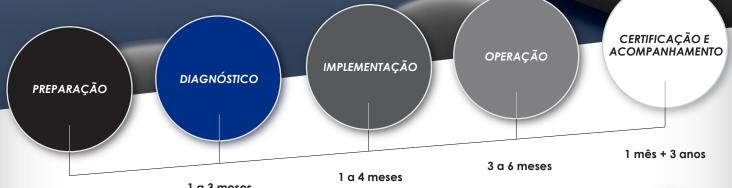


ROADMAP ISO 27001

Integrity 5-step approach to 27001



1 a 2 meses

1 a 3 meses

1. PREPARAÇÃO DO SGSI

Definir o âmbito adequado às necessidades de negócio e dotar a organização dos conhecimentos necessários.

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.

3. IMPLEMENTAÇÃO E DOCUMENTAÇÃO DO SGSI

Elaborar a documentação obrigatória e iniciar o tratamento de risco tendo em consideração os controlos aplicáveis.

4. OPERAÇÃO DO SGSI

Executar os processos e cumprimento dos oportunidades de conformidades e gestão de topo.

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).



1. PREPARAÇÃO DO SGSI

(1 a 2 meses)

DEFINIR O 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 terminar 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 documento com a descrição das metodologías de análise e tratamento de risco, identificando as responsabilidades, as fontes de ameaças e vulnerabilidades, controlos existentes, a eficácia dos mesmos e o critério de aceitação do risco.

AVALIAÇÃO DO RISCO

Início da execução continuada das atividades de análise 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 DE INFORMAÇÃO

Documentar os objetivos de segurança de informação 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 SGSI

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 SGSI, da colítica de segurança, da análise de risco, plano de tratamento de risco e SOA.

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 formo continuada das tarefas dos diversos processos definidos e documentados.

MONITORIZAÇÃO DO SGSI

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)

Execução de uma auditoria nos mesmos moldes que a auditoria de concessão de forma a preparar a equipa de projeto para a certificação efetiva e otimizar aspetos finais do sistema.

AUDITORIA DE CONCESSÃO (1º ano)

AUDITORIA DE ACOMPANHAMENTO (2º e 3º ano)

Executado pela entidade certificadora.

Avaliação de desempenho do SGSI

Ações de Sensibilização e Formação

Auditorias internas

EXECUÇÃO CONTINUADA

Tratamento de risco

Processos e procedimentos operacionais

Revisões pela Gestão