# 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 organizações 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

## Pré-requisitos

Os pré-requisitos necessários para frequentar este curso são:

- Ter acesso a um computador ou um tablet com ligação à Internet e um browser (programa para navegar na web), como o Chrome, Safari, Firefox ou Internet Explorer.
- Pode aceder ao curso a partir de qualquer computador (por exemplo, em casa e no escritório), tablet ou smartphone.

# Conteúdo de Formação a Distância

## Carga Horária

30 Horas

## Conteúdo Programático

**Módulo 0 – Apresentação de Plataforma e Método de Utilização**

**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.

## Metodologia

Este curso tem sempre presente o formador, que irá mesmo dar a formação presencial através da plataforma.

O Formando pode intervir juntamente com o formador ou com os restantes formandos tal como faz na sala de aula.

As apresentações e exercícios serão sempre disponibilizados pelo formador no final de cada sessão de formação.

No final do curso receberá um Certificado de Formação Profissional caso frequente pelo menos 90% das aulas, realize os trabalhos e os testes propostos, participe nas discussões online e tenha avaliação final positiva.

Esta formação é certificada e reconhecida.