\*\* VERSIÓN DE MUESTRA GRATIS \*\*

Gracias por descargar la vista previa gratuita del Paquete de documentos de ISO 27001.

[logo de la organización]

[nombre de la organización]

**PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES**

|  |  |
| --- | --- |
| 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](#_Toc129592229)

[2. Documentos de referencia 3](#_Toc129592230)

[3. Gestión de incidentes 3](#_Toc129592231)

[3.1. Recepción y clasificación de incidentes, debilidades y eventos 3](#_Toc129592232)

[3.2. Proceso de tratamiento para debilidades o eventos de seguridad 4](#_Toc129592233)

[3.3. Tratamiento de incidentes menores 4](#_Toc129592234)

[3.4. Tratamiento de incidentes graves 4](#_Toc129592235)

[3.5. Aprendizaje a partir de los incidentes 4](#_Toc129592236)

[3.6. Acciones disciplinarias 4](#_Toc129592237)

[3.7. Recolección de evidencia 4](#_Toc129592238)

[4. Gestión de registros guardados en base a este documento 5](#_Toc129592239)

[5. Validez y gestión de documentos 5](#_Toc129592240)

[6. Apéndices 5](#_Toc129592241)

# Objetivo, alcance y usuarios

El objetivo del presente documento es garantizar la detección temprana de eventos y debilidades de seguridad, como también la rápida reacción y respuesta ante incidentes de seguridad.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los empleados y demás activos que se utilizan dentro del alcance del SGSI, como también a los proveedores y demás personas externas a la organización que entran en contacto con los sistemas y con la información alcanzados por el SGSI.

Los usuarios de este documento son todos los empleados de [nombre de la organización], como también todas las personas mencionadas precedentemente.

# Documentos de referencia

* Norma ISO/IEC 27001, cláusulas 7.4, A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4 y A.6.8
* Política de seguridad de la información
* [Lista de requisitos legales, normativos, contractuales y de otra índole]

# Gestión de incidentes

Un incidente de seguridad de la información es un "evento, o serie de eventos, indeseado e inesperado que tiene una alta probabilidad de poner en riesgo las actividades comerciales y de amenazar la seguridad de la información" (ISO/IEC 27000:2018).

## Recepción y clasificación de incidentes, debilidades y eventos

Cada empleado, proveedor o tercero que esté en contacto con información, sistemas, o áreas sensibles de [nombre de la organización] debe reportar de la siguiente manera toda amenaza, debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente:

1. Toda la información y los eventos relacionados con tecnología de la comunicación deben ser reportados al [cargo].
2. Todos los demás eventos deben ser reportados al [cargo].

Los incidentes, amenazas, debilidades y eventos deben ser reportados lo antes posible por teléfono o en persona.

La persona que recibe la información debe clasificarla de la siguiente manera:

1. Amenaza, debilidad de seguridad o evento: no se produjo un incidente, pero el evento relacionado a un sistema, proceso u organización podría generar un incidente en el corto o mediano plazo.
2. Incidente menor: un incidente que no puede tener consecuencias significativas sobre la confidencialidad o integridad de la información, y que no puede producir una indisponibilidad prolongada.

…

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

Si ha decidido que el Paquete de documentos de ISO 27001 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 $897** | **US $1397** | **US $2397** |
| **45 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** | 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=4718229&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-expert-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718230&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-extended-support&utm_content=lang-es) | [**SOLICÍTELO AHORA**](https://shop.advisera.com/order/checkout.php?PRODS=4718232&QTY=1&CART=1&CARD=1&SHORT_FORM=1&LANG=es?utm_source=toolkit-document-preview&utm_medium=downloaded-content&utm_campaign=iso-27001-templates&utm_term=toolkit-with-power-support&utm_content=lang-es) |
|  | (haga clic en el siguiente enlace presionando CTRL+clic) | | |