Gestão de Segurança da Informação e Cibersegurança

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.

Este Curso 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:

- Implementar soluções técnicas para a definição, manutenção e melhoraria da Gestão de Segurança da Informação;
- Implementar dos mecanismos de controlo;
- Identificar e caraterizar 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;
- Caraterizar 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 uma política de segurança de acordo com as normas em vigor e com os mecanismos de segurança mais recentes.

Carga Horária

60 Horas

Conteúdo Programático

Módulo I – Introdução ao Conceito de Segurança

Módulo II – Normas ISO 27001 e ISO 17799

Módulo III – Segurança Lógica

Módulo IV – Segurança em Redes e Comunicações

Módulo V – Plano de Capacitação e Storage

Módulo VI – Planos de Business Continuity

Módulo VII – Planos de Disaster & Recovery

Módulo VIII - Introdução à Cibersegurança e à Ciberdefesa

- Introdução ao ciberespaço e terminologia;
- Tipos de ataque e de atacantes, métodos e técnicas de proteção correspondentes;
- Impacto e boas práticas individuais de cibersegurança:
  - Desktop e web;
- Regulação e enquadramento legal do ciberespaço:
  - Lei do cibercrime;
  - Leis internacionais;
  - Conflitos armados no ciberespaço.
- Impacto e boas práticas de segurança das redes sociais;
- Estratégia Nacional de cibersegurança e de ciberdefesa;
- Compreensão e avaliação do ambiente da ameaça cibernética;
- Tecnologias emergentes;
- Gestão dinâmica do risco;
- 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.