Paquete de documentos sobre ISO 27001

https://advisera.com/27001academy/es/paquete-de-documentos-sobre-iso-27001/

Nota: Se recomienda implementar los documentos en el orden detallado aquí. El orden de implementación de los documentos relacionados con el Anexo A está definido en el Plan de tratamiento del riesgo.

No.	*Código del documento*	*Nombre del documento*	*Cláusulas relevantes de la norma*	*Obligatorio según ISO 27001*
	00	**Gestión de documentos**		
1	00	Procedimiento para el control de documentos y registros	ISO/IEC 27001 7.5	
	01	**Preparaciones para el proyecto**		
2	01	Plan de proyecto		
	02	**Identificación de requisitos**		
3	02	Procedimiento para la identificación de requisitos	ISO/IEC 27001 4.2, A.18.1.1	
4	02.1	Apéndice 1 – Lista de requisitos legales, normativos, contractuales y de otra índole	ISO/IEC 27001 4.2, A.18.1.1	✓*
	03	**Alcance del SGSI**		
5	03	Documento sobre el alcance del SGSI	ISO/IEC 27001 4.3	✓
	04	**Políticas generales**		
6	04	Política de seguridad de la información	ISO/IEC 27001 5.2, 5.3	✓
	05	**Evaluación de riesgos y tratamiento de riesgos**		
7	05	Metodología de evaluación y tratamiento de riesgos	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3	✓
8	05.1	Apéndice 1 – Cuadro de evaluación de riesgos	ISO/IEC 27001 6.1.2, 8.2	✓
9	05.2	Apéndice 2 – Cuadro de tratamiento de riesgos	ISO/IEC 27001 6.1.3, 8.3	✓
10	05.3	Apéndice 3 – Informe sobre la evaluación y tratamiento de riesgos	ISO/IEC 27001 8.2, 8.3	✓
	06	**Aplicabilidad de controles**		
11	06	Declaración de aplicabilidad	ISO/IEC 27001 6.1.3 d)	✓

No.	Código del documento	Nombre del documento	Cláusulas relevantes de la norma	Obligatorio según ISO 27001
	07	**Plan de implementación**		
12	07	Plan de tratamiento del riesgo	ISO/IEC 27001 6.1.3, 6.2, 8.3	✓
	08	**Anexo A: Controles de Seguridad****		
	A.6	**Organización de la seguridad de la información**		
13	A.6.1	Política trae tu propio dispositivo (BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1	
14	A.6.2	Política sobre dispositivos móviles y tele-trabajo	ISO/IEC 27001 A.6.2 A.11.2.6	
	A.7	**Seguridad relacionada con el personal**		
15	A.7.1	Declaración de confidencialidad	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*
16	A.7.2	Declaración de aceptación de los documentos del SGSI	ISO/IEC 27001 A.7.1.2	✓*
	A.8	**Gestión de activos**		
17	A.8.1	Inventario de activos	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*
18	A.8.2	Política de seguridad de TI	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	✓*
19	A.8.3	Política de clasificación de la información	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	
	A.9	**Control de acceso**		

No.	Código del documento	Nombre del documento	Cláusulas relevantes de la norma	Obligatorio según ISO 27001
20	A.9.1	Política de control de acceso	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	✓*
21	A.9.2	Política de claves (Aviso: puede ser implementada como parte de la Política de control de acceso)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3	
	A.10	**Criptografía**		
22	A.10	Política del uso del encriptado	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5	
	A.11	**Seguridad física y ambiental**		
23	A.11.1	Política de pantalla y escritorio limpios (Aviso: puede ser implementado como parte de la Política de seguridad de TI)	ISO/IEC 27001 A.11.2.8, A.11.2.9	
24	A.11.2	Política de eliminación y destrucción (Aviso: puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI)	ISO/IEC 27001 A.8.3.2, A.11.2.7	
25	A.11.3	Procedimientos para trabajo en áreas seguras	ISO/IEC 27001 A.11.1.5	
	A.12	**Seguridad operativa**		
26	A.12.1	Procedimientos de seguridad para el departamento de TI	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	✓*
27	A.12.2	Política de gestión de cambio (Aviso: puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI)	ISO/IEC 27001 A.12.1.2, A.14.2.4	

No.	Código del documento	Nombre del documento	Cláusulas relevantes de la norma	Obligatorio según ISO 27001
28	A.12.3	Política de creación de copias de seguridad (Aviso: puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI)	ISO/IEC 27001 A.12.3.1	
	A.13	**Seguridad de las comunicaciones**		
29	A.13	Política de transferencia de la información (Aviso: puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI)	ISO/IEC 27001 A.13.2.1, A.13.2.2	
	A.14	**Adquisición de sistemas de desarrollo y mantenimiento**		
30	A.14	Política de desarrollo 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	✓*
31	A.14.1	Apéndice 1 – Especificaciones de requisitos del sistema de información	ISO/IEC 27001 A.14.1.1	✓*
	A.15	**Relaciones con proveedores**		
32	A.15.1	Política de seguridad para proveedores	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	✓*
33	A.15.2	Cláusulas de seguridad para proveedores y socios	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*
	A.16	**Gestión de los incidentes de seguridad de la información**		
34	A.16	Procedimiento para gestión 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	✓*

No.	Código del documento	Nombre del documento	Cláusulas relevantes de la norma	Obligatorio según ISO 27001
35	A.16.1	Apéndice 1 – Registro de incidentes	ISO/IEC 27001 A.16.1.6	
	A.17	**Continuidad de negocio**		
36	A.17	Apéndice 6 – Plan de recuperación ante desastres	ISO/IEC 27001 A.17.1.2	✓*
	09	**Formación y concienciación**		
37	09	Plan de formación y concienciación	ISO/IEC 27001 7.2, 7.3	✓
	10	**Auditoría interna**		
38	10	Procedimiento para auditoría interna	ISO/IEC 27001 9.2	
39	10.1	Apéndice 1 – Programa anual de auditoría interna	ISO/IEC 27001 9.2	✓
40	10.2	Apéndice 2 – Informe de auditoría interna	ISO/IEC 27001 9.2	✓
41	10.3	Apéndice 3 – Lista de verificación de auditoría interna	ISO/IEC 27001 9.2	
	11	**Revisión por la dirección**		
42	11.1	Informe de medición	ISO/IEC 27001 6.2, 9.1	✓
43	11.2	Actas de revisión por la dirección	ISO/IEC 27001 9.3	✓
	12	**Acciones correctivas**		
44	12	Procedimiento para acciones correctivas	ISO/IEC 27001 10.1	
45	12.1	Apéndice 1 – Formulario para acciones correctivas	ISO/IEC 27001 10.1	✓

*Los documentos detallados solamente son obligatorios si los controles correspondientes están señalados como aplicables en la Declaración de aplicabilidad.

**La carpeta “Anexo A” no incluye una carpeta separada para la sección “A.18 - Cumplimiento” de la Norma ISO 27001 porque la documentación que cubre los controles de esta sección se puede encontrar en estas carpetas:

- 02 – Identificación de requisitos
- 08, A.8 – Gestión de activos
- 08, A.10 – Criptografía