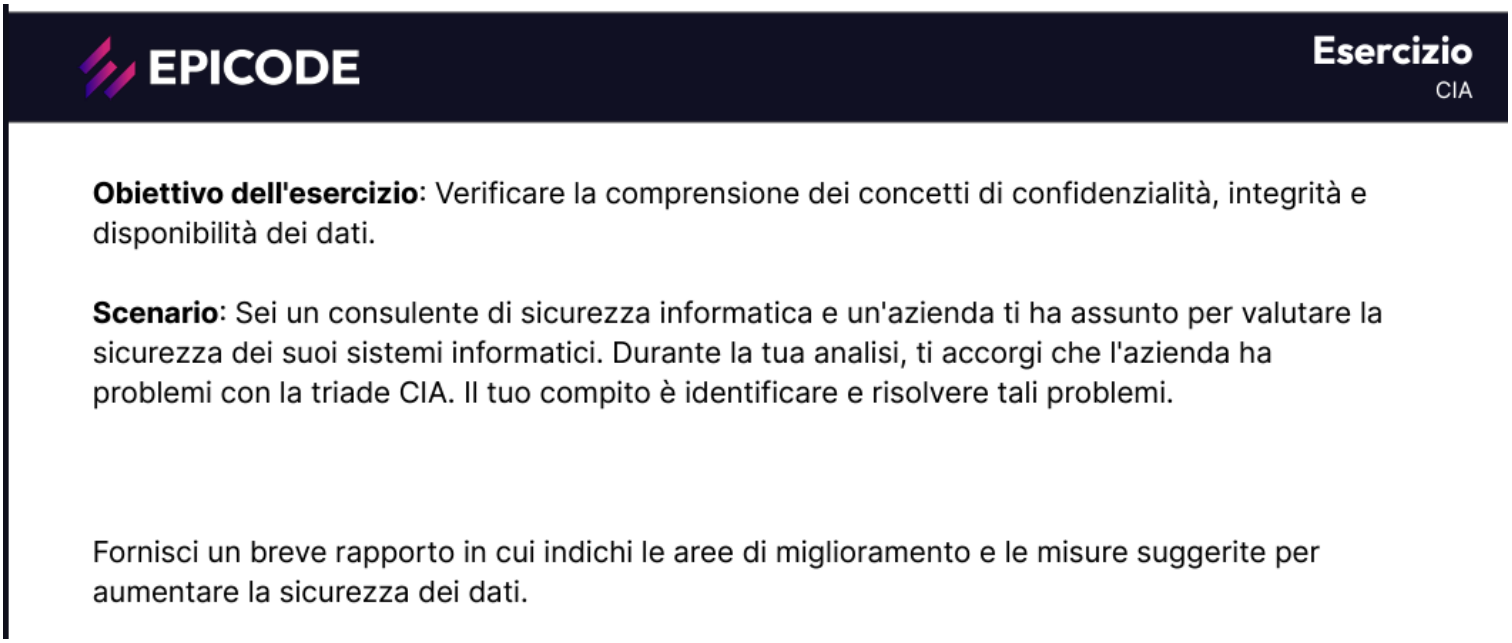
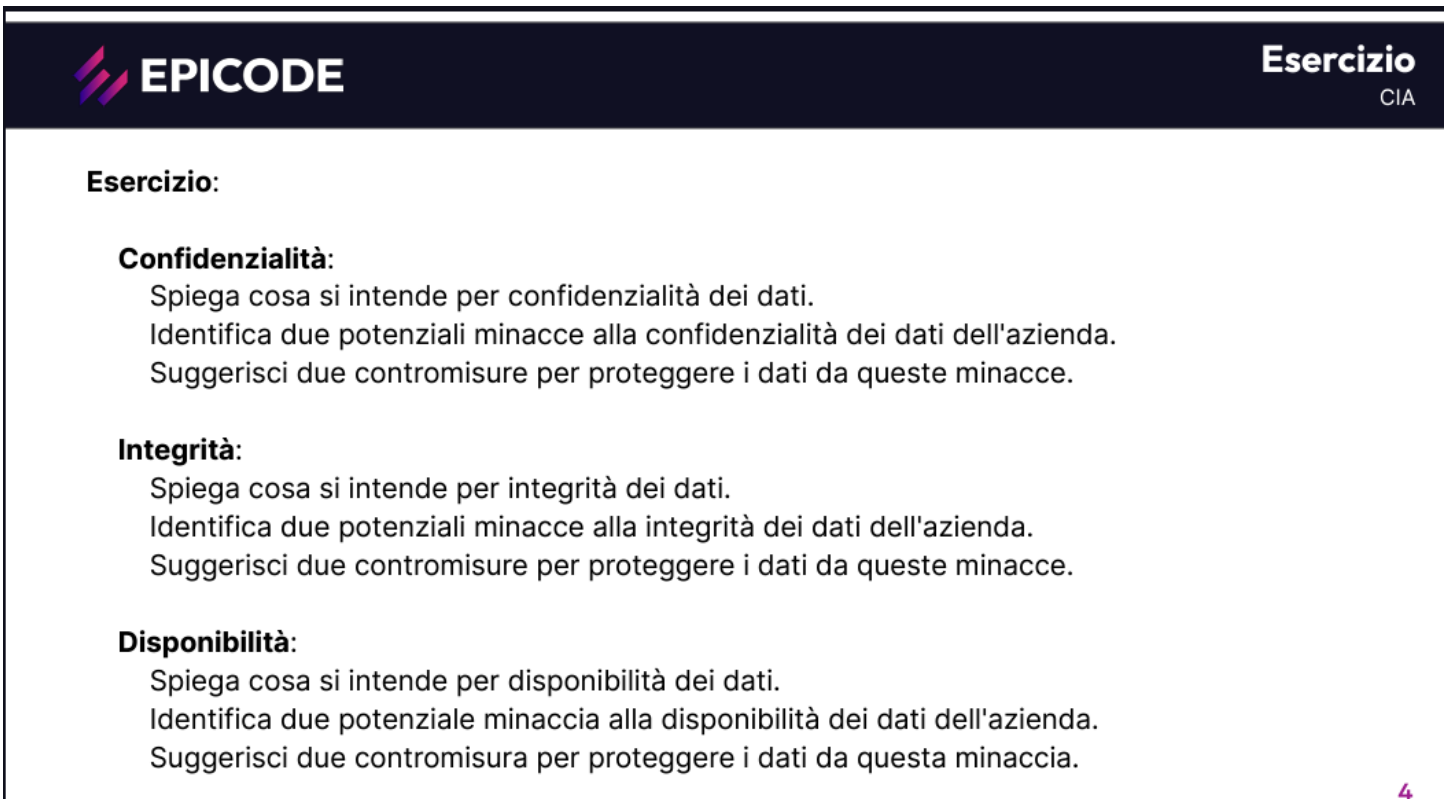
ESERCITAZIONE W18D1(2)





