PERCORSO CYBER RISK MANAGEMENT

I moduli si svolgeranno in aula virtuale fino a diversa comunicazione

1° MODULO • **15 e 16 aprile 2021**
2° MODULO • **29 e 30 aprile 2021**

1° MODULO • 15 e 16 aprile 2021
INTRODUZIONE AL CYBER RISK E ALLA CYBER SECURITY

Primo giorno • **15 aprile 2021**

- **Il panorama normativo nazionale ed europeo per la gestione del rischio informatico: le sovrapposizioni, le peculiarità, le opportunità di integrazione dei diversi requisiti**
- **Le recenti attività dei regolatori**
  - Raccomandazioni EBA
  - "Direttiva NIS - Network and Information Security"
  - Direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti
  - Commissione Europea: proposta di regolamento relativo all'ENISA, Agenzia dell'Unione europea per la cyber security
- **I modelli di gestione della sicurezza e gli standard internazionali di riferimento**
  - Gli obiettivi dei modelli di gestione della sicurezza e le norme ISO
  - Le norme della famiglia ISO 27000 e approfondimenti sulla 27001
  - I rischio e le norme ISO 27005 e ISO 31000
  - La norma ISO 22301: lo standard internazionale per raggiungere elevati livelli di cyber resilience
  - Il NIST
- **La Cyber Security all'interno delle principali normative di rilievo (PSD2, GDPR...)**
  - Requisiti EBA sull'IT Risk di compliance all'interno dello SREP
- **La Cyber Security alla luce del GDPR**
  - Requisiti normativi in termini di misure di sicurezza informatica
  - L'esecuzione della DPIA: approcci e logiche di calcolo del Rischio IT
  - Data Breach: l'importanza di prevenire gli eventi e gli impatti sulla Brand Reputation

Secondo giorno • **16 aprile 2021**

- **I modelli di gestione della cyber security**
  - Il confine tra la gestione della sicurezza dell'informazione e gli approcci orientati specificatamente alla protezione contro gli attacchi da internet della cyber security
  - Use Case: una metodologia di valutazione, misurazione, gestione e reporting del rischio cyber, applicata ai sistemi di pagamento
- **L'evoluzione della sicurezza informatica nella valutazione dell'affidabilità dei fornitori**
  - L'esternalizzazione dei servizi IT
  - La protezione dei dati esternalizzati: la conformità al GDPR e l'approccio risk based
  - La gestione dei rischi legati alle cd. fintech
- **La gestione dei sistemi informativi in cloud**
  - Il cloud computing sotto il profilo contrattuale e normativo nazionale ed europeo
  - Cloud: profili legali e contrattuali
  - I vantaggi del cloud computing e i rischi legati al trattamento dei dati
  - Il Cloud computing e la protezione dei dati personali
  - Le criticità legate alla gestione dei contratti

2° MODULO • 29 e 30 aprile 2021

METODI E PROCESSI DI GESTIONE DEL CYBER RISK

Primo giorno • **29 aprile 2021**

- **Il sistema informativo in banca: organizzazione e processi di gestione per la cyber security**
  - Come cambia il modello di gestione della sicurezza alla luce delle nuove sfide di cyber security
  - Modelli data-driven di protezione della sicurezza e delle informazioni, alla luce del GDPR
  - Le tipologie e i vettori d'attacco: conoscerli per saperli affrontare
  - La sicurezza by design: costruzione di un processo/servizio ICT conforme alle policy di cyber security
  - Information Security, Cyber Security, Data Protection, Data Governance, Enterprise Risk Management: relazioni tra i diversi processi, opportunità da cogliere, rischi da evitare
- **La gestione del rischio IT come elemento centrale della Sicurezza Informatica**
  - Il rischio IT e le interrelazioni con le altre tipologie di rischio operativo
  - Il Framework di gestione del cyber risk: identificazione e misurazione, prevenzione, monitoraggio, mitigazione. Cenni al NIST Cyber Security Framework
  - Risk, Threat and Vulnerability Assessment: l'analisi e il trattamento del rischio
  - Strumenti per il monitoraggio e la mitigazione del rischio
- **L'integrazione dei processi aziendali di risk management**
  - Integrazione del processo di risk management con gli altri processi del sistema informativo: change management, incident management, gestione dei fornitori e delle terze parti, gestione della sicurezza
  - Integrazione del processo di risk management con i processi del ciclo di vita
- **L'integrazione delle metodologie di valutazione de rischi**
  - Metodologie integrate tra rischi operativi, rischi IT, rischi di data protection

Secondo giorno • **30 aprile 2021**

- **Cyber Risk Mitigation**
  - Strumenti di copertura e trasferimento del rischio
  - Come decidere "dove" coprirsi/mitigare il rischio
- **Il controllo e il monitoraggio del cyber risk: Risk Appetite e Indicatori di Rischio**
  - La definizione del Risk Appetite framework per il rischio informatico e cyber risk
  - Gli strumenti per il monitoraggio del cyber risk
  - Approccio Data Driven per la definizione e gestione degli indicatori di rischio
- **Strumenti di gestione dei rischi cyber e applicazione della Cyber Threat Intelligence**
  - Valutazione periodica dell'esposizione al rischio cyber
  - Monitoraggio degli eventi di rischio
  - Utilizzo di soluzioni Analytics e Threat Intelligence per migliorare analisi dei rischi
- **Cyber Resilience e contromisure per prevenire il rischio cyber**
  - Contesto di mercato sottostante la gestione della cyber resilience
  - Modello operativo e coordinamento dei flussi informativi tra le funzioni coinvolte
  - Strumenti analytics come acceleratore per una più efficace cyber resilience
- **Digital Cyber Culture & Awareness**
  - Perché rilevante per la cyber security
  - Approccio Digital per la diffusione della Cyber Culture & Awareness all'interno dell'organizzazione a tutti i livelli
  - Principali soluzioni di mercato per incrementare il livello di Culture & Awareness