Kit de documentação premium da ISO 27001 e ISO 22301

http://www.iso27001standard.com/pt/produtos/Kit-de-ferramentas-da-documentacao-premium-da-ISO-27001-e-da-BS-25999

Nota: a documentação deve ser implementada preferencialmente na ordem listada neste documento. A ordem da implementação da documentação relacionada ao Anexo A está definida no Plano de tratamento de riscos. A documentação sobre gestão de continuidade de negócios (item 8 A.17 do pacote) é implementada na ordem listada neste documento.

Número no pacote	***Nome do documento***	***Cláusulas relevantes da norma***	***O documento é obrigatório de acordo com a ISO 27001***	***O documento é obrigatório de acordo com a ISO 22301***	***O documento é obrigatório de acordo com a BS 25999-2***
0.	Procedimento de documentação e controle de registros	ISO/IEC 27001 7.5 ISO 22301 7.5 BS 25999-2 3.4.2, 3.4.3	✓		✓
1.	Plano do projeto				
2.	Procedimento para identificação de requisitos	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2			
2.1	Lista de obrigações legais, regulamentares, contratuais e outras	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2	✓*	✓	
3.	Documento sobre o escopo do SGSI	ISO/IEC 27001 4.3	✓		
4.	Política da segurança da informação	ISO/IEC 27001 5.2, 5.3	✓		
5.	Metodologia de avaliação e tratamento de riscos	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3BS 25999-2 4.1.2.1	✓		✓
5.1.	Anexo 1 - Tabela de avaliação de riscos	ISO/IEC 27001 6.1.2, 8.2 BS 25999-2 4.1.2	✓		

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
5.2.	Anexo 2 - Tabela de tratamento de riscos	ISO/IEC 27001 6.1.3, 8.3 BS 25999-2 4.1.3.1	✓		
5.3.	Anexo 3 - Relatório de avaliação de riscos	ISO/IEC 27001 8.2, 8.3	✓		
6.	Declaração de aplicabilidade	ISO/IEC 27001 6.1.3 d)	✓		
7.	Plano de tratamento de riscos	ISO/IEC 27001 6.1.3, 6.2, 8.3 BS 25999-2 4.1.3.2	✓		
8.	(Anexo A - controles)				
8. A.6	Política de traga seu próprio dispositivo (BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1			
8. A.6	Política de dispositivo móvel e trabalho remoto	ISO/IEC 27001 A.6.2 A.11.2.6			
8. A.7	Declaracao de confidencialidade	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*		
8. A.7	Declaração de aceitação da Documentação do Sistema de gestão da segurança da informação	ISO/IEC 27001 A.7.1.2	✓*		
8. A.8	Inventário de ativos	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*		

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.8	Política de uso aceitável	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2	✓*		
8. A.8	Política de classificação da informação	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3			
8. A.9	Política de controle de acesso	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3	✓*		
8. A.9	Política de senhas (Nota: pode ser implementado como parte da Política de controle de acesso)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3			
8. A.10	Política para o uso de controles criptográficos	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5			

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.11	Política de mesa limpa e tela limpa (Nota: pode ser implementado como parte da Política de uso aceitável)	ISO/IEC 27001 A.11.2.8, A.11.2.9			
8. A.11	Política de descarte e destruição (Nota: pode ser implementado como parte da Procedimentos operacionais para a TI)	ISO/IEC 27001 A.8.3.2, A.11.2.7			
8. A.11	Procedimentos para trabalho em áreas seguras	ISO/IEC 27001 A.11.1.5			
8. A.12	Procedimentos operacionais para a tecnologia da informação e comunicação	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4	✓*		
8. A.12	Política de gestão de mudanças (Nota: pode ser implementado como parte da Procedimentos operacionais para a TI)	ISO/IEC 27001 A.12.1.2, A.14.2.4			

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.12	Política de cópias de segurança (Nota: pode ser implementado como parte da Procedimentos operacionais para a TI)	ISO/IEC 27001 A.12.3.1			
8. A.13	Política de trânsfencia de informações (Nota: pode ser implementado como parte da Procedimentos operacionais para a TI)	ISO/IEC 27001 A.13.2.1, A.13.2.2			
8. A.14	Política de desenvolvimento seguro	ISO/IEC A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	✓*		
8. A.14.1	Especificação dos requisitos do sistema de informação	ISO/IEC 27001 A.14.1.1	✓*		
8. A.15	Política de segurança do fornecedor	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2			

