Normas de sistemas de gestão

ISO/IEC 27005:2022 — Riscos SI

Dois dias para conduzir a avaliação e o tratamento dos riscos de segurança da informação exigidos pela ISO/IEC 27001:2022, seguindo as recomendações da ISO/IEC 27005:2022. Abordagem por eventos ou por ativos, cenários, critérios, plano de tratamento, aceitação dos riscos residuais: o método é aplicado aos seus sistemas de informação e aos seus prestadores, até um registo de riscos utilizável.

Duração : 2 dias

Objetivos

1. Explicar o papel da ISO/IEC 27005:2022 face aos requisitos da ISO/IEC 27001:2022
2. Definir o contexto, os critérios de aceitação e os critérios de avaliação dos riscos
3. Identificar cenários de risco segundo uma abordagem por eventos ou por ativos
4. Analisar e avaliar os riscos e construir depois um plano de tratamento ligado aos controlos do anexo A
5. Organizar a monitorização, a revisão e a comunicação dos riscos ao longo do tempo

Programa

Dia 1 — manhã

• Porquê um método: o que a ISO/IEC 27001:2022 exige sobre a avaliação e o tratamento dos riscos

• Vocabulário: fonte de risco, ameaça, vulnerabilidade, evento, consequência, probabilidade

• Contexto, critérios de aceitação dos riscos e critérios de avaliação

• Proprietários dos riscos e papel da direção

Dia 1 — tarde

• Abordagem por eventos e abordagem por ativos: quando escolher uma ou outra

• Ativos, ameaças e vulnerabilidades; construção de cenários de risco

• Análise: consequências, probabilidade, nível de risco

• Exercício: cenários de risco sobre um perímetro da sua empresa (correio eletrónico, ERP, dados de clientes)

Dia 2 — manhã

• Avaliação e hierarquização dos riscos

• Opções de tratamento: reduzir, evitar, partilhar, reter

• Plano de tratamento ligado aos controlos do anexo A e à declaração de aplicabilidade

• Aceitação dos riscos residuais e informação da direção

Dia 2 — tarde (oficina)

• Monitorização e revisão dos riscos: indicadores, gatilhos de atualização

• Comunicação e consulta sobre os riscos

• Oficina: registo de riscos e plano de tratamento do seu perímetro

• Teste de conhecimentos e apresentação do registo

Metodologia

• Exercícios sobre os seus sistemas de informação, os seus fluxos de dados e os seus contratos de subcontratação informática

• Comparação das duas abordagens sobre um mesmo perímetro

• Modelo de registo de riscos e de plano de tratamento, adaptável à sua ferramenta

• Estudo de caso: risco ligado a um prestador de serviços na nuvem

• Quiz de meio da formação e teste final sobre o método

Avaliação e documentos

Quiz de meio da formação e teste de conhecimentos no final da sessão, avaliação a quente em D+1. Certificado de formação numerado, verificável online, para cada participante; relatório de formação, registo de riscos e plano de tratamento resultantes da oficina entregues à empresa.

Materiais bilingues para cada participante; cada formação presencial inclui o seu gémeo digital no OmniLearn.

Bom saber

Esta formação pressupõe o conhecimento dos requisitos da ISO/IEC 27001:2022: a formação “ISO/IEC 27001:2022 — Requisitos” (2 dias) apresenta-os. O método geral de gestão do risco é tratado em “ISO 31000:2018 — Gestão do risco”.

Informações práticas

Duração	2 dias
Público	Responsáveis de segurança da informação, diretores de sistemas de informação, gestores de risco, responsáveis de conformidade, auditores internos do sistema de segurança da informação
Pré-requisitos	Conhecimento de base da ISO/IEC 27001:2022
Número de participantes	Grupos de 6 a 12 participantes, na empresa
Formato	Na empresa, presencial nas suas instalações
Língua	Francês, darija ou inglês; materiais bilingues
Financiamento	Contratos especiais de formação da OFPPT (TFP), GIAC, Maroc PME: preparamos os processos consigo, sem custo adicional.
Personalização do programa	Programa adaptado aos seus procedimentos, aos seus equipamentos e ao seu público

Perguntas frequentes

A ISO/IEC 27005 é certificável?
Não. A ISO/IEC 27005:2022 dá recomendações. Ajuda a satisfazer os requisitos da ISO/IEC 27001:2022 sobre os riscos, que, esses sim, são auditados na certificação.

É preciso um software de gestão de riscos?
Não. Uma folha de cálculo bem estruturada basta para começar. A formação fornece um modelo; a escolha de uma ferramenta vem depois, consoante a dimensão do perímetro e o número de proprietários de riscos.

Qual a diferença para a ISO 31000:2018?
A ISO 31000:2018 dá diretrizes gerais de gestão do risco. A ISO/IEC 27005:2022 aplica-as à segurança da informação: ativos, ameaças, vulnerabilidades, cenários e ligação com os controlos do anexo A da ISO/IEC 27001:2022.

Quem deve participar?
O responsável de segurança da informação, o diretor de sistemas de informação, os gestores de risco e os proprietários de processos de negócio. Os proprietários dos riscos devem compreender o método para poderem aceitar os riscos residuais com conhecimento de causa.