Information Security & Risk Management

Programma

- La necessità di disporre di standard e best practice nella rivoluzione industriale
- La produzione degli Standard Internazionali: Organismi BSI e ISO
- La Normazione Internazionale ISO, lo standard per il Sistema di Gestione della Qualità ISO 9001 e l'estensione agli altri Sistemi di Gestione
- Gli Standard Internazionali e le Best Practice di Information & Cyber Security
- Il processo di Certificazione volontaria di terza parte
- La famiglia ISO/IEC 27000
- Introduzione alle norme ISO/IEC 27001 e 27002
- La compliance di un ISMS allo standard ISO/IEC 27001
- Procedure e modalità e gestione degli Audit interni di prima e seconda parte.
- Norme internazionali di riferimento
- Introduzione alla Continuità Operativa: Alta Affidabilità, Fault Tolerance, Business Continuity e Disaster Recovery
- La Gestione del Rischio:
- Scope, Asset e Classificazione dell'Informazione
- Risk Assessment, Gap Analysis, Risk Treatment e Reduction
- Esempi di Calcolo del Rischio: con metodi artigianali e mediante strumenti SW commerciali
- L'Analisi del Rischio secondo gli standard ISO 31000 e ISO/IEC 27005
- L'organizzazione delle attività di Vulnerability Assessment e Penetration Test
- La definizione di un modello di Information Security Governance:
- Contromisure ispirate alla Defense in Depth e Maturity Model
- Requisiti e Policy per la Sicurezza delle Informazioni
- Strumenti SW a supporto delle conformità di legge
- Vulnerability Management & Exposure, Virtual Patching
- Etica nell'Informatica: i pericoli della Tecnomediazione, il Codice Etico, i nuovi
- interrogativi posti dai sistemi autonomi e robotizzati

Iscrizioni entro il 9 gennaio 2025