Valutazione dell’impatto finanziario sui beni aziendali in caso di disastri

Veniamo incaricati di analizzare l’impatto economico che diversi disastri naturali o incidenti potrebbero avere su alcuni asset aziendali. L’obiettivo è calcolare la perdita annuale stimata (ALE - Annual Loss Expectancy) nel caso di disastri come inondazioni, terremoti o incendi. Il metodo che utilizzeremo si basa sulla formula dell’ALE, che è il prodotto tra la Perdita Singola Stimata (SLE) e la Frequenza Annuale dell'Evento (ARO).

La SLE (Single Loss Expectancy) rappresenta la perdita economica in caso di un singolo evento ed è calcolata moltiplicando il valore dell’asset per il fattore di esposizione (EF). Questo fattore indica la percentuale di danno che un determinato evento potrebbe causare all’asset. L’ARO (Annual Rate of Occurrence), invece, rappresenta la frequenza annuale stimata di accadimento dell'evento e si ottiene dividendo 1 per il numero di anni in cui è previsto che l’evento si verifichi.

Analizziamo ora ciascuna delle situazioni che ci sono state presentate.

Nel caso di un’inondazione sull’edificio secondario, il valore dell'asset è pari a **150.000€**, mentre il fattore di esposizione per un’inondazione è del **40%**. Questo significa che, in caso di inondazione, si prevede una perdita del **40%** del valore dell’edificio. La frequenza stimata per un’inondazione è di **1 volta ogni 50 anni**, quindi l’ARO è **1/50**. La Perdita Singola Stimata (SLE) sarà dunque **150.000€ moltiplicato per 0,40**, che dà come risultato **60.000€**. Moltiplicando questa cifra per l'ARO, si ottiene la perdita annuale stimata (ALE), pari a **1.200€**. Pertanto, la perdita annuale che la compagnia subirebbe per un’inondazione sull’edificio secondario è di **1.200€**.

Considerando ora l'impatto che un terremoto avrebbe sul datacenter, il valore dell’asset è di **100.000€**, e il fattore di esposizione in questo caso è del **95%**, il che riflette l’alto rischio di danni gravi. La frequenza stimata di un terremoto è di **1 volta ogni 30 anni**, quindi l’ARO è **1/30**. La SLE, moltiplicando il valore del datacenter per il fattore di esposizione (**100.000€ × 0,95**), è pari a **95.000€**. Calcolando la perdita annuale, si ottiene un ALE pari a **95.000€ moltiplicato per 1/30**, che dà come risultato **3.166,67€**. Di conseguenza, la perdita annuale stimata per un terremoto che colpisca il datacenter è di **3.166,67€**.

Per quanto riguarda l’impatto di un incendio sull’edificio primario, il valore dell’asset è pari a **350.000€**, mentre il fattore di esposizione per un incendio è del **60%**. Questo significa che, in caso di incendio, si stima una perdita del **60%** del valore dell’edificio. La frequenza stimata per un incendio è di **1 volta ogni 20 anni**, quindi l’ARO è **1/20**. La SLE, moltiplicando il valore dell’edificio per il fattore di esposizione (**350.000€ ×**

0,60), è pari a **210.000€**. La perdita annuale stimata, calcolando l'ALE come **210.000€ moltiplicato per 1/20**, è pari a **10.500€**. Quindi, la perdita annuale stimata per un incendio sull'edificio primario è di **10.500€**.

Infine, nel caso di un incendio sull'edificio secondario, il valore dell'asset è pari a **150.000€**, mentre il fattore di esposizione per un incendio è del **50%**. Questo significa che si prevede una perdita del **50%** del valore dell'edificio. La frequenza stimata per un incendio è di **1 volta ogni 20 anni**, quindi l'ARO è **1/20**. La SLE, moltiplicando il valore dell'edificio per il fattore di esposizione (**150.000€ × 0,50**), è pari a **75.000€**. La perdita annuale stimata sarà dunque **75.000€ moltiplicato per 1/20**, che dà come risultato **3.750€**. Di conseguenza, la perdita annuale stimata per un incendio sull'edificio secondario è di **3.750€**.

In conclusione, dai calcoli effettuati possiamo determinare che le perdite annuali attese per i vari scenari sono: **1.200€** per un'inondazione sull'edificio secondario, **3.166,67€** per un terremoto sul datacenter, **10.500€** per un incendio sull'edificio primario, e **3.750€** per un incendio sull'edificio secondario. Questi valori offrono una visione chiara delle possibili perdite economiche, consentendo all'azienda di prendere decisioni informate sulle strategie di gestione del rischio e le eventuali misure preventive da adottare.

FACOLTATIVO

Dopo aver esaminato gli scenari iniziali, estendiamo l'analisi valutando l'impatto di un'inondazione e di un terremoto sull'asset «edificio primario». Come fatto in precedenza, utilizziamo la formula dell'ALE (Annual Loss Expectancy), che è il prodotto tra la Perdita Singola Stimata (SLE) e la Frequenza Annuale dell'Evento (ARO).

