QMS CERTIFICATION

www.qmsbrasil.com.br
contato@qmsbrasil.com.br
+55 11 2628-6095

VOCÊ ESTÁ PRONTO PARA A CERTIFICAÇÃO ISO/IEC 27001:2022 e 27701:2019?

ITEM	ELEMENTO	27001 e 27701	CONFORMIDADE (S/N)	COMENTÁRIOS E EVIDÊNCIAS
1	Entendimento da organização e seu contexto: Foram determinadas as questões externas e internas relevantes ao propósito e que afetam sua capacidade de alcançar o(s) resultado(s) pretendido(s) do ISMS?	4.1 (27001) 5.2.1 (27701)		
2	Foram definidas as necessidades e expectativas de partes interessadas, com monitoramento e análise crítica dos requisitos considerados relevantes e abordados pelo o SGSI?	4.2 (27001) 5.2.2 (27701)		
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? O escopo é mantido disponível como informação documentada?	4.3 (27001) 5.2.3 (27701)		
4	Os processos do sistema de gestão de Segurança da Informação são estabelecidos, implementados e mantidos?	4.4 (27001) 5.2.4 (27701)		
5	A alta direção demonstra liderança e compromisso com respeito ao sistema de gestão de Segurança da Informação, assegurando recursos e promovendo sua melhoria?	5.1 (27001)		
6	A Política do ISMS 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 ISMS?	5.2 (27001) 6.2.1.1 (27701)		
7	As responsabilidades e autoridades para funções relevantes são atribuídas, comunicadas e compreendidas? Relatórios de desempenho e integridade do ISMS são mantidos?	5.3 (27001) 6.3.1.1 – 6.3.2.1 (27701)		
8	Risco e oportunidades foram determinados? Incluindo os resultados pretendidos do ISMS podem ser alcançados, para melhorar os efeitos desejáveis, reduzir / prevenir efeitos indesejados e obter melhorias? A organização determinou como integrar e implementar estas ações dentro dos processos do seu sistema de gestão da segurança da informação e avaliou a eficácia destas ações?	6.1.1 (27001) 5.4.1.1 (27701)		
9	O processo de avaliação de risco de segurança da informação foi definido e aplicado?	6.1.2 - 8.2 (27001) 5.4.1.2 (27701)		

ITEM	ELEMENTO	27001 e 27701	CONFORMIDADE (S/N)	COMENTÁRIOS E EVIDÊNCIAS
10	Foi definido e aplicado um processo para o tratamento de riscos de segurança da informação, determinando os controles necessários?	6.1.3 - 8.3 (27001) 5.4.1.3 (27701)		
11	Foi desenvolvida uma Declaração de Aplicabilidade (SoA), incluindo justificativas para as inclusões e exclusões dos controles estabelecidos no Anexo A?	5.4.1 (27701) Anexos A e B (27701)		
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 qualificações necessárias para garantir que as pessoas são competentes com base em educação, treinamento ou experiência; além da avaliação da eficácia das ações tomadas para adquirir competência? As informações apropriadas são documentadas e mantidas como evidência de competência?	7.2 (27001) 6.4.2.2 (27701)		
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 para adequação e adequação?	7.5.2 (27001) 6.5.2 (27701)		
17	A distribuição, acesso, recuperação, uso, armazenamento, preservação, controle de mudanças, retenção e descarte 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, periodicidade e resultados?	9.1		
20	Foi estabelecido um programa de auditoria planejado e mantido como informação documentada, sendo evidência do programa e resultados de auditoria?	9.2		
21	É realizada uma Análise Crítica do SGSI em intervalos planejados para garantir a continuidade da adequação e eficácia?	9.3		
22	Não conformidades e ações corretivas são analisadas, avaliadas e revisadas para efetividade, além de serem retidas como informações documentadas?	10.1		

ITEM	ELEMENTO	27001 e 27701	CONFORMIDADE (S/N)	COMENTÁRIOS E EVIDÊNCIAS
23	A organização assegurou a melhoria contínua do SGSI, incluindo adequação e eficácia?	10.2		