

Kit de documentação da ISO 27001

<https://advisera.com/27001academy/pt-br/kit-de-ferramentas-da-documentacao-da-iso-27001/>

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 na ISO 27001	Obrigatório de acordo com a ISO 27001
	01	Gestão de documentos		
1	01	Procedimento de controle de documentos e registros	7.5; A.5.33	
	02	Preparações para o projeto		
2	02	Plano do projeto		
	03	Identificação de requisitos		
3	03	Procedimento para identificação de requisitos	4.2; A.5.31	
4	03.1	Anexo 1 – Lista de obrigações legais, regulamentares, contratuais e outras	4.2; A.5.29; A.5.31	✓ *
	04	Escopo do SGSI		
5	04	Documento sobre o escopo do SGSI	4.3	✓
	05	Políticas gerais		
6	05	Política de segurança da informação	5.2; 5.3**; 6.2; 7.4; A.6.3	✓
	06	Avaliação de riscos e tratamento de riscos		
7	06	Metodologia de avaliação e tratamento de riscos	6.1.2; 6.1.3; 8.2; 8.3	✓
8	06.1	Anexo 1 – Tabela de avaliação de riscos	6.1.2; 8.2	✓
9	06.2	Anexo 2 – Tabela de tratamento de riscos	6.1.3; 8.3	✓
10	06.3	Anexo 3 – Relatório de avaliação e tratamento de riscos	8.2; 8.3	✓

No.	Código do doc.	Nome do documento	Cláusulas relevantes na ISO 27001	Obrigatório de acordo com a ISO 27001
	07	Aplicabilidade de controles		
11	07	Declaração de aplicabilidade	6.1.3 d)	✓
	08	Plano de implementação		
12	08	Plano de tratamento de riscos	6.1.3; 6.2; 7.1; 8.3; 9.1	✓
	09	Anexo A – Controles de segurança		
13	09.01	Política de segurança de TI	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)	A.7.7; A.8.1	
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)	A.6.7; A.7.9; A.8.1	
16	09.04	Política de traga seu próprio dispositivo (BYOD)	A.5.14; A.6.7; A.8.1	
17	09.05	Procedimentos para trabalho em áreas seguras	A.7.4; A.7.6	
18	09.06	Política de classificação da informação	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	A.5.9	✓ *
20	09.08	Procedimentos de segurança para o departamento de TI	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	✓ *

No.	Código do doc.	Nome do documento	Cláusulas relevantes na ISO 27001	Obrigatório de acordo com a ISO 27001
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)	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)	A.8.13	
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)	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)	A.7.10; A.7.14; A.8.10	
25	09.13	Política para o uso de criptografia	A.5.31; A.8.24	
26	09.14	Política de controle de acesso	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)	A.5.16; A.5.17; A.5.18	
28	09.16	Política de desenvolvimento seguro	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	A.8.26	
30	09.18	Política de segurança do fornecedor	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	
31	09.19	Cláusulas de segurança para fornecedores e parceiros	A.5.20; A.5.21; A.6.2; A.6.6; A.8.30	

No.	Código do doc.	Nome do documento	Cláusulas relevantes na ISO 27001	Obrigatório de acordo com a ISO 27001
32	09.20	Procedimento de gestão de incidentes	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	A.5.27	
34	09.22	Plano de recuperação de desastre	7.4; A.5.29; A.5.30; A.8.14	
35	09.23	Declaração de confidencialidade	A.5.20; A.6.2; A.6.5; A.6.6	✓ *
36	09.24	Declaração de aceitação da documentação do SGSI	A.6.2	
	10	Treinamento e conscientização		
37	10	Plano de treinamento e conscientização	7.2; 7.3; 7.4; A.6.3	✓
	11	Auditoria interna		
38	11	Procedimento de auditoria interna	9.2; A.5.30; A.5.35; A.8.34	
39	11.1	Anexo 1 – Programa anual de auditoria interna	9.2	✓
40	11.2	Anexo 2 – Relatório de auditoria interna	9.2	✓
41	11.3	Anexo 3 – Checklist de auditoria interna	9.2	
	12	Análise crítica pela direção		
42	12.1	Relatório de medição	6.2; 9.1	✓
43	12.2	Minuta da análise crítica pela direção	9.3	✓
	13	Ações corretivas		
44	13	Procedimento de ação corretiva	10.1; A.5.27	
45	13.1	Anexo 1 – Formulário de ação corretiva	10.1; 10.2	✓

* 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.