PRINICIPI ESSENZIALI DELLA CYBERSECURITY E GOVERNO DEL RISCHIO IT

CORSO DI ALTA FORMAZIONE

DESTINATARI

Il programma è destinato a manager operanti nel settore finanziario, in particolare a:

- IT Risk officer e IT Risk Manager
- addetti all'IT security e antifrode
- operation Risk Manager
- addetti e Responsabili Audit e Compliance
- addetti e Responsabili delle unità di business
- responsabili ed analisti organizzativi
- high potential e tutti coloro che, a qualsiasi livello aziendale, si trovano a dover impostare un'adeguata gestione del rischio.

INTRODUZIONE E OBIETTIVI DEL CORSO

La circ. 285, che riprende i temi introdotti dalla ex. Circ. 263, chiede alle banche di governare il rischio informatico, lasciando tuttavia ampi spazi all'interpretazione e alle modalità di implementazione. In ambito assicurativo, il Reg. 20 riprende di fatto le linee della Circ. 285 e lascia ancor più spazio all'interpretazione e alle modalità di implementazione. In uno scenario dove l'ampiezza e pervasività del tema e l'importanza che esso riveste nel contesto finanziario, dove l'IT è la «macchina tecnologica produttiva» e non solo è il fattore abilitante ai servizi, ma detiene informazioni rilevanti, riservate e sensibili, una dimensione del rischio IT è rappresentata dall'insieme di eventi potenziali che derivano dal manifestarsi di incidenti di sicurezza informatica: in altri termini, il *cyber risk* che deriva dalla *cyber security*. **Obiettivo del corso** è inquadrare l'evoluzione del concetto di rischio informatico introdotto dalla Circ. 285, introdurre un framework organizzativo di presidio (auditabile) e introdurre alle tecniche di valutazione e gestione del rischio informatico, con alcuni riferimenti agli standard internazionali che possono supportare nel suo inquadramento, valutazione e controllo. L'approfondimento al cyber risk ha l'obiettivo di illustrare la dimensione del fenomeno e correlare questa specifica dimensione del rischio a tecniche predittive e condivise che consentano, nel caso di manifestarsi di un incidente di cyber security, di disporre di linee guida di reazione che consentano di minimizzare il principale effetto negativo (reputazionale) e le sue potenziali conseguenze economiche e normative.

Direzione e coordinamento scientifico
PROF. FEDERICO RAJOLA
PROF.SSA CHIARA FRIGERIO

LOCATION

Università Cattolica del Sacro Cuore
AULA I, Via Lanzone, 29

CALENDARIO

✓ 18-19 dicembre 2017

Le date potrebbero essere soggette a variazione

ORARIO

9.30 alle 13.00 e dalle 14.00 alle 17.30

QUOTE DI PARTECIPAZIONE

La quota di partecipazione può essere finanziata con le risorse messe a disposizione dai fondi interprofessionali.

ADERENTE CeTIF: € 1.400 + IVA
NON ADERENTE CeTIF: € 1.600 + IVA

(E' previsto uno sconto di € 100 per iscrizioni pervenute entro il 27 novembre 2017)

CONTATTI

Mail: cetif.academy@unicatt.it
Tel: 02.7234.2590
www.cetif.it

** I contenuti del corso possono essere personalizzati e riproposti direttamente presso la sede dell'azienda interessata sulla base di specifiche esigenze formative*

PROGRAMMA DELLE LEZIONI

GIORNO 1

- Warm-up
- Stato dell'arte del governo del rischio IT
- Sintesi normativa
  - ✓ Punti salienti ella Circ. 285 e delle criticità implementative.
  - ✓ Ampliamento delle definizioni (non esaustive) contenute nella normativa.
- Sintesi e contenuti delle principali best practices internazionali
- Framework organizzativo per la gestione integrata del rischio IT
- Introduzione alle tecniche quantitative (1)
- Introduzione alle tecniche quantitative (2)
- Valutare il rapporto costi/benefici
- Debriefing

