Il presente elaborato estende l'esercizio di valutazione quantitativa del rischio precedentemente svolto, includendo ulteriori scenari di impatto sugli asset aziendali. Successivamente, viene analizzato uno scenario selezionato dal punto di vista della sicurezza delle informazioni, con riferimento ai principi di Confidenzialità, Integrità e Disponibilità dei dati.

Estensione dei calcoli quantitativi

Inondazione sull'asset "edificio primario"

Il valore dell'asset edificio primario è pari a 350.000 €.
L'Exposure Factor associato all'evento inondazione è del 55%.
La frequenza dell'evento è pari a una volta ogni 50 anni, corrispondente a un ARO di 0,02.
SLE = 350.000 € × 0,55 = 192.500 €
ALE = 192.500 € × 0,02 = **3.850 € / anno**

Terremoto sull'asset "edificio primario"

Il valore dell'asset edificio primario è pari a 350.000 €.
L'Exposure Factor associato all'evento terremoto è dell'80%.
La frequenza dell'evento è pari a una volta ogni 30 anni, corrispondente a un ARO di 0,033.
SLE = 350.000 € × 0,80 = 280.000 €
ALE = 280.000 € × 0,033 = **9.333,33 € / anno**

Analisi di sicurezza delle informazioni (CIA)

Scenario analizzato: terremoto sull'asset "datacenter"
Il datacenter rappresenta un asset critico in quanto ospita sistemi informativi e dati essenziali per il funzionamento dell'organizzazione.
Un evento sismico può compromettere non solo le infrastrutture fisiche, ma anche la sicurezza delle informazioni gestite.

Confidenzialità

La confidenzialità riguarda la protezione dei dati da accessi non autorizzati.
Nel caso di un terremoto, la distruzione o il danneggiamento delle infrastrutture può esporre i sistemi a accessi fisici non controllati, furti di dispositivi o perdita dei supporti di memorizzazione.

Minacce principali

- Accesso fisico non autorizzato ai server,
- Furto di dispositivi di storage,
- Esposizione di dati sensibili durante le operazioni di emergenza.

Contromisure

- Crittografia dei dati a riposo,
- Controlli di accesso fisico ai locali del datacenter,
- Procedure di sicurezza per la gestione delle emergenze.

Integrità

L'integrità dei dati garantisce che le informazioni non vengano alterate in modo non autorizzato o accidentale.
Un terremoto può causare danneggiamenti hardware, corruzione dei dati o interruzioni improvvise dei sistemi.

Minacce principali

- Corruzione dei database,
- Perdita di dati durante arresti improvvisi,
- Errori nei processi di ripristino.

Contromisure

- Backup periodici e verificati,
- Sistemi di controllo dell'integrità dei dati,
- Procedure di ripristino testate regolarmente.

Disponibilità

La disponibilità assicura che i dati e i servizi siano accessibili quando necessario.
Un evento sismico può causare lunghi periodi di indisponibilità dei sistemi informativi.

Minacce principali

- Interruzione dei servizi IT,
- Inaccessibilità dei dati critici,
- Ritardi operativi significativi.

Contromisure

- Soluzioni di disaster recovery,
- Datacenter ridondanti o geografici,
- Piani di business continuity.

Conclusione

L'estensione dell'analisi quantitativa e l'approfondimento sugli aspetti di sicurezza delle informazioni evidenziano come la gestione del rischio debba integrare valutazioni economiche e misure di protezione dei dati.
Un approccio strutturato consente di ridurre l'impatto degli eventi critici e di garantire la continuità operativa dell'organizzazione anche in scenari avversi.