Auditing e controllo della sicurezza informatica

Monitorare la sicurezza

A distanza

2 giorni (14 Ore)

Open : 1.690,00 € +IVA
Packaged in azienda : 3.750,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.19

L'attuazione di una politica di sicurezza dei sistemi informativi richiede indirizzo e monitoraggio a **tutti i livelli** gerarchici dell'organizzazione, sia dal punto di vista tecnico sia dal punto di vista funzionale. La capacità dell'organizzazione di controllare i rischi e migliorare continuamente il livello di protezione del proprio patrimonio informativo deve essere dimostrata e monitorata.

Questo seminario di sintesi si propone di presentare gli approcci e le modalità utilizzate per gestire la sicurezza dei sistemi informativi attraverso **audit e indicatori** conformi alle sfide dell'organizzazione e agli obblighi normativi vigenti.

A chi è rivolto

Per chi

- CISO o corrispondenti di sicurezza
- Risk Manager
- DPO
- DSI
- Project Manager
- Revisori
- Responsabili tecnici

Prerequisiti

Conoscenza di base della sicurezza informatica

Programma

1 - Premessa: richiamo alle problematiche e agli obblighi in tema di gestione del SGSI

- Definizioni
- Promemoria sui principi di un sistema di gestione del SGSI (ISO 27001)
- Requisiti normativi e legali per la gestione del SGSI

2 - Ruoli e responsabilità in termini di indirizzo e monitoraggio del SGSI

- Ruoli e responsabilità degli attori coinvolti nel SII (Direzione Generale, Direzioni Aziendali, DSI, RSSI, DPO, Revisore, Auditor, controllo interno, ecc.)
- Organi decisionali
- La governance da progettare nell'ambito della gestione e del monitoraggio del SGSI

3 - Verifica della sicurezza informatica

- Categorie di audit (audit della configurazione, test intrusivi, audit del codice, ...)
- L'approccio che deve essere adottato dal revisore (preparazione della missione, svolgimento della missione, restituzione della missione, metriche, ecc.)
- L'audit nell'ambito del subappalto
- Certificazione dei revisori
- La presa in considerazione dei risultati dell'audit da parte dell'ente (arbitrato, miglioramento dei sistemi operativi, ecc.)
- Indicatori di monitoraggio dell'audit

4 - Cruscotti di sicurezza informatica

- Gli approcci proposti (norme ISO 27004)
- Categorie di indicatori di sicurezza a livello strategico e operativo
- La costruzione e la fornitura di cruscotti di sicurezza informatica
- Il trattamento delle difformità (identificazione delle non conformità, definizione delle misure correttive, ecc.)

5 - Controlli di sicurezza informatica

- Controlli permanenti (intrusion detection, log management, logging, ecc.)
- Verifiche periodiche (survey, trace management, ecc.)
- Revisioni della direzione (approccio, obiettivi, ecc.)

6 - Considerazione di audit, tabelle e controlli di sicurezza negli approcci progettuali

- Le nuove regole europee imposte dal regolamento europeo (Privacy By Design)

7 - Caso di studio

- Implementazione di dashboard SGSI

Obiettivi del corso

- Essere in grado di costruire gli indicatori e i dashboard necessari per l'auditing e il monitoraggio della sicurezza informatica
- Conoscere i problemi e gli obblighi in termini di gestione della sicurezza
- Avere una metodologia di controllo della sicurezza
- Scoprire come creare dashboard significativi ed efficaci
- Capacità di padroneggiare le tecniche di controllo della sicurezza informatica

Esercitazioni

- Una **panoramica** completa degli strumenti e delle tecniche per l'auditing e il controllo della sicurezza.
- Il seminario **alterna** presentazione di fondamenti teorici e casi di studio.
- I **feedback** e i consigli di un esperto consulente di sicurezza che supporterà il suo approccio con numerosi esempi concreti.

Date 2026

Ultimi posti Edizione garantita

dal 26 feb al 27 feb	dal 14 set al 15 set
dal 3 giu al 4 giu	dal 5 nov al 6 nov