devoteam
Cyber Trust

Roadmap ISO 27701

Integrity **5-step** approach to 27701

Preparação	1 mês	**1. Preparação** 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 os controlos de mitigação. Compreender o negócio e determinar o GAP entre os requisitos da norma e as práticas da organização de forma a alocar recursos para uma implementação eficiente do SGIP.
Implementação	1 a 3 meses	**3. Implementação** Elaborar a documentação obrigatória e iniciar o tratamento de risco tendo em consideração os controlos aplicáveis.
Operação	3 meses	**4. Operação** 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	1 mês	**5. Certificação** Auditoria de terceira parte de modo a demonstrar a maturidade do SGSI e redução do risco de acordo com os objetivos definidos.

devoteam
Cyber Trust

Roadmap ISO 27701

1. Preparação | 1 mês

Definição do âmbito

Caracterizar o contexto da organização envolvido no tratamento de dados pessoais e as respetivas atividades de tratamento, os ativos de informação relacionados e as geografias envolvidas a proteger.

Formação específica em ISO 27701

Dotar a equipa de projeto e todas as partes interessadas com conhecimentos em sistemas de gestão da informação de privacidade.

Pontos de situação mensais

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

2. Diagnóstico | 1 a 3 meses

Diagnóstico específico

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

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 riscos

Elaborar um documento com a descrição das metodologias de avaliação e tratamento de riscos, identificando as responsabilidades, fontes de ameaças e vulnerabilidades, os controlos existentes e sua eficácia e os critérios de aceitação dos riscos.

Avaliação de risco

Início da execução continuada das atividades de avaliação de risco previstas na metodologia de gestão de risco no âmbito no âmbito da proteção de dados pessoais.

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 para os riscos no âmbito da proteção de dados pessoais.

Pontos de situação mensais

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

3. Implementação | 1 a 3 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 | 3 meses

Formação sobre operacionalização SGIP

Planeamento e execução de ações de formação e sensibilização a toda a organização sobre a operacionalização do SGIP.

Gestão de processos

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

Monitorização do SGIP

Acompanhamento e aferição das métricas e objetivos do SGIP.

Auditoria interna

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

Revisão do SGSI

Revisão formal pela gestão de topo dos inputs e outputs do SGIP de acordo com a norma.

Pontos de situação mensais

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

5. Certificação | 1 mês

Auditoria de concessão (1º ano)

Executado pela entidade certificadora.

Auditoria de acompanhamento (2º e 3º ano)

Execução da auditoria pela entidade certificadora.

Auditoria de re-certificação (após 3º ano)

Execução da auditoria pela entidade certificadora.

Manutenção da certificação
(tarefas fora do âmbito do projeto)