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

Cibersegurança para Gestores

FOR-CYBER-M3-A · Cibersegurança e Conformidade

Gerir a segurança digital da sua equipa e da sua organização

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 estratégicos e financeiros da cibersegurança para a organização
- Identificar os principais riscos e o seu impacto no negócio (interrupção da atividade, imagem, conformidade)
- Integrar a segurança na gestão: política, sensibilização, cultura do risco
- Conhecer as normas e os quadros de referência úteis para a gestão (ISO 27001, NIST, recomendações da ANSSI)
- Construir e gerir um plano de resposta a incidentes e um plano de continuidade
- Dialogar eficazmente com as equipas técnicas e os prestadores (RSSI, DSI)

Público-alvo

- Gestores, chefes de equipa, chefes de serviço e responsáveis operacionais
- Dirigentes de micro e pequenas empresas / PME, responsáveis de RH, responsáveis de local
- Qualquer pessoa em posição de chefia chamada a gerir ou a defender a segurança digital

Pré-requisitos

- Saber utilizar um computador e as ferramentas de escritório comuns.
- Exercer uma função de chefia ou de responsabilidade (uma mais-valia).
- Ter uma sensibilização de base para a cibersegurança (módulo Iniciação aconselhado).
- Ter motivação para gerir a segurança digital do seu perímetro.

Programa

TEORIA Módulo Teórico — Gerir a cibersegurança à escala da organização

Este módulo posiciona a cibersegurança como um desafio estratégico (riscos de negócio, custos de um incidente, responsabilidade do gestor) e ensina a mapear os riscos para além da vertente técnica (ativos sensíveis, vulnerabilidades organizacionais). Dá destaque ao fator humano (sensibilização, cultura do risco, política de segurança, carta informática), apresenta os quadros de referência para a gestão (ISO 27001, NIST, recomendações da ANSSI) e aborda a gestão de crises cibernéticas (plano de resposta a incidentes, PCA/PRA, comunicação), bem como o diálogo com as equipas técnicas e os prestadores.

Objetivo : dar aos gestores as referências para gerir a segurança digital do seu perímetro, decidir e mobilizar as suas equipas.

- Ângulo de gestão e estratégico, acessível a não técnicos.
- Mapeamento de riscos orientado para o impacto no negócio.
- Quadros de gestão (ISO 27001, NIST, ANSSI) e gestão de crises.

Avaliação : Questionário de escolha múltipla sobre os desafios e os quadros de referência, exercício de mapeamento dos riscos de negócio.

Acolhimento e apresentação	15 min	Apresentar o programa, os objetivos e o desenrolar. Apresentação oral, suporte visual (diapositivos), ronda de apresentações.	
A cibersegurança, desafio estratégico	40 min	Riscos de negócio, custos de um incidente, responsabilidade do gestor. Exposição interativa, exemplos de incidentes, debate.	Perguntas orais de compreensão.
Mapeamento dos riscos	45 min	Ativos sensíveis, ameaças, vulnerabilidades organizacionais. Método de mapeamento, modelo, exercício.	Exercício de mapeamento dos riscos de negócio.
Fator humano e política	45 min	Sensibilização, cultura do risco, política de segurança, carta informática. Exposição, exemplos de políticas, discussão em grupo.	Questionário intermédio de escolha múltipla.
Quadros e gestão de crises	50 min	ISO 27001, NIST, ANSSI; plano de resposta a incidentes, PCA/PRA, diálogo RSSI/DSI. Exposição estruturada, esquema NIST, exemplos de planos.	Questionário de escolha múltipla sobre os quadros de referência.
Síntese	10 min	Resumir os pontos-chave e preparar a oficina. Resumo, feedback dos participantes.	Questionário rápido de escolha múltipla no final do módulo.

OFICINA Oficina Prática — Construir a sua gestão da segurança

A partir da sua organização ou de um caso condutor, os participantes mapeiam os riscos cibernéticos prioritários e o seu impacto no negócio, elaboram as linhas gerais de uma política de segurança e de um plano de sensibilização das equipas, constroem um plano simplificado de resposta a incidentes (papéis, etapas, comunicação) e definem indicadores de gestão, bem como um roteiro priorizado.

Objetivo : sair com um mapeamento dos riscos, um esboço de política de segurança, um plano de resposta a incidentes e um roteiro de gestão.

- Possibilidade de trabalhar diretamente sobre o contexto real da organização.
- Produção de ferramentas de gestão: política, plano de sensibilização, plano de resposta.
- Definição de indicadores de gestão (KPI de segurança).
- Roteiro priorizado e orientado para a decisão.

Avaliação : produção dos entregáveis (mapeamento dos riscos, esboço de política, plano de resposta a incidentes, roteiro), apresentação oral curta e revisão coletiva.

Início da oficina	15 min	Apresentar o objetivo e escolher a sua organização ou um caso condutor. Apresentação, constituição dos grupos.	
Mapeamento dos riscos	50 min	Mapear os riscos cibernéticos prioritários e o seu impacto no negócio. Trabalho prático guiado, modelo de mapeamento, acompanhamento.	Entregável: mapeamento dos riscos.
Política e sensibilização	50 min	Elaborar as linhas gerais de uma política de segurança e de um plano de sensibilização. Trabalho prático colaborativo, modelos, debate.	Entregável: esboço de política + plano de sensibilização.
Plano de resposta a incidentes	45 min	Construir um plano de resposta simplificado (papéis, etapas, comunicação). Trabalho prático guiado, modelo de plano de resposta, jogo de papéis curto.	Entregável: plano de resposta a incidentes.
KPI e roteiro	25 min	Definir indicadores de gestão e um roteiro; apresentar. Modelo de indicadores, apresentações curtas, feedback.	Avaliação sumativa: roteiro + questionário final de escolha múltipla.
Inquérito de satisfação	10 min	Recolher a satisfação a quente. 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 :

8 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.