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.15.1	Cláusulas de segurança para fornecedores e parceiros	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*		
8. A.16	Procedimento de gestão de incidentes	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	✓*		
8. A.16.1	Anexo - Registro de incidentes	ISO/IEC 27001 A.16.1.6			
8. A.17 1.	Política de continuidade de negócios	ISO 22301 4.1, 4.3, 5.3, 6.2, 9.1.1 BS 25999-2 3.2.1, 3.2.2, 3.2.3 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 2.	Metodologia de análise de impacto nos negócios	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 2.1.	Questionário de análise de impacto nos negócios	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.	Estratégia de continuidade de negócios	ISO 22301 8.3, 8.4.2 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8.	Anexo 1 - Lista de	ISO 22301 8.2.2		✓	✓

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
A.17 3.1.	atividades	BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1			
8. A.17 3.2.	Anexo 2 - Prioridades de recuperação das atividades	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.3.	Anexo 3 - Objetivos de tempo de recuperação para atividades	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.4.	Anexo 4 - Exemplos de cenários de incidentes disruptivos	ISO 22301 8.5 BS 25999-2 4.1.2.2 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 3.5.	Anexo 5 - Plano de preparação para a continuidade de negócios	ISO 22301 6.2 BS 25999-2 3.2.3.1		✓	✓
8. A.17 3.6.	Anexo 6 - Estratégia de recuperação de atividade	ISO 22301 8.3 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8. A.17 4.	Plano de continuidade de negócios	ISO 22301 8.4 BS 25999-2 4.3 ISO/IEC 27001 A.17.1.2	✓	✓	✓
8. A.17 4.1.	Anexo 1 - Plano de resposta a incidentes	ISO 22301 8.4.3, 8.4.4 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.2	✓	✓	✓

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.17 4.2.	Anexo 2 - Registro de incidentes	ISO 22301 8.4.3 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 4.3.	Anexo 3 - Lista de sites de continuidade de negócios	ISO 22301 8.4.4 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.4.	Anexo 4 - Plano de transporte	ISO 22301 8.3.2 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.5.	Anexo 5 - Principais contatos	ISO 22301 8.4.3 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.6.	Anexo 6 - Plano de recuperação de atividade	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2	✓	✓	✓
8. A.17 5.1.	Plano de exercícios e testes	ISO 22301 8.5 BS 25999-2 4.4.2 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.2.	Anexo - Formulário - Relatório de exercício e testes	ISO 22301 8.5 BS 25999-2 4.4.2.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 5.3.	Plano de revisão e manutenção do SGCN	ISO 22301 9.1.2 BS 25999-2 4.4.3 ISO/IEC 27001 A.17.1.3			✓

Número no pacote	*Nome do documento*	*Cláusulas relevantes da norma*	*O documento é obrigatório de acordo com a ISO 27001*	*O documento é obrigatório de acordo com a ISO 22301*	*O documento é obrigatório de acordo com a BS 25999-2*
8. A.17 5.4.	Formulário de revisão de pós-incidentes	ISO 22301 9.1.2 BS 25999-2 4.4.3.4 ISO/IEC 27001 A.17.1.3, A.16.1.6		✓	✓
9.	Plano de treinamento e conscientização	ISO 22301 7.2, 7.3 BS 25999-2 3.2.4, 3.3 ISO/IEC 27001 7.2, 7.3	✓	✓	✓
10.	Procedimento de auditoria interna	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1			✓
10.1.	Anexo 1 - Programa de auditoria interna anual	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.2.	Anexo 2 - Relatório de auditoria interna	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.3.	Anexo 3 – Checklist de Auditoria Interna para o ISO 27001 e ISO 22301	ISO/IEC 27001 9.2 ISO 22301 9.2			
11.	Minutas de revisão da gestão	ISO/IEC 27001 9.3 ISO 22301 9.3 BS 25999-2 5.2	✓	✓	✓
12.	Procedimento para ações corretivas	ISO/IEC 27001 10.1 ISO 22301 10.1 BS 25999-2 6.1			✓
12.1.	Anexo - Formulário de ação corretiva	ISO/IEC 27001 10.1 ISO 22301 10.1 BS 25999-2 6.1	✓	✓	✓

*Os documentos listados são obrigatórios somente se os controles correspondentes estiverem identificados conforme aplicável na Declaração de aplicabilidade

Para aprender como completar estes documentos, consulte:

1) Tutoriais em vídeo http://www.iso27001standard.com/tutoriais-em-video
2) Webinars http://www.iso27001standard.com/webinars