FORMAZIONE HSPI

SECURITY & RISK MANAGEMENT

INFORMATION RISK MANAGEMENT & BUSINESS CONTINUITY

Una catena è forte quanto il suo anello più debole. La consapevolezza del grado di rischio a cui è esposta l'organizzazione passa per una gestione esplicita, strutturata ed organica della tutela degli asset aziendali.

CHE COS'È INFORMATION RISK MANAGEMENT & BUSINESS CONTINUITY

La gestione dei rischi IT è sempre di più al centro di tutte le prassi di assurance e delle normative internazionali. Con la pervasività dell'informatica in tutti i processi aziendali, la gestione di impresa non può prescindere dai nuovi rischi indotti, peraltro in continua ascesa in termini di complessità e pericolosità. Tuttavia spesso si tende a circoscrivere il problema nell'ambito puramente tecnologico, sottovalutando il fattore organizzativo e, soprattutto, la necessità di Governance, intesa come capacità di indirizzare le scelte in materia di protezione dei dati in modo coerente con gli interessi aziendali.

A CHI È RIVOLTO IL CORSO

CIO, CISO (Chief Information Security Officer), CRO (Chief Risk Officer), responsabili della sicurezza delle informazioni, responsabili IT, responsabili dell'ufficio legale, IS Auditor, Business Owner.

OBIETTIVI DEL CORSO

Al fine di migliorare le capacità di valutazione dei rischi legati all'informatizzazione dei processi aziendali e di progettazione dei controlli atti a monitorarli e a mitigarli per aumentare la retention dei clienti, il business value dei prodotti e migliorare l'immagine aziendale, il corso ha l'obiettivo di:

- introdurre ai processi di gestione e governo della sicurezza delle informazioni e alle metodologie di analisi del rischio e analisi degli impatti;
- aumentare la comprensione dei requisiti fondamentali di sicurezza delle informazioni nonché delle principali normative, standard e best practice in materia di protezione dei dati e prevenzione dalle frodi;
- introdurre alla progettazione dei controlli di sicurezza.

DURATA
3 GIORNI

HSPI FORMAZIONE@HSPI.IT
WWW.HSPI.IT

CONTENUTI DEL CORSO

Primo Giorno

- Information Risk Management, driver e sistemi di gestione
- Fondamenti sulla responsabilità giuridica (tipi, classificazione, fonti, attribuzione della responsabilità e onere della prova)
- Tipologia di illeciti collegati alla gestione dei sistemi IT che possono coinvolgere l'azienda
- La responsabilità penale dell'impresa (d.lgs. 231/01)
- Le indagini amministrative, penali ed interne (computer forensics)
- Gli impatti normativi sui Sistemi Informativi: obbligo di secure programming nello sviluppo (anche in outsourcing) di applicazioni e piattaforme; certificazione delle misure di sicurezza installate da terze parti; il ruolo dei sistemi di identity management; Firma digitale; Privacy (d.lgs. 196/2003), misure di sicurezza per il trattamento dei dati personali e linee guida del Garante; la nuova legge sul Risparmio – Adeguatezza delle procedure amministrativo-contabili (L. 262/05) – Aspetti di auditing delle procedure e dei sistemi informativi.

Secondo Giorno

- Standard e best practice internazionali (es.: ISO27001, BS25999, DRII, ISC2, NIST, COBIT, COSO)
- Cenni di Enterprise Risk Management e Internal Auditing
- I processi di gestione dei rischi delle informazioni
- Ruoli e responsabilità, tenendo anche conto della trasversalità delle attività di tutela delle informazioni all'interno dell'organizzazione e degli outsourcer
- Analisi del Rischio e Business Impact Analysis
- Controlli di sicurezza: introduzione ai controlli di sicurezza, policy e sistemi di controllo interno (SCI, Audit); controlli organizzativi, logici e fisici; controlli preventivi, di rilevazione, correttivi, di ripristino; controlli di cogenza, trasparenza e deterrenza; principi di segregation of duties e need to know.
- Sviluppo e gestione dei programmi per la sicurezza
- Comunicazione e awareness

Terzo Giorno

- Piani di sicurezza e Business Continuity (selezione dei controlli, sviluppo e gestione dei Piani di BC e Piani di Sicurezza, gestione degli incidenti e delle crisi informatiche, cenni di computer forensics)
- Policy compliance (Identity e Access Management, Information Security Event Management)
- Dashboard direzionale per la compliance alle policy di sicurezza e la valutazione dell'efficacia dei controlli)

PERSONALE DOCENTE

I docenti HSPI hanno un'esperienza pluriennale nella conduzione di progetti complessi, presso organizzazioni IT di medie e grandi dimensioni, e sono in possesso delle certificazioni AgilePM Approved Trainer, PRINCE2 Approved Trainer, MoP Approved Trainer, DevOps Approved Trainer, PRINCE2 Agile Approved Trainer e Professional Scrum Master. Grazie all'esperienza maturata nell'attuazione delle best practice del corso e nell'insegnamento delle metodologie di Project & Portfolio Management, Service Management ed Enterprise Architecture, i trainer HSPI riescono a portare in aula esempi concreti di applicazione pratica dei concetti trattati.

L'AZIENDA

HSPI SpA è una società di consulenza direzionale specializzata in progetti di ICT Governance, gestione del cambiamento organizzativo e Information Risk Management. Fortemente orientata all'utilizzo di best practice internazionali quali ITIL®, COBIT®, PMP, PRINCE2 e TOGAF®, ne sostiene la diffusione mediante l'applicazione nel contesto dei propri clienti, la formazione e le attività di volontariato.

HSPI è certificata UNI EN ISO9001:2015 per l'erogazione dei servizi di formazione e accreditata ente di formazione specializzato (ATO e AEO) da APMG International e PEOPLECERT.

HSPI è certificata secondo la norma ISO37001:2016 sulle politiche di anticorruzione.

CONTATTI

Per iscrizioni al corso e informazioni, invia un'e-mail a formazione@hspi.it.