Normas de sistemas de gestão

ISO/IEC 27001:2022 — Requisitos

Dois dias para compreender o que exige a ISO/IEC 27001:2022 e preparar a certificação de um sistema de gestão da segurança da informação. Âmbito, avaliação e tratamento de riscos, declaração de aplicabilidade, 93 controlos do anexo A, incidentes e continuidade: cada noção é aplicada aos seus ativos, aos seus prestadores e aos seus procedimentos. Sai com uma primeira declaração de aplicabilidade e a lista das suas lacunas prioritárias.

Duração : 2 dias

Objetivos

1. Explicar a estrutura da ISO/IEC 27001:2022 e o lugar do anexo A na abordagem
2. Definir o âmbito do sistema a partir do contexto, das partes interessadas e das interfaces com os prestadores
3. Aplicar um método de avaliação e tratamento dos riscos ligados à segurança da informação
4. Construir uma declaração de aplicabilidade justificada a partir dos 93 controlos do anexo A
5. Preparar a gestão de incidentes, a continuidade, a auditoria interna e a revisão pela gestão

Programa

Dia 1 — manhã

• Confidencialidade, integridade, disponibilidade: o que um certificado ISO/IEC 27001 demonstra aos seus clientes

• A família ISO/IEC 27000: papéis respetivos da 27001, da 27002 e da 27005

• Contexto, partes interessadas, requisitos legais e contratuais, incluindo a Lei n.º 09-08 para os dados pessoais

• Âmbito de aplicação: locais, atividades, sistemas de informação, prestadores

Dia 1 — tarde

• Liderança, política de segurança da informação, funções e responsabilidades

• Avaliação de riscos: critérios, identificação, análise, ponderação

• Opções de tratamento, plano de tratamento e aceitação dos riscos residuais pelos respetivos responsáveis

• Exercício: avaliação de riscos de um processo da sua empresa

Dia 2 — manhã

• Anexo A: 93 controlos repartidos em quatro temas — organizacional, humano, físico e tecnológico

• Declaração de aplicabilidade: controlos selecionados, exclusões justificadas, estado de implementação

• Controlos frequentemente examinados em auditoria: direitos de acesso, cópias de segurança, fornecedores e serviços na nuvem, registo de eventos

• Gestão de incidentes de segurança e segurança da informação durante uma perturbação

Dia 2 — tarde (oficina)

• Monitorização, medição, auditoria interna e revisão pela gestão do sistema

• Não conformidades e ações corretivas

• Oficina: esboço da sua declaração de aplicabilidade e lista das lacunas prioritárias

• Teste de conhecimentos e apresentação dos trabalhos

Metodologia

• Leitura comentada dos requisitos e do anexo A
• Exercícios sobre os seus ativos, os seus fluxos de dados e os seus contratos com prestadores informáticos
• Construção guiada de uma declaração de aplicabilidade
• Estudo de caso de um incidente de segurança, da deteção à ação corretiva
• Quiz de meio da formação e teste final sobre os requisitos do sistema

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, esboço da declaração de aplicabilidade e lista de lacunas entregues à empresa.

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

Bom saber

Para aprofundar o método de avaliação de riscos, a formação “ISO/IEC 27005:2022 — Riscos SI” (2 dias) completa esta. A proteção dos dados pessoais e a Lei 09-08 são tratadas em “ISO/IEC 27701:2025 e Lei 09-08”.

Informações práticas

Duração	2 dias
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

É preciso ser informático para frequentar a formação?
Não. Os requisitos da norma incidem primeiro sobre a organização: âmbito, riscos, funções, fornecedores, incidentes. Os controlos técnicos são explicados sem jargão; a presença do diretor de sistemas de informação ou do responsável de segurança ajuda a ligá-los à sua infraestrutura.

A declaração de aplicabilidade deve reter os 93 controlos?
Não. Indica, para cada controlo do anexo A, se é retido ou excluído, e porquê. Estas escolhas decorrem da avaliação e do tratamento dos riscos; o auditor de certificação verifica a sua coerência.

Qual a relação com a Lei 09-08?
A Lei n.º 09-08 enquadra o tratamento de dados de caráter pessoal. A ISO/IEC 27001:2022 pede que se identifiquem os requisitos legais aplicáveis e se tenham em conta: a lei entra no contexto e no tratamento dos riscos, sem que a certificação valha como conformidade legal.

Um local já certificado ISO 9001 pode apoiar-se no seu sistema?
Sim. As duas normas partilham a estrutura harmonizada: controlo documental, auditoria interna, revisão pela gestão e ações corretivas podem ser comuns. O trabalho próprio da ISO/IEC 27001 incide sobre os riscos de segurança da informação e os controlos do anexo A.