Metodologia e fasi dell' Information Security Risk Management

Descrizione

Per information security risk management viene definito il processo di identificazione, controllo, eliminazione o minimizzazione di eventi incerti che possono danneggiare le risorse di un sistema IT. L'Information Security Risk Management dagli anni '70 è uno degli aspetti fondamentali della Corporate Governance.

Il corso si prefigge l'obiettivo di fornire ai partecipanti i concetti, gli strumenti e le metodologie di approccio al Risk Management nel settore informatico.

Durata: 3 giorni

A chi si rivolge

- Professionisti IT
- Manager IT
- Consulenti IT
- Business Manager
- Security Manager
- Chiunque sia coinvolto nella gestione delle informazioni aziendali

Sede Legale: 70125 - Bari, Via Pasubio, 35 Tel +39.0805427549, Fax +39.0805427549, e-mail info@pcsoftware.it, URL *www.pcsoftware.it*
CCIAA BARI N° 406755 - P.IVA 05235280723

Risk management concetti generali:

Classificazione dei rischi.

Misurazione del rischio.

Mappatura del rischio.

Fattori chiave del processo di Risk management.

Metodologia e fasi della Gestione del Rischio IT:

Definizione di Rischio informatico.

Relazione fra Rischio, Asset e Processi.

Le metriche del Rischio.

Valutazione dei rischi: approccio quantitativo, qualitativo ed ibrido.

Fasi di gestione del Rischio.

Metodi di Gestione del Rischio e Standard di riferimento :

Metodi di Risk Management.

Lo standard ISO/IEC 31000 .

Lo standard ISO/IEC 27005.

Il metodo Mehari.

La Metodologia de Analisis y Gestion de Riesgos de los Sistemas de Informacion (MAGERIT).

Fonti Tassonomiche per la definizione delle minacce e delle vulnerabilità:

Classificazione delle minacce.

Concetto di vulnerabilità e classificazione.

Le metriche della vulnerabilità.

Piano di Gestione del Rischio IT:

Analisi del piano di Gestione del Rischio.

Casi di studio.

Esercitazioni:

Applicazione dei concetti appresi durante le lezioni teoriche.