



Neural

Innovazione digitale in Veneto

Competenze e tecnologie
per accompagnare le imprese
nella trasformazione digitale

PERCORSO FORMATIVO

Cyber security

**Awareness dipendenti:
fondamenti di sicurezza**



Finanziato
dall'Unione europea
NextGenerationEU

In un contesto in cui le minacce informatiche sono in costante evoluzione, le aziende devono adottare un approccio strutturato e strategico alla sicurezza. La cybersecurity non è più solo una questione tecnica, ma una responsabilità che coinvolge il management, la compliance, la gestione del rischio e la pianificazione della resilienza. Questo corso nasce per rispondere all'esigenza crescente di integrare Governance, Risk Management e Compliance (GRC) nei processi aziendali, offrendo una visione completa delle principali pratiche di sicurezza informatica.

I BENEFICI

Frequentando il corso, i partecipanti:

- Comprendranno i concetti fondamentali di **cybersecurity** e le principali **minacce** del panorama attuale.
- Apprenderanno il significato di **GRC** e il ruolo centrale della **governance** nella protezione dei sistemi aziendali.
- Capiranno l'importanza del **coinvolgimento del management** e della costruzione di una cultura aziendale orientata alla sicurezza.
- Impareranno a identificare, analizzare e gestire i **rischi informatici**, con l'ausilio di **standard internazionali** e strumenti operativi.
- Esploreranno il quadro normativo in materia di **compliance**, compreso il **GDPR** e le implicazioni della non conformità.
- Approfondiranno gli **standard di sicurezza** e i **framework di riferimento** (es. ISO 27001, NIST).
- Svilupperanno competenze operative sui **fondamenti di sicurezza IT**, dall'analisi delle vulnerabilità al disaster recovery.

Partecipanti:
20 imprese

Struttura:
7 moduli

Durata:
8 h in presenza 100% partecipazione obbligatoria
12 h online 80% partecipazione obbligatoria

Sede:
Centro formazione Esac
via Piazzon, 40 36051 Creazzo, Vicenza

Docente: Vincenzo Lena, Technical PM e Cybersecurity Trainer Tinexta Cyber

MODULO **1**

Martedì **21 Ottobre**
h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Introduzione alla Governance

- Introduzione alla cybersecurity e alle minacce attuali
- Cos'è il GRC?
- Concetti fondamentali di governance in cybersecurity

MODULO **2**

Giovedì **23 Ottobre**
h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Governance in azienda: il ruolo del Management

- Costruire una cultura della cybersecurity
- Ruolo del management e degli stakeholder nella sicurezza informatica
- Creare un programma di cybersecurity
- Misurare la resilienza

MODULO 3

Martedì 28 Ottobre

h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Introduzione alla Risk Analysis e al Risk Management

- Introduzione al rischio
- I principali standard internazionali di gestione, assessment e controllo del rischio
- Risk Management

MODULO 4

Giovedì 30 Ottobre

h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Risk Analysis nella pratica

- Risk Analysis e strumenti per svolgerla al meglio

MODULO 5

Martedì 4 Novembre

h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Introduzione alla Compliance aziendale

- Normative e leggi sulla cybersecurity
- Conformità normativa e conseguenze per la non conformità
- Preparazione e gestione degli incidenti di sicurezza (IRP)

MODULO 6

Giovedì 06 Novembre

h: 11.00/13.00

REMOTO ((•))

2 h 00 m

Standard di sicurezza per la gestione del GRC

- Pianificazione della continuità operativa (BCP) e ripristino delle attività (DRP)
- Normativa in materia di protezione di dati personali: GDPR
- Standard di sicurezza internazionali (es. ISO 27001) e framework (es. NIST Cybersecurity Framework)

MODULO 7

Venerdì 14 Novembre

h: 10.00/18.00

PRESENZA (•)

8 h 00 m

Fondamenti di sicurezza informatica

- Definizione di Sicurezza Informatica



www.neuraledih.eu



www.ediconfcommercio.it



Scan e Scopri



@ediconfcom