

CORSO RISK MANAGEMENT IT E BUSINESS IMPACT ANALYSIS

Durata: 10,5 ore



PROGRAMMA

MODULO 1: RISCHIO IT E CONTINUITÀ OPERATIVA: IL QUADRO PER L'AZIENDA

- Dal rischio IT al rischio di business: perché un fermo dei sistemi riguarda tutta l'organizzazione
- Risk Management, Business Continuity Management e Disaster Recovery: differenze e punti di contatto
- Ruoli e responsabilità: direzione, IT, responsabili di processo, fornitori
- Il contesto normativo: NIS2 (art. 21, recepita con il D.Lgs. 138/2024), DORA per il settore finanziario, GDPR
- Gli standard di riferimento (ISO 31000, ISO/IEC 27005, ISO 22301, ISO/TS 22317) e come usarli senza appesantire l'organizzazione

MODULO 2: PROCESSI, ASSET E MINACCE: MAPPARE COSA PROTEGGERE

- Il rischio e le sue componenti: minaccia, vulnerabilità, probabilità, impatto
- Relazione fra rischio, asset e processi: dai processi di business ai sistemi, dati, persone, fornitori e servizi cloud che li sostengono
- Classificazione delle minacce: tecniche, umane, ambientali, legate alla supply chain
- Vulnerabilità tecniche, organizzative e di processo
- Dipendenze critiche e single point of failure
- Scenari di rischio ricorrenti nelle aziende: ransomware, perdita di dati, fermo di un fornitore critico, indisponibilità di un servizio cloud

MODULO 3: VALUTARE IL RISCHIO IT: METODO E PROCESSO

- Le fasi del processo di gestione del rischio: contesto, identificazione, analisi, ponderazione, trattamento, monitoraggio
- Approccio qualitativo, semi-quantitativo e quantitativo: quando usare ciascuno
- Matrici di rischio e criteri di accettazione coerenti con gli obiettivi aziendali
- Rischio inerente e rischio residuo
- Gli errori più frequenti nella valutazione e come evitarli

CORSO RISK MANAGEMENT IT E BUSINESS IMPACT ANALYSIS

Durata: 10,5 ore



MODULO 4: IL PIANO DI GESTIONE DEL RISCHIO IT

- Struttura e contenuti del piano di gestione del rischio
- Opzioni di trattamento: mitigare, trasferire, evitare, accettare
- Scegliere le contromisure valutando costi e benefici
- Il registro dei rischi: responsabili, priorità, scadenze
- Indicatori di rischio (KRI), monitoraggio e riesame periodico
- Comunicare il rischio alla direzione: dal dato tecnico alla decisione
- Analisi di casi aziendali

MODULO 5: BUSINESS IMPACT ANALYSIS (BIA)

- Obiettivi della BIA e relazione con la valutazione dei rischi
- Metodi di approccio: interviste, questionari, workshop con i responsabili di processo
- Individuare i processi critici e le risorse da cui dipendono
- Valutare gli impatti nel tempo: economici, operativi, legali, reputazionali
- I parametri chiave: MTPD, RTO, RPO, MBCO
- Stimare il costo di un'interruzione
- Dipendenze da fornitori e terze parti
- Validare e condividere i risultati con la direzione

MODULO 6: DALLA BIA ALLE DECISIONI: STRATEGIE DI CONTINUITÀ E RIPRISTINO

- Tradurre RTO e RPO in requisiti concreti per IT e fornitori: backup, ridondanza, disaster recovery, cloud
- Gap analysis tra requisiti di continuità e capacità attuali
- Definire le priorità di investimento e costruire il business case
- Il collegamento con Business Continuity Plan, piano di Disaster Recovery e gestione delle crisi
- Mantenere aggiornate analisi dei rischi e BIA nel tempo

CORSO RISK MANAGEMENT IT E BUSINESS IMPACT ANALYSIS

Durata: 10,5 ore



OVERVIEW DEL CORSO

Un fermo dei sistemi, un attacco ransomware o l'indisponibilità di un fornitore cloud non sono solo problemi tecnici: bloccano ordini, produzione e servizi ai clienti. Il corso insegna a valutare il rischio IT partendo dai processi di business e a stabilire quali attività vanno ripristinate per prime, in quanto tempo e con quale perdita di dati accettabile.

Il percorso segue il processo di gestione del rischio di ISO 31000 e ISO/IEC 27005 e la metodologia di Business Impact Analysis di ISO 22301 e ISO/TS 22317, applicati in modo proporzionato alle dimensioni dell'azienda, con l'analisi di casi aziendali e i riferimenti a NIS2 e DORA.

A CHI È RIVOLTO IL CORSO?

Il corso è rivolto a:

- IT manager e responsabili dei sistemi informativi che devono valutare i rischi dell'infrastruttura e motivare gli investimenti in continuità e ripristino
- CISO e responsabili della sicurezza delle informazioni che impostano il processo di gestione del rischio IT
- Risk manager, compliance officer e internal auditor che integrano il rischio IT nella gestione dei rischi aziendali
- Responsabili di processo e operations coinvolti nella Business Impact Analysis
- Referenti di aziende soggette a NIS2 o DORA

COSA SAPRAI FARE ALLA FINE DEL CORSO?

Al termine del corso i partecipanti saranno in grado di:

- Collegare il rischio IT al rischio di business e distinguere Risk Management, Business Continuity Management e Disaster Recovery
- Mappare processi, asset, dipendenze critiche e single point of failure, compresi fornitori e servizi cloud
- Valutare il rischio IT con approccio qualitativo, semi-quantitativo o quantitativo
- Costruire il piano di gestione del rischio e il registro dei rischi, con responsabili, priorità, scadenze e KRI
- Condurre una Business Impact Analysis e definire MTPD, RTO, RPO e MBCO
- Tradurre i risultati della BIA in requisiti di continuità e in un business case per la direzione