Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

MODELLO DI IMPLEMENTAZIONE CSI

GO CLOUD GO SECURE

Fase 1: ANALIZZARE

- Passaggio 1: Elenco dei servizi cloud
- Passaggio 2: Mappatura dei rischi
- Passaggio 3: Conformità

Fase 2: DEFINIRE

- Passaggio 4: Ruoli e responsabilità
- Passaggio 3: Definizione degli obiettivi di controllo
- Passaggio 2: Priorità dei rischi
- Passaggio 1: Sviluppo delle politiche

Fase 3: PIANIFICARE

- Passaggio 1: Azioni di mitigazione
- Passaggio 2: Mappatura dei controlli
- Passaggio 3: Documentazione
- Passaggio 4: Programma di formazione

Fase 4: IMPLEMENTARE

- Passaggio 2: Formazione e sensibilizzazione
- Passaggio 1: Azioni tecniche

Fase 5: VERIFICARE

- Passaggio 1: Test
- Passaggio 2: Monitoraggio
- Passaggio 3: Feedback

Cofinanziato dall'Unione europea

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

MODELLO DI IMPLEMENTAZIONE CSI

GO CLOUD GO SECURE

Fase 1: ANALIZZARE

Passaggio 1: Elenco dei servizi cloud

Crea un elenco completo di tutti i servizi cloud utilizzati dall'organizzazione. Prima della valutazione è essenziale sapere quali servizi sono in uso e quali sono critici.

Passaggio 2: Mappatura dei rischi

La matrice CSI individua minacce, vulnerabilità e rischi per ciascun servizio cloud, offrendo una visione chiara dei principali punti deboli dell'organizzazione.

Passaggio 3: Conformità

Verifica la conformità dell'organizzazione alle normative UE e agli standard internazionali per evitare sanzioni, perdita di dati e danni reputazionali. Alcuni requisiti prevedono controlli specifici, come registrazione degli accessi, crittografia e segnalazione degli incidenti.

Fase 2: DEFINIRE

Passaggio 1: Sviluppo delle politiche

Redigi una politica di sicurezza cloud che stabilisca regole per l'uso sicuro del cloud, il controllo degli accessi e la protezione dei dati, creando la base del sistema di sicurezza.

Passaggio 2: Priorità dei rischi

Utilizza la matrice CSI per valutare i rischi in base a probabilità e impatto, concentrandoti su quelli più urgenti.

Passaggio 3: Definizione degli obiettivi di controllo

Definisci obiettivi chiari di mitigazione per ogni rischio prioritario individuato nella matrice CSI, trasformandoli in azioni concrete.

Passaggio 4: Ruoli e responsabilità

Assegna ruoli chiari: l'amministratore cloud gestisce le piattaforme, il responsabile dei dati ne controlla l'accesso, il responsabile della sicurezza segue monitoraggio e incidenti, mentre il responsabile della conformità assicura il rispetto delle norme.

Fase 3: PIANIFICARE

Passaggio 1: Azioni di mitigazione

Per ogni rischio prioritario della matrice CSI, definisci misure di mitigazione specifiche e attuabili, così da garantire un'applicazione rapida e coerente, soprattutto nelle PMI senza personale dedicato alla sicurezza.

Passaggio 2: Mappatura dei controlli

Crea una tabella che colleghi le azioni di mitigazione ai singoli servizi cloud, chiarendo cosa viene protetto e come vengono applicati i controlli.

Passaggio 3: Documentazion

Prepara modelli e checklist, come liste di controllo per l'implementazione, modelli di risposta agli incidenti e schede per la revisione dei log di audit, a supporto dell'applicazione delle politiche, delle verifiche e del miglioramento continuo.

Passaggio 4: Programma di formazione

Progetta un programma pratico di formazione CSI su principi del cloud, principali vulnerabilità ed errori di configurazione, per formare il personale e prevenire gran parte degli incidenti di sicurezza.

Cofinanziato dall'Unione europea

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

MODELLO DI IMPLEMENTAZIONE CSI

GO CLOUD GO SECURE

Fase 4: IMPLEMENTARE

Attua le misure tecniche previste nella Fase 3, come MFA, crittografia, politiche IAM e RBAC, utilizzando strumenti integrati come AWS Config e Azure Security Center. Inizia dagli interventi più rapidi, come l'attivazione di MFA e RBAC.

Passaggio 1: Azioni tecniche

Applica il piano formativo della Fase 3 utilizzando la matrice e i materiali didattici, con moduli brevi e pratici adattati alla realtà tecnica e al profilo di rischio dell'organizzazione.

Passaggio 2: Formazione e sensibilizzazione

Fase 5: VERIFICARE

Passaggio 1: Test

Esegui test di resilienza tramite esercitazioni, attacchi simulati, controlli e valutazioni di sicurezza, per verificare che le misure siano correttamente applicate, efficaci e aggiornate e che l'organizzazione sia pronta ad affrontare minacce reali.

Passaggio 2: Monitoraggio

Definisci indicatori KPI per monitorare la sicurezza cloud, gestire i rischi in modo proattivo e misurare i miglioramenti. Gli indicatori principali possono includere accessi non riusciti, avvisi di configurazione errata e patch obsolete, raccolti in una semplice dashboard.

Passaggio 3: Feedback

Crea un registro degli incidenti con dettagli, cause, impatti e misure adottate. Utilizzalo per aggiornare le valutazioni dei rischi, migliorare le politiche e adattare la formazione, mantenendo il sistema di sicurezza dinamico e aggiornato.

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Cofinanziato dall'Unione europea