L’AKADÉMIE DU DIGITAL · PROGRAMA DE FORMAÇÃO Certificação Qualiopi em preparação

# Iniciação à Cibersegurança

**FOR-CYBER-M1-A · Cibersegurança e Conformidade**

Compreender as bases e aplicá-las

**DURAÇÃO**
7 h

**PREÇO**
450 € s/ IVA

**PÚBLICO**
Empresas e particulares

**PRAZO DE ACESSO**
Acesso em 2 dias úteis após validação da necessidade e dos pré-requisitos.

Preços indicados «a partir de», excluindo orçamento específico e promoções. Preços sem IVA, a partir de 2 participantes. IVA a 20 %.

## Objetivos pedagógicos

- Compreender os desafios da cibersegurança na vida pessoal e profissional
- Compreender as principais ameaças digitais: phishing, ransomware, usurpação de identidade, malware, fuga de dados, engenharia social
- Compreender as noções de risco, ameaça, vulnerabilidade, ataque e dado sensível
- Aplicar as boas práticas essenciais de higiene digital
- Reforçar a segurança das suas contas, dispositivos e utilizações digitais
- Reagir de forma adequada em caso de suspeita de incidente cibernético
- Construir um plano de ação simples para melhorar a sua segurança digital

## Público-alvo

- Colaboradores de empresas, dirigentes, trabalhadores independentes, responsáveis associativos
- Pessoal administrativo e utilizadores regulares de ferramentas digitais
- Particulares que queiram proteger as suas utilizações pessoais
- Formandos ou estudantes que descobrem os desafios da cibersegurança

## Pré-requisitos

Os participantes devem saber utilizar um computador ou um smartphone, utilizar regularmente o correio eletrónico, navegar na Internet e dispor de uma experiência básica das ferramentas digitais do dia a dia (contas online, ficheiros, palavras-passe, aplicações, navegador web). Não é exigida nenhuma competência prévia em informática, redes ou cibersegurança. Estes elementos são validados por um formulário online e / ou por uma entrevista prévia.

- Saber utilizar um computador ou um smartphone.
- Utilizar regularmente o correio eletrónico e navegar na Internet.
- Dispor de uma experiência básica das ferramentas digitais do dia a dia (contas, ficheiros, palavras-passe).

- Não é exigida nenhuma competência prévia em informática, redes ou cibersegurança.

## Programa

### TEORIA Módulo Teórico — Compreender os riscos cibernéticos e os bons reflexos

Este primeiro módulo introduz as noções fundamentais da cibersegurança e permite compreender por que razão a segurança digital diz respeito a todos, tanto na esfera pessoal como profissional. Aborda as principais ameaças do quotidiano (phishing, ransomware, usurpação de identidade, burlas online, fuga de dados, software malicioso, engenharia social) através de exemplos simples e concretos. As recomendações assentam nomeadamente nos recursos da ANSSI e da Cybermalveillance.gouv.fr.

**Objetivo :** compreender os riscos digitais comuns e identificar os bons reflexos a adotar para limitar os incidentes cibernéticos num contexto pessoal ou profissional.

- Abordagem acessível a um público não técnico, com exemplos do quotidiano (e-mail, smartphone, cloud, redes sociais, banca online).
- Divulgação do vocabulário de cibersegurança: ameaça, vulnerabilidade, risco, ataque, dado sensível.
- Identificação dos sinais de alerta de uma tentativa de fraude ou de phishing.
- Introdução às boas práticas: palavras-passe robustas, MFA, cópias de segurança, atualizações, vigilância face a ligações e anexos.

