se il rischio più elevato è legato a un incidente informatico:** Rafforzare la sicurezza informatica, implementare sistemi di rilevamento delle intrusioni e effettuare regolari aggiornamenti dei software.
- **Se il rischio più elevato è legato a un guasto tecnico:** Aumentare la ridondanza dei sistemi critici, implementare procedure di manutenzione preventiva e disporre di componenti di ricambio.