

AÇÃO DE SENSIBILIZAÇÃO EM CIBER-HIGIENE

Descrição:

Ação que desenvolve as *soft skills* em cibersegurança, trabalhando competências essenciais para a promoção de comportamentos seguros e para uma prevenção básica de ameaças à cibersegurança. Estes módulos pretendem transmitir os conhecimentos e as atitudes primordiais para a adoção de comportamentos seguros no ciberespaço.

Objetivos de aprendizagem:

1. Identificar e compreender as principais ameaças em ambientes digitais;
2. Identificar as diferentes formas de proteção e medidas de segurança, tendo em conta a confiabilidade e a privacidade na utilização dos dispositivos digitais;
3. Proteger os dados pessoais e a privacidade em ambientes digitais, bem como os próprios dispositivos e conteúdos digitais.

Público-alvo:

Cidadão/colaborador em geral.

Módulos:

Ciber (in)segurança (50m)

Ciber-higiene e boas práticas de Cibersegurança (50m)

MÓDULOS

Módulo	Ciber (in)segurança
Destinatários	Cidadãos/colaboradores em geral
Carga horária	50 minutos
Descrição	Neste módulo são apresentadas algumas tipologias comuns de incidentes de segurança informática, apresentando a metodologia de um ciberataque (a sua infraestrutura ofensiva) e explicando cada uma das suas fases. Identificam-se vários casos, particularmente relacionados com o uso quotidiano. Pretende-se reconhecer e combater a ingenuidade no uso do ciberespaço.
Objetivos de aprendizagem	Identificar e compreender os riscos e as ameaças em ambientes digitais.
Conteúdos programáticos	<ol style="list-style-type: none"> 1. As nossas ilusões e o receio necessário; 2. Cibersegurança e cibercrime; 3. Principais ameaças e casos; 4. Visualização de ataques.
Metodologia de ensino	Método dialógico, com apresentação de casos e exercícios ao longo da apresentação.
Modelos de maturidade	Prevenção.

Módulo	Ciber-higiene e boas práticas de Cibersegurança
Destinatários	Cidadãos/colaboradores em geral
Carga horária	50 minutos
Descrição	A melhor forma de mitigar os efeitos nocivos de um ciberataque é através da prevenção. Esta consegue-se com boas práticas que protejam o acesso de terceiros a informação confidencial ou evitem o uso de plataformas maliciosas. Para o efeito, apresentam-se alguns pontos críticos e respetivas boas práticas, promovendo os comportamentos adequados em cada caso.
Objetivos de aprendizagem	Identificar as diferentes formas de proteção e medidas de segurança, tendo em conta a confiabilidade e a privacidade na utilização dos dispositivos digitais; Proteger os dados pessoais e a privacidade em ambientes digitais, bem como os próprios dispositivos e conteúdos digitais.
Conteúdos programáticos	<ol style="list-style-type: none"> 1. Viver em rede; 2. Cuidados de ciber-higiene; 3. Pontos críticos; 4. Boas práticas: <i>password</i>, <i>email</i>, redes sociais, <i>hardware</i> e navegação; 5. Desafio para elaboração de manual de boas práticas.
Metodologia de ensino	Método dialógico, com apresentação de casos, vídeos e exercícios ao longo da apresentação.
Modelos de maturidade	Prevenção.