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

ISO 27001: primeiros passos (SGSI)

FOR-CYBER-M5-A · Cibersegurança e Conformidade

Descobrir o sistema de gestão da segurança da informação e iniciar o seu processo

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 o que é um SGSI (Sistema de Gestão da Segurança da Informação) e a lógica da ISO/IEC 27001
- Situar a ISO 27001 na família ISO 27000 e face aos outros quadros (NIST, ANSSI, RGPD)
- Compreender as noções-chave: perímetro, partes interessadas, avaliação e tratamento dos riscos, declaração de aplicabilidade (SoA)
- Identificar as grandes etapas de um processo de certificação (PDCA, auditorias, medidas do Anexo A)
- Realizar uma avaliação de riscos simplificada e iniciar uma declaração de aplicabilidade
- Construir um roteiro realista rumo a um processo ISO 27001

Público-alvo

- Responsáveis de segurança, RSSI em início de funções, diretores de sistemas de informação, responsáveis de qualidade e conformidade
- Gestores de projeto e responsáveis envolvidos num processo de certificação
- Dirigentes de PME/empresas de média dimensão que ponderam um processo ISO 27001

Pré-requisitos

- Saber utilizar um computador e as ferramentas de escritório comuns.
- Ter uma sensibilização para a cibersegurança (módulo Iniciação aconselhado) ou para a gestão (módulo Gestores).
- Uma experiência em qualidade/conformidade (ISO 9001, RGPD) facilita a compreensão (uma mais-valia).
- Ter motivação para iniciar um processo estruturado de segurança da informação.

Programa

TEORIA Módulo Teórico — Compreender a ISO 27001 e o SGSI

Este módulo explica os desafios da segurança da informação (confidencialidade, integridade, disponibilidade), a família ISO 27000 e o posicionamento da ISO 27001 face ao NIST, à ANSSI e ao RGPD. Apresenta o espírito do SGSI (abordagem baseada nos riscos, melhoria contínua PDCA, empenho da direção), a estrutura da norma, a avaliação e o tratamento dos riscos, o panorama das medidas do Anexo A, a declaração de aplicabilidade (SoA) e o percurso de certificação.

Objetivo : compreender a lógica e o vocabulário da ISO 27001 e do SGSI para poder iniciar um processo estruturado.

- Divulgação da norma e da lógica do SGSI (CID, PDCA).
- Posicionamento claro face aos outros quadros (NIST, ANSSI, RGPD).
- Compreensão da avaliação de riscos, do Anexo A e da SoA.

Avaliação : Questionário de escolha múltipla sobre a norma e o vocabulário do SGSI, exercício de posicionamento dos quadros de referência.

Acolhimento e apresentação	15 min	Apresentar o programa, os objetivos e o quadro (iniciação não certificante). Apresentação oral, suporte visual (diapositivos), ronda de apresentações.	
Segurança da informação e CID	35 min	Desafios; confidencialidade, integridade, disponibilidade; porquê uma norma. Exposição interativa, exemplos, debate.	Perguntas orais de compreensão.
Família ISO 27000 e quadros	40 min	Posicionamento da ISO 27001; articulação com NIST, ANSSI, RGPD. Exposição, quadro de posicionamento, exercício.	Exercício de posicionamento dos quadros.
O espírito do SGSI	50 min	Abordagem baseada nos riscos, PDCA, empenho da direção, estrutura da norma. Exposição estruturada, esquema PDCA, exemplos.	Questionário de escolha múltipla sobre a norma e o SGSI.
Riscos, Anexo A e SoA	55 min	Avaliação/tratamento dos riscos, medidas do Anexo A, declaração de aplicabilidade, certificação. Exposição, panorama do Anexo A, exemplo de SoA.	Questionário intermédio de escolha múltipla sobre o vocabulário.
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 — Iniciar o seu processo SGSI

A partir de um caso condutor ou da sua organização, os participantes definem o perímetro de um SGSI e identificam as partes interessadas, realizam uma avaliação de riscos simplificada (ativos, ameaças, vulnerabilidades, avaliação), escolhem medidas de tratamento e iniciam uma declaração de aplicabilidade (SoA) sobre uma amostra do Anexo A e constroem depois um roteiro realista rumo a um processo ISO 27001.

Objetivo : iniciar concretamente um processo SGSI: perímetro, avaliação de riscos, esboço de SoA e roteiro.

- Possibilidade de trabalhar diretamente sobre o contexto real da organização.
- Avaliação de riscos simplificada e acionável.
- Início de uma declaração de aplicabilidade (SoA) sobre o Anexo A.
- Roteiro realista rumo à certificação.

Avaliação : produção dos entregáveis (perímetro, avaliação de riscos, esboço de SoA, 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.	
Perímetro e partes interessadas	45 min	Definir o perímetro de um SGSI e identificar as partes interessadas. Trabalho prático guiado, modelo de perímetro, acompanhamento.	Entregável: perímetro + partes interessadas.
Avaliação de riscos	1h00	Identificar ativos, ameaças, vulnerabilidades e avaliar os riscos. Trabalho prático colaborativo, grelha de avaliação de riscos.	Entregável: avaliação de riscos.
Tratamento e esboço de SoA	45 min	Escolher medidas e iniciar uma declaração de aplicabilidade (amostra do Anexo A). Trabalho prático, extrato do Anexo A, modelo de SoA.	Entregável: esboço de SoA.
Roteiro e apresentação de resultados	25 min	Construir um roteiro rumo à ISO 27001; apresentar. Modelo de roteiro, 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.