CYBER CRIME E CYBER SECURITY: IL RUOLO DELL'INTERNAL AUDIT SUI PROCESSI DI PRESIDIO DEI RISCHI DI FRODE

Tipologia	**Corsi interaziendali**
Temi	**Internal Audit, Controlli Interni**
Target	Responsabili e specialisti delle aree Internal audit, Rischi operativi, Organizzazione.
Obiettivi	Il corso fornisce ai partecipanti le conoscenze utili a: • riconoscere gli elementi fondamentali della cyber-security, del cyber-crime, delle criptovalute e le principali disposizioni dettate dalla normativa sulla privacy; • rappresentare l'evoluzione del cyber-risk e del contesto normativo di riferimento; • definire il ruolo della Funzione Internal audit nella governance del rischio di frodi informatiche; • esaminare il framework di Fraud Risk Assessment in una logica di internal audit; • delineare l'importanza della prevenzione del pensiero criminologico e del rischio di frodi attraverso il COSO framework.
Data	23/24 novembre 2021
Sede	**Aula virtuale, attraverso piattaforma dedicata, con possibilità di interazione real time con i docenti**

PRESENTAZIONE

Il conteso di emergenza sanitaria dovuta al Covid-19 ha indotto la maggioranza dei clienti dei servizi bancari a optare per l'accesso da remoto ai servizi della propria banca, proprio in ragione delle restrizioni e delle limitazioni alla mobilità dettate dalle misure di contenimento della pandemia. Ciò ha determinato, tra l'altro, un notevole incremento nel settore bancario degli attacchi telematici e delle frodi informatiche.

È presumibile, inoltre, che anche nella fase di post-pandemia i clienti continueranno a propendere per i sistemi di home-banking, che consentono di effettuare operazioni in tempo reale e senza attese allo sportello. Per tali motivi è sempre più necessario che la Funzione Internal audit sia in grado di adeguare i sistemi di presidio interno all'evoluzione dei rischi prodotta dalle nuove abitudini della clientela e dalle esigenze produttive aziendali.

Il corso risponde alla crescente esigenza di formare specialisti di internal audit in grado di valutare e prevenire gli attacchi informatici, nonché di contribuire a promuovere in azienda la cultura della cyber-sicurezza, attraverso l'adozione di processi operativi in linea con le migliori pratiche internazionali.

PROGRAMMA

PRIMA GIORNATA

Cyber crime

- Cosa si intende per cyber crime? Le tipologie di cyber crime
- Come proteggersi dal cyber crimine e scegliere la migliore soluzione per la prevenzione del cyber crimine
- La Frode informatica nel nostro ordinamento penale
- Cybercrime: Report FBI 2020;
- Cybercrime: gli attacchi più utilizzati (es. BEC/EAC, ecc.)
- BEC/EAC: le principali varianti; Come prevenire e proteggersi?
- Social Engineering (Ingegneria sociale); canali e metodi; come difendersi dalla minaccia del social engineering
- Social Engineering: tecniche psicologiche utilizzate nel Social Engineering;
- PHISHING: cos'è; le : principali tipologie di phishing
- Ransomware: cos'è, come infetta e come rimuoverlo; l'evoluzione dei ransomware e le nuove tecniche d'attacco;
- protezione da ransomware e prevenzione; cosa fare se siamo stati colpiti da un ransomware

Criptovalute

- Cosa sono le Criptovalute; quali sono e le principali caratteristiche;
- Regolamentazione e Criptovalute
- Criptovalute: aspetti positivi/negativi; provvedimenti CONSOB
- Criptovalute: contromisure dei Regulators (GAFI/Bankitalia/UIF) aspetti economici e regolamentari delle
- Cripto-attività (18 marzo 2019) - I PRINCIPI CONTABILI – schemi di IPOTESI;
- OBBLIGHI AML DA V° DIRETTIVA EU
- Criptovalute e riciclaggio;

- Criptovalute e casi pratici fraudolenti

Il ruolo dell'internal audit nella governance del rischio di cyber fraud
- Organizzazione della funzione di Internal Audit
- Governance del rischio frode; Assessment del rischio frode; Prevention; Detection; Investigation; Reporting
- Attività di Internal Audit sul rischio frode cyber
- Diffusione della cultura del rischio
- Peculiarità delle frodi cyber

Case study e best practices

Testimonianza: Il ruolo dell'Internal Auditor nella identificazione delle cyber fraud: casi pratici di Social Engineering e di Business Email Compromise (BEC)

SECONDA GIORNATA

Cyber security e privacy
- Cybersecurity, cos'è?
- Le differenti tipologie di cybersecurity
- Come funziona la sicurezza informatica
- La cybersecurity e il dilemma tra privacy e sicurezza
- Privacy e cyber security: le norme comunitarie
- Privacy e Cyber security nel regolamento europeo
- Garante privacy: no alla diffusione dei dati che rivelano un disagio economico
- Privacy e Cybersecurity: fiducia alla norma o fiducia all'etica - il caso PANDORA PAPERS

Deep web e il dark web
- Che cosa c'è nel deep web e come si accede
- Che cos'è il dark web
- Come si accede al dark web
- Che cosa si trova nel dark web
- La parabola di Silk Road
- Tor: cos'è e come usarlo in sicurezza per navigare nel Dark Web
- I numeri di Tor

Frodi ai tempi del coronavirus
- Frodi PONZI
- Frodi Connesse ai furti di identità

Frodi interne e il pensiero della crimonologia
- Definizione
- I principali schemi fraudolenti
- L'importanza della percezione del rilevamento
- Le principali red flag comportamentali
- Come vengono scoperte le frodi
- Durata media delle frodi
- Schemi maggiormente rilevanti
- Profilo del frodatore
- Prevenzione delle frodi: i contributi della criminologia
- COSO Framework: baluardo per contrastare l'opportunity

CONTATTI

Elisa Isacco

e.isacco@abiservizi.it

06.6767.517