Kit de documentação Premium da ISO 27001 e ISO 22301

https://advisera.com/27001academy/pt-br/kit-de-ferramentas-da-documentacao-premium-da-iso-27001-e-da-iso-22301/

Nota: A documentação deve preferencialmente ser implementada na ordem em que está listada aqui. A ordem de implementação da documentação relativa ao Anexo A está definida no Plano de tratamento de riscos.

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
	01	**Gestão de documentos**			
1	01	Procedimento de controle de documentos e registros	ISO 27001 7.5; A.5.33 ISO 22301 7.5		
	02	**Preparações para o projeto**			
2	02	Plano do projeto			
	03	**Identificação de requisitos**			
3	03	Procedimento para identificação de requisitos	ISO 27001 4.2; A.5.31 ISO 22301 4.2		
4	03.1	Anexo 1 – Lista de obrigações legais, regulamentares, contratuais e outras	ISO 27001 4.2; A.5.29; A.5.31 ISO 22301 4.2	✓*	✓
	04	**Escopo do SGSI**			
5	04	Documento sobre o escopo do SGSI	ISO 27001 4.3	✓	
	05	**Políticas gerais**			
6	05	Política de segurança da informação	ISO 27001 5.2; 5.3**; 6.2; 7.4; A.6.3	✓	
	06	**Avaliação de riscos e tratamento de riscos**			

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
7	06	Metodologia de avaliação e tratamento de riscos	ISO 27001 6.1.2; 6.1.3; 8.2; 8.3 ISO 22301 8.2.1; 8.2.3	✓	
8	06.1	Anexo 1 – Tabela de avaliação de riscos	ISO 27001 6.1.2; 8.2 ISO 22301 8.2.3	✓	
9	06.2	Anexo 2 – Tabela de tratamento de riscos	ISO 27001 6.1.3; 8.3 ISO 22301 8.2.3	✓	
10	06.3	Anexo 3 – Relatório de avaliação e tratamento de riscos	ISO 27001 8.2; 8.3 ISO 22301 8.2.3	✓	
	07	**Aplicabilidade de controles**			
11	07	Declaração de aplicabilidade	ISO 27001 6.1.3 d)	✓	
	08	**Plano de implementação**			
12	08	Plano de tratamento de riscos	ISO 27001 6.1.3; 6.2; 7.1; 8.3; 9.1	✓	
	09	**Controles de segurança do Anexo A da ISO 27001**			
13	09.01	Política de segurança de TI	ISO 27001 A.5.9; A.5.10; A.5.11; A.5.14; A.5.17; A.5.32; A.6.7; A.7.7; A.7.9; A.7.10; A.8.1; A.8.7; A.8.10; A.8.12; A.8.13; A.8.19; A.8.23	✓*	
14	09.02	Política de mesa limpa e tela limpa (Nota: Esta Política pode ser implementada como parte da Política de segurança de TI)	ISO 27001 A.7.7; A.8.1		

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
15	09.03	Política de dispositivo móvel, teletrabalho e trabalho em home office (Nota: Esta Política pode ser implementada como parte da Política de segurança de TI)	ISO 27001 A.6.7; A.7.9; A.8.1		
16	09.04	Política de traga seu próprio dispositivo (BYOD)	ISO 27001 A.5.14; A.6.7; A.8.1		
17	09.05	Procedimetnos para trabalho em áreas seguras	ISO 27001 A.7.4; A.7.6		
18	09.06	Política de classificação da informação	ISO 27001 A.5.9; A.5.10; A.5.12; A.5.13; A.5.14; A.7.10; A.8.3; A.8.5; A.8.11; A.8.12	✔*	
19	09.07	Inventário de ativos	ISO 27001 A.5.9	✔*	
20	09.08	Procedimentos de segurança para o departamento de TI	ISO 27001 A.5.7; A.5.14; A.5.37; A.7.10; A.7.14; A.8.4; A.8.6; A.8.7; A.8.8; A.8.9; A.8.10; A.8.12; A.8.13; A.8.15; A.8.16; A.8.17; A.8.18; A.8.20; A.8.21; A.8.22; A.8.23; A.8.31; A.8.32	✔*	
21	09.09	Política de gestão de mudanças (Nota: Esta Política pode ser implementada como parte dos Procedimentos de segurança para o departamento de TI)	ISO 27001 A.8.32		
22	09.10	Política de cópias de segurança (Nota: Esta Política pode ser implementada como parte dos Procedimentos de segurança para o departamento de TI)	ISO 27001 A.8.13		

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
23	09.11	Política de transferência de informações (Nota: Esta Política pode ser implementada como parte dos Procedimentos de segurança para o departamento de TI)	ISO 27001 A.5.14		
24	09.12	Política de descarte e destruição (Nota: Esta Política pode ser implementada como parte dos Procedimentos de segurança para o departamento de TI)	ISO 27001 A.7.10; A.7.14; A.8.10		
25	09.13	Política para o uso de criptografia	ISO 27001 A.5.31; A.8.24		
26	09.14	Política de controle de acesso	ISO 27001 A.5.15; A.5.16; A.5.17; A.5.18; A.8.2; A.8.3; A.8.4; A.8.5; A.8.11		
27	09.15	Política de senhas (Nota: Esta Política pode ser implementada como parte da Política de controle de acesso)	ISO 27001 A.5.16; A.5.17; A.5.18		
28	09.16	Política de desenvolvimento seguro	ISO 27001 A.5.33; A.8.11; A.8.25; A.8.26; A.8.27; A.8.28; A.8.29; A.8.30; A.8.31; A.8.32; A.8.33	✅*	
29	09.17	Anexo 1 – Especificação dos requisitos do sistema de informação	ISO 27001 A.8.26		
30	09.18	Política de segurança do fornecedor	ISO 27001 A.5.7; A.5.11; A.5.19; A.5.20; A.5.21; A.5.22; A.5.23; A.6.1; A.6.2; A.6.3; A.8.30		

