\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete ISO 27001/ISO 22301 Evaluación de riesgos.

[logo de la organización]

[nombre de la organización]

**DECLARACIÓN DE APLICABILIDAD**

|  |  |
| --- | --- |
| Código: |  |
| Versión: |  |
| Fecha de la versión: |  |
| Creado por: |  |
| Aprobado por: |  |
| Nivel de confidencialidad: |  |

**Historial de cambios**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción del cambio** |
|  | 0.1 | Advisera | Esquema básico del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Tabla de contenido**

[1. Objetivo, alcance y usuarios 3](#_Toc131425462)

[2. Documentos de referencia 3](#_Toc131425463)

[3. Aplicabilidad de los controles 3](#_Toc131425464)

[4. Aceptación de riesgos residuales 19](#_Toc131425465)

[5. Validez y gestión de documentos 19](#_Toc131425466)

# Objetivo, alcance y usuarios

El propósito de este documento es definir qué controles son apropiados para implementar en [nombre de la organización], los objetivos de estos controles y cómo se implementan, así como aprobar los riesgos residuales y aprobar formalmente la implementación de dichos controles.

Este documento incluye todos los controles enumerados en el Anexo A de la norma ISO 27001. Los controles son aplicables a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son todos los empleados de [nombre de la organización] que tienen un rol en el SGSI.

# Documentos de referencia

* Norma ISO/IEC 27001, cláusula 6.1.3 d)
* Política de seguridad de la información
* Metodología de evaluación y tratamiento de riesgos
* Informe sobre la evaluación y tratamiento de riesgos

# Aplicabilidad de los controles

Los siguientes controles del Anexo A de ISO 27001 son aplicables:

| ID | Controles según la norma ISO/IEC 27001 | Aplicabilidad (SI/NO) | Justificación para selección/ no selección | … | … | … |
| --- | --- | --- | --- | --- | --- | --- |
| A.5.1 | Políticas para seguridad de la información |  |  |  | Todas las políticas a las que se hace referencia a continuación en esta columna; cada póliza tiene un propietario designado que tiene que revisar el documento a intervalos planificados. |  |
| A.5.2 | Roles y responsabilidades sobre seguridad de la información |  |  |  | Los roles y responsabilidades para la seguridad de la información se enumeran en varios documentos del SGSI. Si es necesario, el [cargo] define roles y responsabilidades adicionales |  |
| A.5.3 | Segregación de deberes |  |  |  | Cualquier actividad que incluya información confidencial es aprobada por una persona e implementada por otra |  |
| A.5.4 | Responsabilidades de la dirección |  |  |  | La dirección requiere activamente que todos los empleados, proveedores y socios externos implementen todas las reglas del SGSI. |  |
| A.5.5 | Contacto con autoridades |  |  |  | El [cargo] es responsable del contacto con las autoridades correspondientes (por ejemplo, policía, bomberos, etc.)  [Estrategia de continuidad de negocio], [Plan de respuesta a los incidentes] |  |
| A.5.6 | Contacto con grupos de interés especial |  |  |  | El [cargo] es responsable de monitorear [enumere los nombres de los grupos de interés y los foros de seguridad] |  |
| A.5.7 | Inteligencia sobre amenazas |  |  |  | [Política de seguridad para proveedores], [Procedimiento para gestión de incidentes], [Procedimientos de seguridad para el departamento de TI] |  |
| A.5.8 | Seguridad de la información en la gestión de proyectos |  |  |  | El gerente del proyecto debe incluir las reglas de seguridad de la información aplicables en cada proyecto; al adquirir nuevos sistemas de información o cambiar los existentes, el [cargo] debe documentar los requisitos de seguridad en la [Especificación de requisitos de seguridad] |  |
| A.5.9 | Inventario de información y otros activos asociados |  |  |  | [Inventario de activos], [Política de clasificación de la información], [Política de seguridad de TI] |  |

…

\*\* FIN DE MUESTRA GRATIS \*\*

Si ha decidido que el Paquete ISO 27001/ISO 22301 Evaluación de riesgos es la mejor elección para su compañía, consulte la siguiente tabla para elegir el paquete de documentos con el nivel de soporte experto adecuado.

|  |  |  |
| --- | --- | --- |
|  | **Paquete de documentos con apoyo de un experto** | **Paquete de documentos con ampliación de soporte** |
|  | **US $397** | **US $897** |
| **6 plantillas de documentos que cumplen con ISO 27001 & ISO 22301** | **🗸** | **🗸** |
| **Acceso a tutoriales en video (en inglés)** | **🗸** | **🗸** |
| **Soporte mediante correo electrónico** | 10 preguntas por mes | Ilimitado |
| **Asistencia personalizada con un experto en ISO 27001/ISO 22301** | 1 hora | 5 horas |
| **Revisión de expertos (documentos completos)** | 1 documento | 5 documentos |
| **Revisión previa a la auditoría** | **X** | **🗸** |
|  | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718224&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-22301-risk-assessment-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718225&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-22301-risk-assessment-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | |