Noções básicas de cibersegurança

1. ENQUADRAMENTO

A cibersegurança desempenha um papel fundamental na proteção de sistemas, dados e serviços digitais, sendo especialmente relevante no contexto da Administração Pública. A adoção de boas práticas de segurança permite prevenir ataques informáticos, proteger informação sensível e garantir a continuidade dos serviços prestados aos cidadãos.

As noções básicas de cibersegurança incluem a utilização de palavras-passe seguras, a atualização regular de sistemas, o reconhecimento de tentativas de phishing e a proteção de dispositivos e redes. Estas medidas contribuem para reduzir vulnerabilidades e minimizar riscos associados ao uso das tecnologias digitais.

É importante destacar que a implementação de práticas de cibersegurança requer uma abordagem estruturada e contínua, considerando aspetos como a proteção de dados pessoais, a gestão de acessos e a resposta a incidentes. Além disso, é essencial que os funcionários públicos recebam formação adequada nesta área e que exista uma cultura organizacional orientada para a segurança, envolvendo também os cidadãos na adoção de comportamentos digitais responsáveis.

2. CONTEÚDOS PROGRAMÁTICOS

O Curso de "**Noções básicas de cibersegurança"** encontra-se divido nas seções temáticas que a seguir se discriminam, sendo as mesmas lecionadas de forma sequencial e encadeada, dentro dos propósitos e objetivos que se definem nos pontos seguintes.

1. Noções Básicas de Cibersegurança (1h30m)

Apresentação da Formação | Conceitos e Terminologia Essenciais | Principais Ameaças.

2. Autenticação e Gestão de Palavras Passe (2h00m)

Autenticação Multifator | Técnicas de Criação de Palavras Passe

3. Proteção de Dados e de Sistemas (2h00m)

Atualização de Software| Identificação de Vulnerabilidades. Cópias de Segurança.

4. Segurança de Redes (1h30m)

Configuração de Redes | identificação de Portas e IPs.

3. OBJECTIVOS GERAIS

Dotar os formandos de conhecimentos essenciais sobre cibersegurança, permitindo-lhes identificar riscos e adotar comportamentos seguros na utilização de dispositivos e da internet.

4. OBJECTIVOS ESPECÍFICOS (competências a desenvolver)

No final da formação, os formandos deverão ser capazes de:

Compreender o conceito de cibersegurança e a sua importância no dia a dia

Identificar os principais tipos de ameaças digitais (vírus, phishing, malware, etc.)

Reconhecer comportamentos de risco na utilização da internet

Criar e gerir palavras-passe seguras

Identificar tentativas de fraude (ex: emails falsos, mensagens suspeitas)

Adotar boas práticas de segurança em dispositivos e redes

Saber como agir em caso de incidente de segurança

5. DESTINATÁRIOS

São destinatários do Curso "**Noções básicas de cibersegurança**", os quadros da Administração Pública.

6. METODOLOGIAS DE FORMAÇÃO

O programa será todo ministrado na plataforma *online*, com recurso a programas interativos. O modelo de formação presencial é assim substituído por este formato, utilizando-se plataformas e programas informáticos que permitem a interação entre os formandos e o desenvolvimento de salas e grupos de trabalho mais reduzidos.

Existirá sempre uma breve introdução teórica aos temas. Na apresentação de cada tema e subtemas serão apresentados os objetivos específicos a atingir.

Serão criadas dinâmicas em grupo através da criação de salas virtuais de discussão. No final, serão revistos todos os conteúdos e aferidos os objetivos específicos alcançados.

7. RECURSOS DIDÁCTICOS (Equipamentos)

No desenvolvimento do Curso "**Noções básicas de cibersegurança**" utilizar-se-á, via ligação em rede LAN e Acesso à Internet, a aplicação "Zoom" e outros recursos informáticos que

viabilizarão o leccionamento das matérias e o desenvolvimento dos trabalhos em formato *online.*

8. RECURSOS (SUPORTES) PEDAGÓGICOS ESSENCIAIS

Será facultado o "Manual do Formando" em formato E-book e disponibilizados, em formato digital, os conteúdos e informação necessária ao desenvolvimento dos trabalhos práticos.

9. MODALIDADE E FORMA DE ORGANIZAÇÃO

O Curso "**Noções básicas de cibersegurança**" enquadra-se na seguinte modalidade e forma de organização:

OFP - Outra formação profissional não englobada no catálogo nacional de qualificações

Formação à Distância – Totalmente online.

10. METODOLOGIAS DE AVALIAÇÃO

Não haverá lugar à avaliação das aprendizagens apenas à aplicação dos questionários de avaliação da ação (qualidade da formação).

11. DURAÇÃO (carga horária) e HORÁRIO

O Curso "**Noções básicas de cibersegurança**" desenvolver-se-á durante (7horas/1 dia) no horário compreendido entre 09H00 e as 12H30 e entre as 14h00 e as 17h30.

12. PRÉ-REQUISITOS

Ser associado do STE e ter as quotas em dia.

13. REFERÊNCIAS, DATAS E LOCAIS

Ref.ª 222.2026.01
11 de maio de 2026

14. FORMADOR

Dr. José Rendeiro

Licenciado em Gestão pela Instituto Superior de Gestão. É consultor na área da avaliação de carteira de créditos. É Responsável técnico pela formação no âmbito do sistema de apoio à transformação digital da Administração Pública no município da Azambuja.