devoteam
Cyber Trust

Roadmap ISO 27001

Integrity **5-step** approach to 27001

Versão 2.1

Preparação	1 a 2 meses	**1. Preparação do SGSI** Definir o âmbito adequado às necessidades de negócio e dotar a organização dos conhecimentos necessários.
Diagnóstico	1 a 3 meses	**2. Diagnóstico** No âmbito caracterizado, identificar a maturidade dos processos, dos controlos aplicáveis, dos riscos e dos controlos de mitigação. Compreender o negócio e determinar o gap entre os requisitos do standard e as práticas da organização de forma a alocar recursos para uma implementação eficiente do SGSI.
Implementação	1 a 4 meses	**3. Implementação e documentação do SGSI** Elaborar a documentação obrigatória e iniciar o tratamento de risco tendo em consideração os controlos aplicáveis.
Operação	3 a 6 meses	**4. Operação do SGSI** Executar os processos e procedimentos definidos evidenciando o cumprimento dos objetivos, identificar oportunidades de melhoria e não conformidades e garantir que o SGSI é revisto pela gestão de topo.
Certificação e acompanhamento	1 mês + 3 anos	**5. Certificação e acompanhamento** Auditoria elaborada por uma terceira parte de modo a demonstrar a maturidade do SGSI e redução do risco de acordo com os objetivos definidos. Acompanhamento do SGSI sobre a forma de serviços de operação e gestão (planeamento, avaliação de desempenho e melhoria contínua).

devoteam
Cyber Trust

Roadmap ISO 27001

1. Preparação do SGSI | 1 a 2 meses

Definição do âmbito

Caracterizar as unidades funcionais, processos de negócio, geografia e bens a proteger.

Formação específica em ISO 27001

Dotar a equipa de projeto e todas as partes interessadas com conhecimentos em SGSI.

Formação em segurança de informação

Dotar a equipa de projeto com conhecimentos em segurança da informação alinhados com a atualidade.

2. Diagnóstico | 1 a 3 meses

Diagnóstico específico

Compreender o negócio e determinar o gap entre os requisitos do standard e as práticas da organização de forma a alocar recursos para uma implementação eficaz e eficiente do SGSI.

Apresentação de resultados

Apresentar à gestão de topo e a todas as partes interessadas as conclusões da análise efetuada.

Documentar a metodologia de gestão de risco

Elaborar um documento com a descrição das metodologias de análise e tratamento de risco, identificando as responsabilidades, as fontes de ameaças e vulnerabilidades, controlos existentes, a eficácia dos mesmeos e o critério de aceitação do risco.

Avaliação de risco

Início da execução continuada das atividades de avaliação de risco previstas na metodologia de gestão de risco.

Plano de tratamento de risco

Definição de um plano de tratamento de risco de acordo com a metodologia de gestão de risco definida e adotada.

3. Implementação e documentação do SGSI | 1 a 4 meses

Definir a política de segurança da informação e privacidade

Documentar os objetivos de segurança de informação e privacidade da organização, o comprometimento da gestão de topo com a redução de risco e as implicações do não cumprimento da política definida.

Documentar os processos do SGIP

Elaborar documentos com a descrição dos processos, respetivas responsabilidades, identificando os registos e evidências adequadas.

Declaração de aplicabilidade (SoA)

Elaboração de um registo com a informação dos controlos aplicáveis, eventuais exclusões e as respetivas justificações.

Aprovação da documentação

Aprovação pela gestão de topo do âmbito do SGIP, da política de segurança da informação e privacidade, da avaliação de risco, plano de tratamento de risco, restantes documentos do SGIP e SoA.

Pontos de situação mensais

Atualização do plano de projeto, identificação do atingimento do projeto e eventuais constrangimentos identificados.

4. Operação do SGSI | 3 a 6 meses

Formação e sensibilização

Planeamento e execução de ações de formação e sensibilização a toda a organização no âmbito do SGSI.

Gestão de processos

Execução de forma continuada das tarefas dos diversos processos definidos e documentados.

Monitorização do SGSI

Acompanhamento e aferição das métricas e objetivos do SGSI.

Revisão do SGSI

Revisão formal pela gestão de topo dos inputs e outputs do SGSI de acordo com o standard.

Auditoria interna

Execução de uma ação formal de auditoria interna, analisando registos e evidências da execução dos processos definidos.

5. Certificação e acompanhamento | 1 mês + 3 anos

Pré-Auditoria (1 mês)

Executado pela entidade certificadora.

Auditoria de concessão (1º ano)

Auditoria de acompanhamento (2º e 3º ano)

Executado pela entidade certificadora.