Rapporto di Analisi di Sicurezza Informatica

- Il primo principio della triade CIA è la confidenzialità. La confidenzialità dei dati si riferisce alla garanzia che le informazioni sensibili siano accessibili solo a coloro che sono autorizzati a visualizzarle. Questo implica proteggere i dati da accessi non autorizzati o divulgazioni non intenzionali. Le potenziali minacce alla confidenzialità dei dati possono essere:

  1. Accesso non autorizzato da parte di ex dipendenti, gruppi di hacker o competitors.

2. Attacchi esterni come hacking o phishing mirati a ottenere credenziali d'accesso.

Contromisure suggerite:

1. Implementare un rigoroso controllo degli accessi basato sul principio del privilegio minimo, che limita l'accesso solo alle risorse necessarie per svolgere il lavoro.

2. Utilizzare l'autenticazione a due fattori per aggiungere un livello aggiuntivo di sicurezza alle credenziali d'accesso.

- Il secondo principio della triade CIA è l'integrità, ovvero il concetto di proteggere l'affidabilità e la correttezza del dato. L'integrità dei dati riguarda la protezione dei dati da modifiche non autorizzate o alterazioni involontarie. È importante garantire che i dati mantengano la loro precisione e affidabilità nel tempo. Le potenziali minacce all'Integrità dei dati possono essere:

  1. Modifiche non autorizzate ai dati da parte di utenti interni malintenzionati o da attaccanti esterni.

  2. Errori umani durante l'aggiornamento o la manipolazione dei dati, che possono portare a dati incoerenti o danneggiati.

  Contromisure suggerite:

  1. Implementare controlli di accesso e autorizzazione rigorosi per impedire a utenti non autorizzati di modificare i dati.

  2. Utilizzare firme digitali o hash crittografici per verificare l'integrità dei dati durante il trasferimento e l'archiviazione.

- Il terzo ed ultimo principio della triade CIA è la disponibilità del dato, che deve essere garantita in ogni momento e per i soli utenti autorizzati ad accedere alla risorsa in oggetto. La disponibilità dei dati si riferisce alla capacità di accedere ai dati quando necessario. È cruciale garantire che i servizi e le risorse siano disponibili in modo affidabile per gli utenti autorizzati. Le potenziali minacce alla disponibilità dei dati possono essere:

  1. Attacchi di tipo Denial-of-Service (DoS) o Distributed Denial-of-Service (DDoS) che sovraccaricano i sistemi e ne impediscono l'accesso legittimo.

  2. Guasti hardware o errori di sistema che causano interruzioni dei servizi critici.

  Contromisure suggerite:

  1. Implementare soluzioni di mitigazione DoS/DDoS per rilevare e filtrare il traffico dannoso.

  2. Sviluppare e testare regolarmente piani di continuità operativa e di ripristino di emergenza per garantire la disponibilità continua dei servizi.

Conclusione:

Affrontare adeguatamente le questioni relative alla Triade CIA è essenziale per garantire la sicurezza dei dati dell'azienda. L'implementazione di contromisure efficaci contribuirà a proteggere i dati sensibili, mantenere la fiducia degli stakeholder e ridurre il rischio di violazioni della sicurezza.