\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete Premium de documentos sobre ISO 27001 e ISO 22301.

[logo de la organización]

[nombre de la organización]

**METODOLOGÍA DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS**

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

**Historial de modificaciones**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Creado por** | **Descripción de la modificación** |
|  | 0.1 | Advisera | Descripción básica del documento |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Tabla de contenido**

[1. Objetivo, alcance y usuarios 3](#_Toc130372983)

[2. Documentos de referencia 3](#_Toc130372984)

[3. Metodología de evaluación y tratamiento de riesgos 3](#_Toc130372985)

[3.1. Evaluación de riesgos 3](#_Toc130372986)

[3.1.1. El proceso 3](#_Toc130372987)

[3.1.2. Activos, vulnerabilidades y amenazas 3](#_Toc130372988)

[3.1.3. Identificación de los propietarios de riesgos 4](#_Toc130372989)

[3.1.4. Consecuencias y probabilidad 4](#_Toc130372990)

[3.2. Criterios para la aceptación de riesgos 5](#_Toc130372991)

[3.3. Tratamiento del riesgo 5](#_Toc130372992)

[3.4. Revisiones periódicas de la evaluación y el tratamiento de riesgos 5](#_Toc130372993)

[3.5. Declaración de aplicabilidad y Plan de tratamiento del riesgo 5](#_Toc130372994)

[3.6. Informes 6](#_Toc130372995)

[4. Gestión de registros guardados en base a este documento 6](#_Toc130372996)

[5. Validez y gestión de documentos 7](#_Toc130372997)

[6. Apéndices 7](#_Toc130372998)

# Objetivo, alcance y usuarios

El objetivo del presente documento es definir la metodología para evaluar y tratar los riesgos de la información en [nombre de la organización] y definir el nivel aceptable de riesgo según la norma ISO/IEC 27001.

La evaluación y tratamiento de riesgos se aplican a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización] que participan en la evaluación y tratamiento de riesgos.

# Documentos de referencia

* Norma ISO/IEC 27001, cláusulas 6.1.2, 6.1.3, 8.2, y 8.3
* Norma ISO 22301, cláusulas 8.1.2 y 8.2.3
* Política de seguridad de la información
* Lista de requisitos legales, normativos, contractuales y de otra índole
* Política de seguridad para proveedores
* Declaración de aplicabilidad

# Metodología de evaluación y tratamiento de riesgos

## Evaluación de riesgos

### El proceso

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. El proceso de evaluación de riesgos es coordinado por [cargo]. La identificación de amenazas y vulnerabilidades la realizan los propietarios de los activos, y la evaluación de consecuencias y probabilidad es realizada por los propietarios de los riesgos. El [cargo] es responsable de incluir los datos sobre amenazas, vulnerabilidades, consecuencias y probabilidad en el Cuadro de evaluación de riesgos.

### Activos, vulnerabilidades y amenazas

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del SGSI por los representantes de cada área en el alcance del SGSI; es decir, identificar todos los activos que pueden interrumpir las operaciones. Los activos pueden ser documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados. Al identificar los activos también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo.

El siguiente paso es que los propietarios de los activos identifiquen todas las amenazas y vulnerabilidades relacionadas con cada activo. Las amenazas y vulnerabilidades se identifican utilizando los catálogos incluidos en el Cuadro de evaluación de riesgos. Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

### Identificación de los propietarios de riesgos

Para cada riesgo es necesario identificar un propietario: la persona o unidad organizativa responsable de cada riesgo. Esta persona puede o no ser la misma que el propietario del activo.

### Consecuencias y probabilidad

Una vez que se han identificado los riesgos, es necesario evaluar las consecuencias para cada combinación de amenazas y vulnerabilidades de un activo específico en caso que ello se pueda producir:

|  |  |  |
| --- | --- | --- |
| Baja consecuencia | 0 | … |
| Consecuencia moderada | 1 | … |
| Alta consecuencia | 2 | … |

Luego de la evaluación de consecuencias es necesario evaluar la probabilidad de que se materialice ese riesgo; es decir, la probabilidad de que una amenaza se aproveche de la vulnerabilidad del activo en cuestión.

…

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

Si ha decidido que el Paquete Premium de documentos sobre ISO 27001 e ISO 22301 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** | **Paquete de documentos superior** |
|  | **US $997** | **US $1497** | **US $2497** |
| **64 plantillas de documentos que cumplen con ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Acceso a tutoriales en video (en inglés)** | **🗸** | **🗸** | **🗸** |
| **Plantillas de documentos actualizadas a la versión ISO 27001:2022** | **🗸** | **🗸** | **🗸** |
| **Herramienta de Análisis de Brecha en ISO 27001** | **🗸** | **🗸** | **🗸** |
| **Soporte mediante correo electrónico** | 10 preguntas por mes | Ilimitado | Ilimitado |
| **Asistencia personalizada con un experto en ISO 27001 e ISO 22301** | 1 hora | 5 horas | 15 horas |
| **Revisión de expertos (documentos completos)** | 1 documento | 5 documentos | 15 documentos |
| **Formación en concienciación sobre seguridad (en inglés)** | **X** | 20 usuarios | 50 usuarios |
| **Revisión previa a la auditoría** | **X** | **🗸** | **🗸** |
|  | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718233&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718234&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-extended-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718235&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-iso-22301-templates&utm_term=toolkit-with-power-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | | |