

VOCÊ ESTÁ PRONTO PARA A CERTIFICAÇÃO ISO/IEC 27001:2013?

ITEM	ELEMENTO	27001	CONFORMIDADE (S/N)	COMENTÁRIOS E EVIDÊNCIAS
1	Entendimento da organização e seu contexto: Foram determinadas as questões externas e internas relevantes ao propósito e direcionamento estratégico? Existe evidência do monitoramento e análise crítica das informações sobre essas questões externas e internas?	4.1		
2	Foram definidas as necessidades e expectativas de partes interessadas, com monitoramento e análise crítica?	4.2		
3	O escopo do sistema de gestão de Segurança da Informação (SGSI) foi determinado? Incluindo as questões externas e internas, requisitos das partes interessadas relevantes e dos produtos e serviços da organização. Mantido disponível o escopo como informação documentada.	4.3		
4	Os processos do sistema de gestão de Segurança da Informação são estabelecidos, implementados e mantidos?	4.4		
5	A alta direção demonstra liderança e compromisso com respeito ao sistema de gestão de Segurança da Informação?	5.1		
6	Política do sistema de gestão de Segurança da Informação foi desenvolvida? É apropriada ao contexto da organização e fornece uma estrutura para a definição de objetivos de segurança da informação? Estabelece um compromisso para satisfazer os requisitos aplicáveis e a melhoria contínua do SGSI?	5.2		
7	As responsabilidades e autoridades para funções relevantes são atribuídas, comunicadas e compreendidas? Incluindo relatórios de desempenho e integridade do SGSI mantidos?	5.3		
8	Risco e oportunidades foram determinados? Incluindo os resultados pretendidos do SGSI podem ser alcançados, para melhorar os efeitos desejáveis, reduzir / prevenir efeitos indesejados e obter melhorias.	6.1.1		
9	O processo de avaliação de risco de segurança da informação definido e aplicado?	6.1.2 6.1.3		
11	Uma declaração de aplicabilidade desenvolvida, incluindo justificativa de inclusões e justificativa de exclusões de controles do Anexo A?	Anexo A		
12	Os objetivos de segurança da informação foram estabelecidos em funções / níveis relevantes com informações documentadas mantidas?	6.2		
13	Os recursos foram determinados e fornecidos para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI?	7.1		
14	Foram determinadas competências necessárias? para garantir que as pessoas competentes com base em educação, treinamento, experiência, avaliação da eficácia das ações tomadas e informações apropriadas que sejam documentadas e mantidas como evidência de competência.	7.2		

ITEM	ELEMENTO	14001	CONFORMIDADE (S/N)	COMENTÁRIOS E EVIDÊNCIAS
15	Foram determinadas comunicações internas/ externas? Incluindo o que será comunicado, quando, com quem, como e quem se comunicará.	7.4		
16	A organização assegurou que a documentação tenha identificação e descrições adequadas, formatos e seja revisado/ aprovado?	7.5.2		
17	A distribuição, acesso, recuperação, uso, armazenamento, preservação, controle de mudanças, atividades de retenção e disposição estão em vigor para informações documentadas?	7.5.3		
18	Os processos necessários para atender aos requisitos de segurança da informação são planejados, implementados e controlados? São implementados planos para atingir os objetivos de segurança da informação? Os processos terceirizados são determinados e controlados?	8.1		
19	Forma determinados requisitos de monitoramento e medição? (Incluindo processos e controles de segurança da informação), métodos, quando executados e resultados.	9.1.1		
20	Foi estabelecido um programa de auditoria planejado, estabelecido e mantido com informação documentada? Auditoria interna foi realizada? Os resultados da auditoria interna estão disponíveis?	9.2		
21	É realizado uma Análise Crítica do SGSI em intervalos planejados para garantir a continuidade da adequação, e eficácia?	9.3		
22	Não conformidade e ações corretivas são analisadas e avaliadas? São revisadas para efetividade e retidas como informações documentadas?	10.1		
23	Existe evidência de melhoria contínua do sistema de gestão de segurança da informação?	10.3		