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
31	09.19	Cláusulas de segurança para fornecedores e parceiros	ISO 27001 A.5.20; A.5.21; A.6.2; A.6.6; A.8.30		
32	09.20	Procedimento de gestão de incidentes	ISO 27001 7.4; A.5.7; A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.4; A.6.8	✓*	
33	09.21	Anexo 1 – Registro de incidentes	ISO 27001 A.5.27		
34	09.22	Declaração de confidencialidade	ISO 27001 A.5.20; A.6.2; A.6.5; A.6.6	✓*	
35	09.23	Declaração de aceitação da documentação do SGSI	ISO 27001 A.6.2		
	10	**Documentos principais de continuidade de negócios da ISO 22301**			
36	10.01	Política de continuidade de negócios	ISO 22301 4.1; 4.3; 5.2; 5.3; 6.2; 6.3; 9.1.1 ISO 27001 A.5.29		✓
37	10.02	Metodologia de análise de impacto nos negócios	ISO 22301 8.2.1; 8.2.2 ISO 27001 A.5.29		
38	10.03	Anexo 1 – Questionário de análise de impacto nos negócios	ISO 22301 8.2.1; 8.2.2 ISO 27001 A.5.29		
39	10.04	Estratégia de continuidade de negócios	ISO 22301 8.3; 8.4.2 ISO 27001 A.5.5; A.5.29		
40	10.05	Anexo 1 – Objetivos de tempo de recuperação para atividades	ISO 22301 8.2.2 ISO 27001 A.5.29		

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
41	10.06	Anexo 2 – Exemplos de cenários de incidentes disruptivos	ISO 22301 8.5 ISO 27001 A.5.29		
42	10.07	Anexo 3 – Plano de preparação para a continuidade de negócios	ISO 22301 6.2		
43	10.08	Anexo 4 – Estratégia de recuperação de atividade	ISO 22301 8.3 ISO 27001 A.5.29		
44	10.09	Plano de continuidade de negócios	ISO 22301 8.4 ISO 27001 A.5.29		✔
45	10.10	Anexo 1 – Plano de resposta a incidentes	ISO 22301 8.4.3; 8.4.4 ISO 27001 A.5.5; A.5.26; A.5.29		✔
46	10.11	Anexo 2 – Registro de incidentes	ISO 22301 8.4.3		✔
47	10.12	Anexo 3 – Lista de sites de continuidade de negócios	ISO 22301 8.4.4 ISO 27001 A.5.29		✔
48	10.13	Anexo 4 – Plano de transporte	ISO 22301 8.3.2 ISO 27001 A.5.29		
49	10.14	Anexo 5 – Principais contatos	ISO 22301 8.4.3 ISO 27001 A.5.29		✔
50	10.15	Anexo 6 – Plano de recuperação de desastre	ISO 22301 8.4.5 ISO 27001 7.4; A.5.29; A.5.30; A.8.14	✔*	✔
51	10.16	Anexo 7 – Plano de recuperação de atividade	ISO 22301 8.4.5 ISO 27001 A.5.29		✔

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
52	10.17	Plano de exercícios e testes	ISO 22301 8.5 ISO 27001 A.5.29		
53	10.18	Anexo 1 – Relatório de exercícios e testes	ISO 22301 8.5 ISO 27001 A.5.29		
54	10.19	Plano de revisão e manutenção do SGCN	ISO 22301 8.6 ISO 27001 A.5.29		
55	10.20	Formulário de revisão de pós-incidentes	ISO 22301 8.6 ISO 27001 A.5.27; A.5.29		
	11	**Treinamento e conscientização**			
56	11	Plano de treinamento e conscientização	ISO 27001 7.2; 7.3; 7.4; A.6.3 ISO 22301 7.2; 7.3	✓	✓
	12	**Auditoria interna**			
57	12	Procedimento de auditoria interna	ISO 27001 9.2; A.5.30; A.5.35; A.8.34 ISO 22301 9.2		
58	12.1	Anexo 1 – Programa anual de auditoria interna	ISO 27001 9.2 ISO 22301 9.2	✓	✓
59	12.2	Anexo 2 – Relatório de auditoria interna	ISO 27001 9.2 ISO 22301 9.2	✓	✓
60	12.3	Anexo 3 – Checklist de auditoria interna	ISO 27001 9.2 ISO 22301 9.2		
	13	**Análise crítica pela direção**			

No.	Código do doc.	Nome do documento	Cláusulas relevantes da norma	Obrigatório de acordo com a ISO 27001	Obrigatório de acordo com a ISO 22301
61	13.1	Relatório de medição	ISO 27001 6.2; 9.1 ISO 22301 9.1; 9.3	✓	
62	13.2	Minuta da análise crítica pela direção	ISO 27001 9.3 ISO 22301 9.3	✓	✓
	14	**Ações corretivas**			
63	14	Procedimento de ação corretiva	ISO 27001 10.1; A.5.27 ISO 22301 10.1		
64	14.1	Anexo 1 – Formulário de ação corretiva	ISO 27001 10.1; 10.2 ISO 22301 10.1	✓	✓

* Os documentos listados são obrigatórios somente se os controles correspondentes forem identificados como aplicáveis na Declaração de aplicabilidade.

** As funções e responsabilidades gerais estão descritas na Política de segurança da informação, enquanto as funções e responsabilidades detalhadas são especificadas em cada documento deste Kit de documentação.