Curso ATVC300 - Vibe coding nas organizações | Riscos, regras e adoção

Duração: 4h

Introdução

Com os agentes de IA, qualquer colaborador consegue criar uma aplicação a descrever o que pretende. Isso acelera o trabalho e traz riscos novos: aplicações com dados da organização que ninguém reviu, que ninguém registou e que ninguém sabe manter. Este curso dá à gestão, à equipa de TI e aos responsáveis de segurança e de conformidade o que precisam para decidir como a organização usa o vibe coding.

Numa sessão de quatro horas, em linguagem de gestão, o curso mostra o que é o vibe coding, com uma demonstração do pedido à aplicação a funcionar, percorre os riscos e o enquadramento legal, e termina com as regras e o plano de adoção de cada organização. Não exige conhecimentos de programação.

O Regulamento da Inteligência Artificial da União Europeia, na redação do Regulamento (UE) 2026/1744, prevê no artigo 4.º que as organizações que utilizam sistemas de IA adotem medidas para promover a literacia no domínio da IA do seu pessoal. Esta formação pode ser uma dessas medidas: o certificado de formação e o registo de presenças documentam a participação de cada pessoa.

Público-alvo

Este curso destina-se a administradores, diretores e gestores, a responsáveis de sistemas de informação, de segurança, de proteção de dados, de conformidade e de inovação, e a quem tem de definir ou aprovar as regras de utilização de IA na organização.

No final do curso

Após a conclusão deste curso, os formandos deverão ser capazes de:
• Explicar o que é o vibe coding e que aplicações permite criar.
• Identificar os riscos de segurança, de dados, de continuidade, de propriedade intelectual e de custo.
• Enquadrar o tema no RGPD, no Regulamento da IA e, para as entidades abrangidas, no Regime Jurídico da Cibersegurança.
• Definir níveis de aplicação e o que cada um exige antes de entrar em uso.
• Escolher as ferramentas e os planos autorizados, e as regras para o código e para os dados.
• Preparar o plano de adoção: piloto, formação por perfil e inventário das aplicações criadas.

Pré-requisitos

• Não são necessários conhecimentos de programação.

Exames de certificação

(não existem exames)

Conteúdo programático em detalhe

O que é o vibe coding e quem o está a fazer

• Aplicações criadas a descrever o que se pretende: demonstração, do pedido à aplicação a funcionar
• Quem constrói: programadores com agentes de IA e colaboradores que nunca programaram
• O que já existe na organização sem que ninguém o tenha decidido
• O que se ganha: protótipos, ferramentas internas e tempo das equipas de desenvolvimento

Os riscos

• Segurança: código que ninguém leu, dependências não verificadas e chaves de acesso expostas
• Dados: informação pessoal e confidencial nos pedidos e nas aplicações criadas
• Continuidade: quem mantém uma aplicação que o autor não sabe ler
• Propriedade intelectual e licenças: o que os termos de cada fornecedor preveem
• Custos: subscrições, consumo e alojamento

O enquadramento legal

• O RGPD nas aplicações criadas com IA: as mesmas obrigações de qualquer outro sistema
• A literacia em IA no Regulamento da IA da União Europeia (artigo 4.º)
• Para as entidades abrangidas pelo Regime Jurídico da Cibersegurança (Decreto-Lei n.º 125/2025): a segurança na aquisição, desenvolvimento e manutenção dos sistemas e a segurança da cadeia de abastecimento (artigo 27.º)
• Os planos para organizações dos fornecedores: o que preveem sobre os dados e o treino dos modelos

As regras da organização

• Três níveis de aplicação: protótipo pessoal, ferramenta interna e aplicação com dados de clientes ou exposta ao exterior
• O que cada nível exige: revisão, testes, aprovação e registo
• Ferramentas e contas autorizadas, e as definições geridas pela organização
• Onde podem ficar o código e os dados
• Exercício: a matriz de regras da organização de cada participante

Adoção

• Por onde começar: casos de uso, piloto e medição dos resultados
• Formação por perfil: quem constrói sem programar, quem programa e quem aprova
• O inventário das aplicações criadas e a sua revisão periódica
• O papel da equipa de TI e do responsável de segurança
• O plano dos primeiros 90 dias