PROXYMA®
BPM EXCELLENCE CENTER

Percorso formativo dedicato alla

Cybersecurity

Sicurezza informatica

per l'azienda ed il professionista.

Docente:

- ✓ ***Dr. Luca Cadonici*** *– Consulente Informatico Forense acc. CCIAA PI - ONIF, IISFA*

Cert. IT19/1009
Settori EA35 ed EA37
Ambito BPM

PROXYMA® - Via A. Massaria, 42 - 36100 Vicenza
Tel. 0444 544522 – e-mail: proxyma@proxyma.it

La cybersecurity per l'azienda ed il professionista

L'avvento di nuove sofisticate tecnologie in azienda, l'integrazione di macchine ed utenti secondo principi organizzativi che cercano di ottenere livelli di efficienza più elevati e la necessità di avere dal proprio sistema informativo risposte sempre più complesse, mettono spesso a nudo importanti **criticità sulla sicurezza delle informazioni**.

La marcata adozione di sistemi cloud forniti da terze parti, comportano una difficile gestione dei dati aziendali nella loro integrità e fruibilità, obbligando il professionista a fare costantemente ricorso a comunicazioni esterne basati su protocolli Tcp-ip (internet).

I servizi cloud cercano di innescare, d'altro canto, un profondo senso di fiducia: cioè la percezione di sicurezza che le informazioni non siano accessibili a persone o strumenti non autorizzati grazie all'ausilio di password complesse e contenuti salvaguardati da efficaci back-up.

La realtà, purtroppo, è ben diversa. E' sufficiente che un solo anello della catena informativa, anche in assoluta buona fede, non sia stato opportunamente protetto da un accurato piano di sicurezza, che il danno già compare all'orizzonte. *Istantaneamente.*

Non è solo l'attacco di hacker, phishing o di ransomware tipicamente dolosi che innescano pesanti problemi e danni spesso incalcolabili, ma la perdita di dati è sempre più spesso generata da disattenzioni e da inconsapevoli errori di gestione.

Per venire incontro a queste esigenze è nato questo percorso di **cybersecurity** basato su robusti expertise maturati in ambito forense. Quindi non una semplice sequenza di comandi verso il proprio sistema informativo (notebook, pc, rete, ecc.), ma **un piano ragionato di quello che si deve fare per ottenere concreta sicurezza**.

Le imprese di tutto il mondo richiedono accurate perizie di cybersecurity non solo per appurare la natura del dolo, qualora sussista, ma anche per chiarire i reali accadimenti e quali impatti hanno avuto sui dati per valutarne il ripristino (**Business Continuity**).

Il percorso didattico dedicato alla cybersecurity è una chiave di lettura professionale in grado di soddisfare il manager più esigente. Soprattutto è un valido contributo per raggiungere un ottimo grado di consapevolezza su una materia così vasta e complessa.

PROXYMA® - Via A. Massaria, 42 - 36100 Vicenza
Tel. 0444 544522 – e-mail: proxyma@proxyma.it

Obiettivo del Corso

Il corso è strutturato per fornire ai partecipanti robuste conoscenze sulla gestione della Cybersecurity e della sua concreta applicazione.

Gli argomenti trattati sono sviluppati con riferimento ai principi e metodi codificati anche all'interno della famiglia delle norme sulla sicurezza informatica **UNI EN ISO 27001**.

Durante l'attività didattica saranno illustrati gli accorgimenti pratici e gli strumenti liberamente disponibili in rete che permettono un **significativo incremento** del **livello di sicurezza** nella gestione e nella comunicazione dei dati custoditi.

Verranno fornite le competenze basilari di sicurezza informatica volte ad aumentare il livello di protezione della propria azienda o dello studio professionale da tutto ciò che espone al rischio di furto o di perdita di dati.

Durante le sessioni didattiche erogate in FAD Interattiva verranno applicate le principali tecniche metodologiche di analisi affinché i partecipanti prendano coscienza della concretezza ancorché della enunciazione dei rischi sulla sicurezza in azienda.