GIORNO 2

- Welcome back
- Introduzione: Cyber risk, cyber security e cyber resilienza: cosa sono, da cosa derivano, i trend
- Quadro normativo
  - ✓ PSD2: highlights e requisiti di security
  - ✓ GDPR: highlights e requisiti di security
  - ✓ AML: highlights e requisiti di security
  - ✓ Network Information Security (NIS) Directive
  - ✓ electronic IDentification Authentication and Signature - eIDAS Regulation
- Best practices internazionali (1)
- Best practices internazionali (2)
- Tecniche di attacco e di difesa
- Diffusione della cultura
- IT Security Self Assessment open mind workshop (Durante il workshop verranno illustrate la modalità con la quale costruire, su base quantitativa (sebbene derivante da valutazione qualitative), un piano di risposta e di soluzioni di mitigazione.
- Debriefing

METODOLOGIA DIDATTICA

L'approccio formativo si basa su tecniche didattiche innovative ed efficaci, orientate al trasferimento di conoscenze e comportamenti attraverso l'alternanza di

- ✓ lezioni teoriche
- ✓ momenti di consolidamento e revisione critica dei contenuti
- ✓ esercitazioni in aula
- ✓ simulazioni
- ✓ workshop in cui si applicano i concetti appresi su casi concreti e specifici sul contesto bancario e assicurativo

Domanda di ammissione da inviare entro il giorno 11 dicembre 2017

Spett.le CeTIF
Centro di ricerca su Tecnologie, Innovazione e servizi Finanziari
Università Cattolica del Sacro Cuore
Largo Gemelli, 1 – 20123 Milano MI

alla c.a.: Segreteria Didattica
Tel. 02-72342590
Fax 02-72348340
e-mail: cetif@unicatt.it

Dati dell'Azienda

Denominazione sociale _____

Indirizzo _____

Cap e Città _____

Partita Iva _____

Con la presente il/la sottoscritto/a _____

in qualità di _____

Il corso è compatibile con gli Avvisi di FONDIR e FBA e altri fondi interprofessionali

Quota di partecipazione ADERENTE CeTIF:
□ **2 giornate**: € 1400 (millequattrocento)
+ IVA per partecipante

Quota di partecipazione NON ADERENTE CeTIF:
□ **2 giornate**: € 1600 (milleseicento)
+ IVA per partecipante

(E' previsto uno sconto di € 100 per iscrizioni pervenute entro il 27 novembre 2017)

La quota di partecipazione dovrà essere versata sulla base delle indicazioni che verranno trasmesse da CeTIF unitamente alla conferma di iscrizione e al calendario definitivo delle lezioni. . La fattura sarà spedita solo in formato elettronico. **Indicare cortesemente un indirizzo email: ……**

Soggetto a split payment □ sì □ no

Richiede l'ammissione dei seguenti nominativi al Corso di Formazione:

Il Sig./Dott. _____

Telefono _____ email _____

Qualifica aziendale _____ in qualità di _____

Il Sig./Dott. _____

Telefono _____ email _____

Qualifica aziendale _____ in qualità di _____

LUOGO e DATA **TIMBRO e FIRMA**

INFORMAZIONI GENERALI

Il numero di partecipanti ammessi potrà variare da un minimo di 10 ad un massimo di 25. CeTIF si riserva di attivare o meno il corso, qualora non venga raggiunto il numero minimo previsto di adesioni. Per ulteriori informazioni contattare Serena Piccirillo (serena.piccirillo@unicatt.it 0272342590).

TUTELA DEI DATI PERSONALI INFORMATIVA

CeTIF, ai sensi dell'articolo 07 della legge 30 giugno 2003, n. 196, dichiara che i dati personali inseriti saranno trattati - anche con l'ausilio di mezzi elettronici – per finalità riguardanti l'esecuzione degli obblighi relativi alla suddetta adesione. Il compilatore è informato che a norma dell'articolo 13 della sopraccitata legge 196/2003, in ogni momento potrà avere accesso ovvero richiedere la modifica e/o la cancellazione dei propri dati personali rivolgendosi direttamente al Responsabile dei Dati dell'Università Cattolica, Largo Gemelli 1 - 20123 Milano.