Introdução à Cibersegurança e à Ciberdefesa

Objetivos Gerais:

A extensiva utilização das Tecnologias de Informação e Comunicação associada à elevada taxa de penetração da Internet, promoveu o ciberespaço como um instrumento estruturante do desenvolvimento das sociedades modernas, estimulando o crescimento económico e afirmando-se como uma ferramenta essencial de informação, educação e inclusão social.

O Curso de Cibersegurança tem como finalidade contribuir para a sensibilização e formação de quadros intermédios e superiores, bem como de elementos com potencial para o desempenho de funções relevantes no futuro, habilitando-os a intervir em questões relacionadas com situações de crise no ciberespaço.

Objetivos Específicos:

No final do curso os formandos ficarão aptos a:

- Identificar e caracterizar as componentes tangíveis e intangíveis do ciberespaço;
- Identificar as potenciais ciberameaças e os riscos individuais;
- Identificar as boas práticas associadas à cibersegurança e ciberdefesa;
- Identificar a natureza transversal das ciberameaças e o seu impacto global.
- Caracterizar os constrangimentos operacionais decorrentes do enquadramento legal aplicável à cibersegurança (direito nacional) e ciberdefesa (direito internacional)
- Reconhecer a importância da ciberdefesa das organizacões tanto numa perspetiva nacional como internacional
- Identificar as políticas de cibersegurança e ciberdefesa
- Reconhecer as potenciais ameaças cibernéticas e riscos para as organizações
- Identificar as responsabilidades do indivíduo e o seu papel enquanto agente ativo da cibersegurança e ciberdefesa das organizações.

Destinatários:

Este curso é dirigido a todos os profissionais que necessitem conhecer e aplicar quadros intermédios e superiores, bem como de elementos com potencial para o desempenho de funções relevantes no futuro

Carga Horária:

30 horas

Conteúdo Programático:

Módulo I - Introdução ao ciberespaço e terminologia

Módulo II - Tipos de ataque e de atacantes, métodos e técnicas de proteção correspondentes

Módulo III - Impacto e boas práticas individuais de cibersegurança:

- Desktop e web.

Módulo IV - Regulação e enquadramento legal do ciberespaço:

- Lei do cibercrime;
- Leis internacionais;
- Conflitos armados no ciberespaço.

Módulo V - Impacto e boas práticas de segurança das redes sociais

Módulo VI - Estratégia Nacional de cibersegurança e de ciberdefesa

Módulo VII - Compreensão e avaliação do ambiente da ameaça cibernética

Módulo VIII - Tecnologias emergentes

Módulo IX - Gestão dinâmica do risco

Módulo X - Política de cibersegurança das organizações

- Finalidade e nível de ambição;
- Objetivos a atingir;
- Linhas de ação e definição de prioridades;
- Controlo de execução e alinhamento das ações a desenvolver.