[logo de la organización]

[nombre de la organización]

Commented [AES1]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES

Commented [AES2]: Para obtener más información sobre este tema, lea este artículo:

How to handle incidents according to ISO 27001
https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/

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

Commented [AES3]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

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

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.

Commented [AES4]: Incluya el nombre de su organización.

2. 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]

Commented [AES5]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "05_Politicas_generales".

Commented [AES6]: Si no tiene esta Lista, entonces aquí detalle la legislación y contratos que contengan requerimientos relacionados con gestión de incidentes.

3. Gestión de incidentes

Un incidente de seguridad de la información es un [illegible]

3.1. 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:

Commented [AES7]: Incluya el nombre de su organización.

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

Commented [AES8]: Incluya el cargo de la persona asignada

Commented [AES9]: Incluya el cargo de la persona asignada

Los incidentes, amenazas, debilidades y eventos deben ser reportados lo antes posible [illegible]

Commented [AES10]: Se pueden agregar otros sistemas que

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

a) 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.

b) 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.
c) Incidente grave: un incidente que puede producir un daño significativo debido a la pérdida de confidencialidad o integridad de la información, o que puede producir una interrupción en la disponibilidad de la información y/o de los procesos durante un período de tiempo no aceptable.

3.2. Proceso de tratamiento para debilidades o eventos de seguridad

La persona que recibió la información sobre una amenaza, debilidad o evento la analiza, establece el origen y, si es necesario, sugiere acciones correctivas.

3.3. Tratamiento de incidentes menores

Si se reporta un incidente menor, la persona que recibió la información debe seguir los siguientes pasos:

1. Tomar acciones para controlar el incidente.
2. Analizar el origen del incidente.
3. Tomar acciones correctivas para eliminar la causa del incidente.
4. Informar a las personas que estuvieron involucradas en el incidente, como también al [cargo] sobre el proceso de tratamiento del incidente.

La persona que recibió información sobre un incidente menor debe crear un registro del incidente (detallar la forma de grabación).

Commented [AES11]: Por ejemplo, manual, electrónica o

3.4. Tratamiento de incidentes graves

En el caso de incidentes graves que puedan interrumpir las actividades durante un período de tiempo no aceptable, se aplicará el [Plan de recuperación ante desastres].

Commented [AES12]: Si implementó la continuidad de negocio

3.5. Aprendizaje a partir de los incidentes

Commented [AES13]: Eliminar este punto si el control A.5.27

El [cargo] debe revisar todos los incidentes menores cada tres meses y debe ingresar los que sean recurrentes, o aquellos que se pueden transformar en incidentes graves la próxima vez, en el Registro de incidentes.

El [cargo] debe analizar cada tipo de incidente registrado en el Registro de incidentes (identificando el tipo, relevancia y costo del incidente) y, si fuera necesario, debe sugerir acción correctiva.

3.6. Acciones disciplinarias

Commented [AES14]: Eliminar este punto si el control A.6.4

El [cargo] debe activar el proceso disciplinario por cada violación de las reglas de seguridad.

3.7. Recolección de evidencia

Commented [AES15]: Eliminar este punto si el control A.5.28

El [cargo] definirá las reglas para identificar, recolectar y preservar evidencia que sería aceptada en procedimientos legales y de otros tipos.

4. Gestión de registros guardados en base a este documento

Nombre del registro	[illegible]	[illegible]	[illegible]	[illegible]
Registro de incidentes	[illegible]	[illegible]	[illegible]	[illegible]

Solamente el [cargo] puede permitir el acceso a los registros a otros empleados.

5. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible]

Commented [AES16]: Esto es sólo una recomendación; ajustar [illegible]

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de debilidades o incidentes que no fueron reportados a las personas autorizadas.
- Cantidad de incidentes que no fueron tratados de la forma más adecuada.
- [illegible]

6. Apéndices

- Apéndice 1 – Registro de incidentes

[cargo]
[nombre]

[firma]

Commented [AES17]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.