VETORES DE ATAQUE
E MÉTODOS DE PROTEÇÃO EM CIBERSEGURANÇA

Conhecer o inimigo, as suas táticas, comportamentos, capacidades e métodos de atuação é, em linguagem militar, a base de sucesso para a vitória na batalha pela cibersegurança. Tendo por base os vetores de ataque identificados pelo NIST e para ISO 27032, a metodologia de proteção "kill chain" definida pela ENISA permite aos responsáveis de segurança das empresas identificarem os seus controlos de segurança e procedimentos de resposta a incidentes de Cibersegurança de uma forma eficaz.

DESTINATÁRIOS

Gestores de sistemas e tecnologias de informação; Gestores de infraestruturas tecnológicas; Responsáveis pela segurança da informação; Técnicos de informática e comunicações; Consultores; Auditores internos; Alunos universitários ou de mestrado.

OBJECTIVOS

A compreensão do significado de ciberespaço, deep web, darknet e outras componentes de um sistema complexo que motiva a proteção das empresas em cibersegurança;

Com uma abordagem normativa e suportada por informações de instituições credíveis, como são o caso do NIST e da ENISA, este curso tem como objetivo a apresentação das 15 principais ameaças de cibersegurança. Como as conhecer, identificar, responder (se possível) e como prevenir o impacto de cada uma delas.

CONTEÚDO PROGRAMÁTICO

- **O que é o ciberespaço? O que significa cibersegurança?;**
- **Introdução ao significado da NIST Cyber Security Framework;**
- **O significado da ISO 27032 e a sua integração com a segurança da informação;**
- **O papel da ENISA no espaço europeu da cibersegurança;**
- **Identificação do "Top 15" dos vetores de ataque;**
- **O significado prático da "Unified Kill Chain";**
- **Respostas para os vetores de ataque em cibersegurança;**
- **Como conceber uma estratégia para cibersegurança;**
- **Implementação de um Plano de Ciber Resiliência integrado com o Plano de Continuidade de Negócio;**
- **Próximos passos.**

12 horas | 295,00 €