La didattica in FAD Interattiva non è passiva. Sono previsti numerosi laboratori che consentiranno al partecipante di applicare immediatamente quanto impartito dal docente, aumentando in modo significativo la produttività e la competenza.

A chi è rivolto

ICT Manager, Risk Manager, Business Continuity Manager, Responsabili Sicurezza, Process Owner, Professionisti & Consulenti, Studi Legali.

Il percorso didattico è erogato in FAD Interattiva con un massimo di 9 partecipanti, in 4 sessioni nella modalità 2+2. Ogni sessione inizia alle 9.00 e termina alle 13.00

Tutti i partecipanti avranno, oltre alla docenza, anche i materiali didattici, licenze TRIAL 30 giorni per le esercitazioni ove possibile, l'Attestato di Frequenza e l'assistenza post corso per 30 giorni tramite MRI (modulo richiesta intervento).

PROXYMA® - Via A. Massaria, 42 - 36100 Vicenza
Tel. 0444 544522 – e-mail: proxyma@proxyma.it

Programma del corso

- ✓ **Concetti generali**
  - Introduzione alla sicurezza informatica
  - Definizione di sicurezza informatica
  - La sicurezza informatica in azienda

- ✓ **Le principali tipologie di minacce informatiche**
  - Malware, phishing, spam, spear-phishing

- ✓ **Sicurezza durante la navigazione in rete**
  - http Vs https
  - Sniffing e contromisure
  - Privacy in rete – Cookies e loro disabilitazione
  - Privacy in rete – nei browser e nei motori di ricerca
  - Privaci in rete – protezione anti tracciamento avanzato
  - Cifrare le credenziali nel browser
  - Protezione da phishing e malware
  - Comunicare in sicurezza – mail OpenPGP

- ✓ **Endpoint security**
  - Autenticazione a due fattori – 2FA
  - Google Authenticator e Yubikey
  - Gestione e complessità delle password
  - Password - attacchi a forza bruta, a dizionario, furto di credenziali
  - Password manager - Web, software, hardware
  - Wallet hardware come password manager
  - Havibeenpwned?
  - Cifratura del disco – soluzioni
  - Cifrare le memorie removibili – Bitlocker e Veracrypt
  - Cifrare le memorie removibili – cifratura integrata – PIN
  - Pen drive con sblocco biometrico
  - Cifrare i file - Office
  - Cifrare i file – AxCrypt – Eliminazione sicura file AxCrypt
  - Lo spazio non allocato
  - Sicurezza dei file office – le macro
  - Rimozioni applicazioni non necessarie – dell'Utente e di Windows
  - Gestione Privacy MS Windows
  - Antivirus
  - Patching – MS Windows Update e di Terze Parti

- ✓ **Wi-Fi Security**
  - Sniffing
  - Rogue Access Point
  - BYOD (Bring Your Device)
  - Separazioni delle reti

- ✓ **Mobile Security**
  - Codici di sblocco
  - Cifratura dei dispositivi
  - Backup locale Vs backup in cloud
  - Root e Jailbreak
  - Spyware
  - Geolocalizzazione
  - Wipe da remoto
  - App e sicurezza

- ✓ **La sicurezza informatica in azienda**
  - Sicurezza a più livelli – fisica – hardware - software
  - Normativa sulla protezione dei dati
  - Granularità e segmentazione
  - Active directory
  - Policy utenti e password
  - Dismissione utenti e caselle di posta
  - Backup

- ✓ **Sicurezza informatica e GDPR**
  - Il GDPR
  - La necessità di formare il personale
  - Articolo 32
    - Cifratura e crittografie
    - Resilienza delle reti
    - Backup e disaster recovery
    - Coockies
  - Articoli 33 e 34
    - Data breach e data leak

- ✓ **Esercitazioni**