Checklist ISO 27001 Implementando o padrão

Tenha em mente que isso é apenas um modelo; você deve modificá-lo de acordo com suas necessidades específicas.

Pessoas envolvidas Data de entrega

1 Conseguir a aceitação e o apoio

- [ ] Identifique as vantagens da ISO 27001.
- [ ] Identifique as partes interessadas chave.
- [ ] Informe as equipes de apoio técnico sobre os requisitos para aplicar a norma.

2 Estabelecer um órgão de governança

- [ ] Selecione uma equipe.
- [ ] Designe um diretor de projeto.

3 Criar um plano de ação

- [ ] Detecte lacunas e desafios.
- [ ] Liste ideias de melhoria e correção.
- [ ] Defina marcos importantes.
- [ ] Estabeleça critérios de qualidade.

4 Definir um escopo de aplicação

- [ ] Verifique os requisitos de escopo da norma.
- [ ] Determine o que precisa ser protegido.
- [ ] Identifique as dependências e pontos de contato.
- [ ] Estabeleça o impacto total na sua organização.

5 Criar uma política de segurança da informação

- [ ] Busque modelos de governança, risco e conformidade.
- [ ] Defina os requisitos básicos de segurança da informação.
- [ ] Adicione processos e procedimentos.
- [ ] Inclua objetivos.
- [ ] Atribua funções e responsabilidades.

6 Definir a metodologia de avaliação de riscos

- [ ] Crie uma matriz para identificar a probabilidade e o impacto dos riscos.
- [ ] Identifique cenários que possam comprometer informações, sistemas ou serviços.
- [ ] Crie uma metodologia de avaliação de riscos.

7 Criar um registro de riscos

- [ ] Elabore um resumo claro de cada risco, incluindo a probabilidade e o impacto de cada um.

8 Realizar a avaliação de riscos

- [ ] Identifique ameaças e vulnerabilidades.
- [ ] Avalie a probabilidade e o impacto dos riscos.
- [ ] Aplique os tratamentos de risco escolhidos.

9 Redigir a declaração de aplicabilidade

- [ ] Identifique quais controles se aplicam à sua organização.
- [ ] Descreva brevemente e explique as razões para incluir cada um.
- [ ] Descreva como cada controle deve ser implementado e gerenciado.

10 Redigir o plano de tratamento de riscos

- [ ] Desenhe uma resposta para cada risco.
- [ ] Atribua um responsável para cada risco identificado.
- [ ] Atribua responsabilidades pela mitigação do risco e pelas atividades.
- [ ] Estabeleça prazos para concluir as atividades de tratamento de riscos.

11 Definir como medir a eficácia dos seus controles

- [ ] Elabore um plano para medir os objetivos de controle.
- [ ] Crie indicadores-chave de desempenho para acompanhar os controles.
- [ ] Realize testes periódicos dos controles para identificar pontos fracos e vulnerabilidades.

12 Implementar os controles de segurança

- [ ] Crie um protocolo que imponha novos comportamentos e gerencie as expectativas.

13 Criar um programa de treinamento e conscientização

- [ ] Crie materiais de treinamento.
- [ ] Treine seus colegas sobre as ameaças comuns e como responder.
- [ ] Defina as expectativas de cada colega de acordo com seu papel.

14 Colocar em prática a checklist do SGSI

- [ ] Crie uma lista de verificação que o ajude a gerenciar riscos, controles e incidentes de segurança.

15 Monitorar e medir o SGSI

- [ ] Defina o que deve ser supervisionado.
- [ ] Atribua responsabilidades para supervisionar cada elemento.
- [ ] Elabore um plano sobre como as atividades devem ser supervisionadas.

16 Criar um inventário com o InvGate Insight

- [ ] Instale o Agente nos dispositivos ou carregue um arquivo .xls ou .csv.
- [ ] Se escolher o agente, localize os dispositivos conectados à sua rede usando a função Discovery.
- [ ] Importe usuários e locais.

17 Realizar auditorias internas

- [ ] Verifique a conformidade com os requisitos, com o escopo e com a SoA.
- [ ] Compartilhe os resultados da auditoria interna com o órgão do SGSI e a alta administração.
- [ ] Resolva todos os problemas identificados antes de proceder com a auditoria externa.

18 Dispor de um plano para as auditorias externas

- [ ] Contrate um auditor ISO 27001 independente.
- [ ] Realize a Auditoria de Estágio 1, que consiste na revisão completa da documentação.
- [ ] Realize a Auditoria de Estágio 2, que consiste em testes realizados no SGSI.

19 Tomar medidas corretivas quando necessário

- [ ] Aborde qualquer não conformidade identificada pelo auditor da norma ISO 27001.
- [ ] Elabore um plano para gerenciar as possíveis ações corretivas.

20 Incorporar a melhoria contínua

- [ ] Planeje revisões pelo menos uma vez ao ano.