




## Paquete de documentos sobre ISO 27001

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

Nota: La documentación debe implementarse preferiblemente en el orden en que se enumera aquí. El orden de implementación de la documentación relacionada con el Anexo A se define en el Plan de tratamiento de riesgos.

No.	Código de documento	Nombre del documento	Cláusulas relevantes en ISO 27001	Obligatorio según ISO 27001
	<b>01</b>	<b>Gestión de documentos</b>		
1	01	Procedimiento para el control de documentos y registros	7.5; A.5.33	
	<b>02</b>	<b>Preparaciones para el proyecto</b>		
2	02	Plan de proyecto		
	<b>03</b>	<b>Identificación de requisitos</b>		
3	03	Procedimiento para la identificación de requisitos	4.2; A.5.31	
4	03.1	Apéndice 1 – Lista de requisitos legales, normativos, contractuales y de otra índole	4.2; A.5.29; A.5.31	✓ *
	<b>04</b>	<b>Alcance del SGSI</b>		
5	04	Documento de alcance del SGSI	4.3	✓
	<b>05</b>	<b>Políticas generales</b>		
6	05	Política de seguridad de la información	5.2; 5.3*; 6.2; 7.4; A.6.3	✓
	<b>06</b>	<b>Evaluación y tratamiento de riesgos</b>		
7	06	Metodología de evaluación y tratamiento de riesgos	6.1.2; 6.1.3; 8.2; 8.3	✓
8	06.1	Apéndice 1 – Cuadro de evaluación de riesgos	6.1.2; 8.2	✓
9	06.2	Apéndice 2 – Cuadro de tratamiento de riesgos	6.1.3; 8.3	✓

No.	Código de documento	Nombre del documento	Cláusulas relevantes en ISO 27001	Obligatorio según ISO 27001
10	06.3	Apéndice 3 – Informe sobre la evaluación y tratamiento de riesgos	8.2; 8.3	✓
	<b>07</b>	<b>Aplicabilidad de los controles</b>		
11	07	Declaración de aplicabilidad	6.1.3 d)	✓
	<b>08</b>	<b>Plan de Implementación</b>		
12	08	Plan de tratamiento de riesgos	6.1.3; 6.2; 7.1; 8.3; 9.1	✓
	<b>09</b>	<b>Anexo A – Controles de seguridad</b>		
13	09.01	Política de seguridad 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 escritorio y pantalla limpios (Nota: Esto se puede implementar como parte de la Política de seguridad de TI.)	A.7.7; A.8.1	
15	09.03	Política sobre dispositivos móviles, tele-trabajo y trabajo desde casa (Nota: Esto se puede implementar como parte de la Política de seguridad de TI.)	A.6.7; A.7.9; A.8.1	
16	09.04	Política Trae tu propio dispositivo (BYOD)	A.5.14; A.6.7; A.8.1	
17	09.05	Procedimientos para trabajo en áreas seguras	A.7.4; A.7.6	

No.	Código de documento	Nombre del documento	Cláusulas relevantes en ISO 27001	Obligatorio según ISO 27001
18	09.06	Política de clasificación de la información	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	Inventario de activos	A.5.9	 *
20	09.08	Procedimientos de seguridad para el 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	 *
21	09.09	Política de gestión de cambios (Nota: Puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI.)	A.8.32	
22	09.10	Política de copias de seguridad (Nota: Puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI.)	A.8.13	
23	09.11	Política de transferencia de información (Nota: Puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI.)	A.5.14	

No.	Código de documento	Nombre del documento	Cláusulas relevantes en ISO 27001	Obligatorio según ISO 27001
24	09.12	Política de eliminación y destrucción (Nota: Puede ser implementado como parte de los Procedimientos de seguridad para el departamento de TI.)	A.7.10; A.7.14; A.8.10	
25	09.13	Política del uso del encriptado	A.5.31; A.8.24	
26	09.14	Política de control de acceso	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 claves (Nota: Puede ser implementado como parte de la Política de control de acceso.)	A.5.16; A.5.17; A.5.18	
28	09.16	Política de desarrollo 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	Apéndice 1 – Especificación de los requisitos del sistema de información	A.8.26	
30	09.18	Política de seguridad para proveedores	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 seguridad para proveedores y socios	A.5.20; A.5.21; A.6.2; A.6.6; A.8.30	
32	09.20	Procedimiento para gestión 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	✓ *

No.	Código de documento	Nombre del documento	Cláusulas relevantes en ISO 27001	Obligatorio según ISO 27001
33	09.21	Apéndice 1 – Registro de incidentes	A.5.27	
34	09.22	Plan de recuperación ante desastres	7.4; A.5.29; A.5.30; A.8.14	
35	09.23	Declaración de confidencialidad	A.5.20; A.6.2; A.6.5; A.6.6	✓*
36	09.24	Declaración de aceptación de los documentos del SGSI	A.6.2	
	<b>10</b>	<b>Formación y concientización</b>		
37	10	Plan de formación y concienciación	7.2; 7.3; 7.4; A.6.3	✓
	<b>11</b>	<b>Auditoría interna</b>		
38	11	Procedimiento para auditoría interna	9.2; A.5.30; A.5.35; A.8.34	
39	11.1	Apéndice 1 – Programa anual de auditoría interna	9.2	✓
40	11.2	Apéndice 2 – Informe de auditoría interna	9.2	✓
41	11.3	Apéndice 3 Lista de verificación de auditoría interna	9.2	
	<b>12</b>	<b>Revisión por la dirección</b>		
42	12.1	Informe de medición	6.2; 9.1	✓
43	12.2	Actas de revisión por la dirección	9.3	✓
	<b>13</b>	<b>Acciones correctivas</b>		
44	13	Procedimiento para la acción correctiva	10.1; A.5.27	
45	13.1	Apéndice 1 – Formulario de acción correctiva	10.1; 10.2	✓

\* Los documentos enumerados son obligatorios solo si los controles correspondientes se identifican como aplicables en la Declaración de aplicabilidad.

\*\* Las roles y responsabilidades generales se describen en la Política de seguridad de la información, mientras que las roles y responsabilidades detalladas se especifican en cada documento de este Paquete de Documentos.