Percorso

CYBER RISK MANAGEMENT: DALLA CYBER-WAR ALLE TUTELE AZIENDALI

I moduli si svolgeranno in aula virtuale

1° MODULO • 27 e 28 aprile 2022
2° MODULO • 9 e 10 maggio 2022

1° MODULO • 27 e 28 aprile 2022

INTRODUZIONE AL CYBER RISK E ALLA CYBER SECURITY

Primo giorno • 27 aprile 2022

- **Lo scenario attuale relativo al cyber risk**
  - I dati del rapporto Clusit 2022
  - Come cambia lo scenario di rischio «cyber» dello scontro tra Russia e Ucraina
- **Focus – Le dinamiche della «cyber war» e i rischi per l'Italia**
  - I principali eventi cyber legati alla guerra tra Russia e Ucraina
  - Cosa aspettarsi nel prossimo futuro
  - Quali sono le principali contromisure
- **La cyber security all'interno delle principali normative di rilievo (PSD2, GDPR)**
  - Requisiti EBA sull'IT Risk di compliance all'interno dello SREP
  - Prospettive ed impatti del nuovo Digital Operational Resilience Act (DORA)
- **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 • 28 aprile 2022

- **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 Cybersecurity Framework
  - Risk, Threat and Vulnerability Assessment: l'analisi e il trattamento del rischio
  - Strumenti per il monitoraggio e la mitigazione del rischio
- **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
  - Una metodologia di valutazione, misurazione, gestione e reporting del rischio cyber, applicata ai sistemi di pagamento - use case
- **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

Copyright © ABISERVIZI SpA. Tutti i diritti riservati.
È proibita la riproduzione, anche parziale, in qualsiasi forma senza espresso permesso scritto di ABISERVIZI SpA. - Divisione ABIFormazione.
Il ricevente è tenuto ad utilizzare il documento esclusivamente per esigenze di documentazione personale nell'ambito delle proprie esigenze lavorative; non può in alcun modo ridistribuire o comunicare a terzi le informazioni in esso presenti.

2° MODULO • 9 e 10 maggio 2022

METODI E PROCESSI DI GESTIONE DEL CYBER RISK

Primo giorno • **9 maggio 2022**

- **Il regolamento DORA**

- **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
  - Il rischio e le norme ISO27005 e ISO 31000
  - La norma ISO 22301: lo standard internazionale per raggiungere elevati livelli di cyber resilience
  - Gli standard NIST per la sicurezza delle informazioni e la cybersecurity

- **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

Secondo giorno • **10 maggio 2022**

- **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 acceleratori per una più efficace cyber resilience

- **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

- **Digital cyber culture & awareness**
  - Digital cyber culture – why relevant?
  - Main market solution to enhance digital cyber culture & awareness
  - Digital approach to spread out cyber culture & awareness among organization within all levels

- **Cyber Risk Mitigation**
  - Strumenti di copertura e trasferimento del rischio
  - Come decidere "dove" coprirsi/mitigare il rischio

- **Testimonianza bancaria**

Copyright © ABISERVIZI SpA. Tutti i diritti riservati.
È proibita la riproduzione, anche parziale, in qualsiasi forma senza espresso permesso scritto di ABISERVIZI SpA. - Divisione ABIFormazione.
Il ricevente è tenuto ad utilizzare il documento esclusivamente per esigenze di documentazione personale nell'ambito delle proprie esigenze lavorative; non può in alcun modo ridistribuire o comunicare a terzi le informazioni in esso presenti.