Tabla de contenido

[Política de Gestión de Incidentes y Mejoras en Seguridad de la Información 2](#_Toc181106078)

[Propósito 2](#_Toc181106079)

[Alcance 2](#_Toc181106080)

[Responsabilidades y Procedimientos 2](#_Toc181106081)

[1. Responsabilidad de Gestión de Incidentes 2](#_Toc181106082)

[2. Procesos y procedimientos 3](#_Toc181106083)

[3. Capacitación 3](#_Toc181106084)

[Reporte de Eventos de Seguridad de la información 3](#_Toc181106085)

[1. Evento 3](#_Toc181106086)

[2. Incidente 3](#_Toc181106087)

[3. Amenaza 4](#_Toc181106088)

[4. Vulnerabilidad 4](#_Toc181106089)

[5. Mecanismo de Reporte 5](#_Toc181106090)

[6. Responsabilidad de Reporte 5](#_Toc181106091)

[Reporte de Debilidades de Seguridad 5](#_Toc181106092)

[1. Identificación y Reporte de Vulnerabilidades 5](#_Toc181106093)

[2. Evaluación de Vulnerabilidades 5](#_Toc181106094)

[Evaluación y Decisión sobre Eventos de Seguridad 5](#_Toc181106095)

[1. Evaluación y Respuesta Rápida 5](#_Toc181106096)

[2. Registro y Documentación 6](#_Toc181106097)

[Respuesta a Incidentes de Seguridad 6](#_Toc181106098)

[1. Plan de Respuesta 6](#_Toc181106099)

[2. Comunicación durante el Incidente 7](#_Toc181106100)

[Aprendizaje de Incidentes 7](#_Toc181106101)

[1. Análisis Post-Incidente 7](#_Toc181106102)

[2. Mejora Continua 7](#_Toc181106103)

[3. Capacitación y Retroalimentación 7](#_Toc181106104)

[Recolección de Evidencia 8](#_Toc181106105)

[1. Preservación de Evidencia 8](#_Toc181106106)

[2. Procedimientos Forenses 8](#_Toc181106107)

[3. Almacenamiento Seguro 8](#_Toc181106108)

[Revisión y Mejora de la Política 9](#_Toc181106109)

# Política de Gestión de Incidentes y Mejoras en Seguridad de la Información

## Propósito

Definir un proceso claro y efectivo para identificar, reportar, responder y mejorar la gestión de incidentes de seguridad en la información. Este enfoque busca comunicar de manera oportuna cualquier evento o vulnerabilidad que pueda afectar la seguridad, reduciendo su impacto y fortaleciendo la infraestructura de seguridad de la empresa.

## Alcance

Aplica a todos los empleados y terceros que tengan acceso a los recursos de información de la empresa.

## Responsabilidades y Procedimientos

### Responsabilidad de Gestión de Incidentes

* El Área de sistemas de la Información liderará la gestión de incidentes, desde la identificación y evaluación hasta la respuesta y revisión.
* El usuario será responsable de comunicar cualquier evento inusual que ponga en riesgo la seguridad de la información

### Procesos y procedimientos

* El Área de sistemas mantendrá procedimientos claros y actualizados que cubran desde la detección de incidentes hasta su resolución y mejora continua.
* Estos procesos deben ser conocidos y aplicados por los usuarios al momento de que ocurra un incidente de seguridad
* Los medios de comunicación para el reporte de incidentes son: por medio telefónico, correo electrónico o cualquiera que sea autorizado por el encargado de sistemas de la empresa
* El procedimiento para la gestión de los incidentes se encuentra a continuación:

### Capacitación

* El personal encargado de solucionar las incidencias informáticas que se presentan está capacitado para tal fin.

## Reporte de Eventos de Seguridad de la información

Todo el personal tanto interno como externo a la empresa debe estar informados y familiarizados con los mecanismos de notificación.

A continuación, se definen cuatro conceptos clave en la seguridad de la información:

### Evento

Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad

### Incidente

Cuando el evento se puede clasificar como no deseado o inesperado dentro de los eventos de seguridad de la información y además tienen una probabilidad significativa de comprometer las operaciones comerciales y suponen una seria amenaza para la seguridad de la información

### Amenaza

Una amenaza se refiere a cualquier cosa que tenga el potencial de causar daños graves a un sistema o activo de información. Una amenaza es algo que puede suceder o no, pero tiene el potencial de causar un daño grave.

Las amenazas pueden provocar ataques a sistemas informáticos, redes y más.

### Vulnerabilidad

Se refiere a una debilidad o defecto en un sistema o activo de información que puede dejarlo expuesto a una amenaza o ataque. Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema de información en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza.