**Avaliação :** avaliação formativa: perguntas orais de compreensão, exercícios de reformulação, identificação de situações de risco, quiz intermédio e correção coletiva.

| | | | |
|---|---|---|---|
| Acolhimento e apresentação | 15 min | Apresentar o programa, os objetivos e o desenrolar.<br>Apresentação oral, suporte visual (diapositivos), ronda de apresentações. | |
| Porquê a cibersegurança? | 40 min | Desafios pessoais e profissionais; consequências de um incidente.<br>Exposição interativa, exemplos concretos, debate. | Perguntas orais de compreensão. |
| Panorama das ameaças | 1h00 | Phishing, ransomware, usurpação, malware, fuga de dados, engenharia social.<br>Exposição ilustrada, exemplos reais, recursos ANSSI / Cybermalveillance. | Identificação de situações de risco. |
| Vocabulário de cibersegurança | 45 min | Ameaça, vulnerabilidade, risco, ataque, dado sensível.<br>Exposição, exercícios de reformulação, debate participativo. | Exercícios de reformulação. |
| Boas práticas essenciais | 40 min | Palavras-passe robustas, MFA, cópias de segurança, atualizações, vigilância face a ligações/anexos.<br>Exposição, demonstrações, sinais de alerta do phishing. | Quiz intermédio. |
| Síntese e correção | 10 min | Resumir os pontos-chave; correção coletiva.<br>Resumo, correção coletiva, feedback. | Correção coletiva das aprendizagens. |

### OFICINA Oficina Prática — Construir a sua higiene digital

Este segundo módulo é uma oficina prática dedicada à aplicação das boas práticas. Os participantes realizam um autodiagnóstico das suas utilizações digitais, analisam situações concretas de phishing e constroem um plano de ação pessoal ou profissional. As recomendações sobre palavras-passe e autenticação multifator assentam nomeadamente nos recursos da CNIL. Nenhuma palavra-passe real ou identificador pessoal é solicitado durante a oficina.

**Objetivo :** pôr em prática os bons reflexos de cibersegurança e construir uma lista de verificação de higiene digital aplicável imediatamente após a formação.

- Oficina concreta e orientada para a ação: autodiagnóstico das práticas digitais.
- Análise de falsos e-mails de phishing e identificação dos sinais suspeitos.
- Construção de uma lista de verificação de higiene digital e priorização das ações.
- Elaboração de um plano de ação individual ou profissional, no respeito pela confidencialidade.

**Avaliação :** avaliação prática: grelha de autodiagnóstico preenchida, análise de casos de phishing, lista de verificação de ações prioritárias, plano de ação final, apresentação oral curta e quiz final de validação.

| | | | |
|---|---|---|---|
| Início da oficina | 15 min | Apresentar o objetivo: uma lista de verificação de higiene digital.<br>Apresentação, lembrete de confidencialidade (nenhuma palavra-passe real). | |
| Autodiagnóstico | 45 min | Avaliar as suas próprias utilizações digitais.<br>Grelha de autodiagnóstico, trabalho individual, acompanhamento. | Grelha de autodiagnóstico preenchida. |
| Análise de phishing | 1h00 | Analisar falsos e-mails e identificar os sinais suspeitos.<br>Estudo de caso de phishing, identificação coletiva dos indícios. | Análise de casos de phishing. |
| Lista de verificação e priorização | 45 min | Construir uma lista de verificação e priorizar as ações.<br>Oficina de construção, matriz impacto/facilidade. | Lista de verificação de ações prioritárias. |
| Plano de ação e apresentação de resultados | 35 min | Elaborar um plano de ação e apresentá-lo.<br>Modelo de plano de ação, apresentação oral curta, feedback. | Plano de ação final + quiz final. |
| Inquérito de satisfação | 10 min | Recolher a satisfação a quente.<br>Questionário de satisfação. | Inquérito de satisfação. |

## Modalidades e meios pedagógicos

Formação presencial nas nossas instalações ou nas suas, em grupo reduzido. Alternância de contributos teóricos, oficinas práticas e simulações.

**Material necessário :**

16 GB de RAM

## Modalidades de avaliação

Avaliação das aprendizagens durante e no final da formação; certificado de conclusão entregue a cada formando.

## Acessibilidade

Formação acessível a pessoas com deficiência. Contacte-nos antes da inscrição para estudarmos as adaptações necessárias.

## Financiamento

Orçamento ou convenção de formação a pedido. A certificação Qualiopi está em preparação: a elegibilidade para financiamentos OPCO será aberta após a sua obtenção.

Auditoria de certificação prevista para T1 2027. Sem elegibilidade OPCO antes da sua obtenção.