Nel caso di un'inondazione sull'edificio primario, il valore dell'asset è pari a **350.000€**. Il fattore di esposizione (EF) per un'inondazione su questo asset è del **55%**, il che indica che un'inondazione potrebbe danneggiare circa il 55% del valore dell'edificio. La frequenza stimata dell'evento (ARO) è di **1 volta ogni 50 anni**, quindi l'ARO è **1/50**. La Perdita Singola Stimata (SLE) è quindi **350.000€ moltiplicato per 0,55**, che dà come risultato **192.500€**. Moltiplicando questa cifra per l'ARO, si ottiene la perdita annuale stimata (ALE), pari a **3.850€**. Pertanto, la perdita annuale che la compagnia subirebbe per un'inondazione sull'edificio primario è di **3.850€**.

Considerando ora l'impatto di un terremoto sull'edificio primario, il valore dell'asset è di **350.000€** e il fattore di esposizione per un terremoto è dell'**80%**, riflettendo il fatto che un terremoto potrebbe causare danni sostanziali a questa infrastruttura. La frequenza stimata (ARO) per un terremoto è di **1 volta ogni 30 anni**, quindi l'ARO è **1/30**. La SLE, moltiplicando il valore dell'edificio per il fattore di esposizione (**350.000€ × 0,80**), è pari a **280.000€**. Moltiplicando questa cifra per l'ARO, otteniamo l'ALE, che risulta essere **9.333,33€**. Pertanto, la perdita annuale stimata per un terremoto sull'edificio primario è di **9.333,33€**.

Passando all'analisi dei dati nel contesto di un disastro come il terremoto sull'edificio primario, possiamo esaminare i concetti di Confidenzialità, Integrità e Disponibilità. La **Confidenzialità** si riferisce alla protezione delle informazioni dall'accesso non autorizzato, assicurando che solo persone o sistemi autorizzati possano accedere ai dati. In uno scenario di disastro come un terremoto, le infrastrutture critiche potrebbero subire danni e i dati aziendali potrebbero essere esposti a minacce esterne o interne se non adeguatamente protetti. L'**Integrità** implica che i dati devono rimanere accurati e completi, senza alterazioni non autorizzate o non intenzionali. Un terremoto potrebbe, ad esempio, causare interruzioni nei sistemi di memorizzazione, danneggiare i server o causare corruzione dei dati. Infine, la **Disponibilità** significa che i dati devono essere accessibili quando necessario. Se un terremoto distrugge le infrastrutture fisiche come i data center, i sistemi potrebbero non essere più in grado di fornire accesso ai dati, bloccando l'operatività aziendale.

Le principali minacce alla confidenzialità includono l'accesso non autorizzato ai dati. In uno scenario di emergenza, potrebbero verificarsi situazioni in cui l'accesso ai

server o alle reti aziendali viene temporaneamente meno, esponendo i dati a potenziali violazioni da parte di terzi. Per quanto riguarda l'integrità, le minacce includono la corruzione dei dati, che può avvenire durante un disastro fisico come un terremoto, quando i sistemi informatici sono soggetti a shock fisici o interruzioni improvvise di energia, che potrebbero danneggiare file o database. Le minacce alla disponibilità si concretizzano principalmente nella distruzione fisica delle infrastrutture, che può rendere i dati e i sistemi non disponibili. La perdita di accesso ai data center o ai sistemi di backup a causa di un terremoto può causare un fermo operativo.

Per mitigare le minacce alla confidenzialità, le aziende dovrebbero adottare **sistemi di crittografia** avanzati, garantendo che i dati siano protetti anche se le infrastrutture fisiche vengono compromesse. L'implementazione di **accessi basati su ruoli (RBAC)** può limitare l'accesso ai dati a utenti specifici, riducendo i rischi di accessi non autorizzati. Per proteggere l'integrità dei dati, è importante disporre di **sistemi di backup regolari** che garantiscano che copie accurate dei dati siano disponibili anche in caso di guasti fisici. L'uso di **hashing** per verificare che i dati non siano stati alterati e la presenza di **controlli di ridondanza** possono aiutare a garantire l'integrità dei dati. Infine, per garantire la disponibilità dei dati, l'adozione di **soluzioni di disaster recovery** e **infrastrutture ridondanti** è fondamentale. Sistemi di backup basati sul cloud, che non dipendono da un singolo sito fisico, possono garantire che i dati siano sempre accessibili. L'utilizzo di **data center geograficamente distribuiti** può ridurre l'impatto di un disastro naturale localizzato come un terremoto.

In conclusione, l'analisi estesa ci ha permesso di calcolare le perdite annuali attese per un'inondazione sull'edificio primario (**3.850€**) e un terremoto sullo stesso edificio (**9.333,33€**). Abbiamo anche esplorato i concetti di Confidenzialità, Integrità e Disponibilità dei dati nel contesto di un terremoto, identificando le principali minacce e le contromisure che possono essere adottate per proteggere i dati da tali minacce. Questi accorgimenti permettono di garantire la sicurezza dei dati anche in scenari di emergenza.