Security Manager: Sicurezza e protezione delle informazioni Personali e Istituzionali

Le organizzazioni e gli enti Istituzionali sia in ambito Internazionale che Europeo, in materia di "Security", si avvalgono, per tradizione, di strutture organizzative di indirizzo, di controllo e di gestione dell'operatività varie e molteplici, in funzione dei differenti aspetti di sicurezza: intelligence, safety, sicurezza fisica, sicurezza delle informazioni e delle reti di telecomunicazione, sicurezza informatica. Tuttavia l'evoluzione delle tecnologie e la globalizzazione delle comunicazioni e dei processi sociali, politici ed economici sta creando sovrapposizione e comunanza di ruoli, processi, metodi e strumenti per garantire protezione a vari livelli. Le competenze professionali, infine, sebbene siano spesso provenienti da ambiti accreditati a livello istituzionale, necessitano, comunque, di alta qualifica manageriale, etica e leadership riconosciute, unitamente a competenze avanzate e diversificate per esercitare e concepire, con sempre maggiore efficacia, un ruolo che si sta sempre più innovando nella forma e nei contenuti per contrastare il notevole incremento di sempre nuove forme di attacco (CyberSecurity).

Agenda (2 giorni)

Quadro di riferimento:

codice "Privacy" (D.Lgs.196/03) e il prossimo "Regolamento Europeo in materia di protezione dei dati"
aspetti organizzativi, responsabilità e ruoli di controllo e di gestione
mappa delle competenze, skill, iter ottimale per avviare programmi di certificazioni professionali di processo
misure di sicurezza logiche, fisiche ed organizzative a tutela del cittadino e delle Istituzioni
modalità di supporto alla Autorità Giudiziaria.

Ambiti e Perimetri interessati

Amministrazioni Pubbliche Centrali e Locali
Enti a partecipazione statale
analisi dei principali Standard "de Jure" e "de facto" in materia di sicurezza a protezione dal Cyber Crime
processi, politiche e procedure operative da considerare
casi di studio ed esempi
cenni sulle tecniche di protezione tradizionali e sulle tecnologie emergenti (CyberSecurity).

Obiettivi

Acquisire una visione ad ampio spettro in materia di riservatezza delle informazioni e delle attuali misure di sicurezza logiche, fisiche e organizzative da adottare per la conformità e la corretta conservazione dei dati.

Individuare le competenze, le responsabilità e le indispensabili suddivisioni di ruoli.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili IT, CIO (Chief Information Officer), CTO (Chief Technology Officer), Security Manager, CSO (Chief Security Officer), Titolari, Responsabili di trattamento dati, operatori nel settore della Security e della Gestione della Sicurezza, manager del settore di Security Intelligence, appartenenti alle Forze dell'Ordine e quanti operano nella gestione dei dati informatici e telematici particolarmente delicati.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

Iscrizione

Quota di Iscrizione: 1.280,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com