**En pocas palabras la amenaza es algo que puede o no suceder; sin embargo, tiene el potencial de hacer mucho daño al sistema o la información, una vulnerabilidad hace referencia a una debilidad en el sistema que puede dejar expuesta la seguridad de un sistema o de su información, el evento muchas veces es esperado que ocurra, se aprende de él y ayuda a endurecer la seguridad mientras que el incidente es algo indeseado y que puede comprometer las operaciones y amenazar la seguridad.**



### Mecanismo de Reporte

La empresa contará con un mecanismo accesible y confidencial para que todos los empleados reporten eventos de seguridad sin temor a represalias, estos pueden ser a través del correo electrónico, línea telefónica o cualquiera que sea autorizado por el encargado de sistemas de la empresa

### Responsabilidad de Reporte

Todo el personal debe reportar de inmediato cualquier incidente de seguridad detectado, sin intentar resolverlo personalmente.

## Reporte de Debilidades de Seguridad

### Identificación y Reporte de Vulnerabilidades

Cualquier debilidad observada en sistemas, aplicaciones o procesos debe reportarse de inmediato al Área de sistemas de la Información.

### Evaluación de Vulnerabilidades

El equipo revisará y priorizará cada reporte, evaluando su nivel de criticidad.

**Se aconseja advertir que los usuarios que probar la fortaleza o debilidad de los sistemas a ver si encuentran una vulnerabilidad serán considerados por la compañía como un mal uso del sistema**

## Evaluación y Decisión sobre Eventos de Seguridad

### Evaluación y Respuesta Rápida

El Área de sistemas evaluará cada evento, estableciendo su riesgo y las acciones necesarias para reducir el impacto.

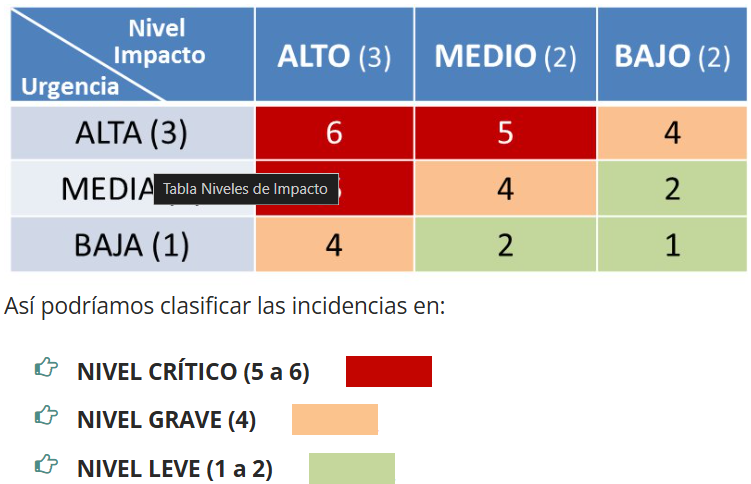
### Registro y Documentación

Todos los eventos deben documentarse, incluyendo su origen, impacto, decisiones y acciones realizadas.

La forma de clasificar los incidentes se hará en base a los siguientes dos parámetros

* Impacto: Daño causado al negocio (en términos económicos, imagen, etc.)
* Urgencia: La rapidez con la cual la empresa necesita corregir el incidente

Para tener una mejor idea, se presenta la siguiente gráfica, donde se expresa el nivel de impacto y la urgencia con que se debe corregir cada incidente, también permiten determinar su prioridad.



## Respuesta a Incidentes de Seguridad

### 1. Plan de Respuesta

La empresa deberá contar con un plan detallado que incluya:

* Detección y contención del incidente.
* Mitigación y corrección de sus efectos.
* Evaluación para determinar si se puede resolver el problema o si se requiere de un tercero.
* Mantener un registro con las evidencias de las incidencias.
* Establecer el sistema de comunicaciones entre los empleados y el Área de sistemas para llevar un control en el proceso de resolución de las incidencias.
* Registrar las acciones llevadas a cabo y sus resultados.
* Realizar un cierre formal de la incidencia una vez este resuelta.
* Realizar un análisis para determinar las causas de cada incidente.
* Realizar una evaluación posterior para aplicar lecciones aprendidas.

### 2. Comunicación durante el Incidente

Toda comunicación interna o externa relacionada con un incidente será gestionada por el Área de sistemas para asegurar la claridad y control de la información.

## Aprendizaje de Incidentes

### 1. Análisis Post-Incidente

Al concluir cada incidente, el Área de sistemas analizará la causa raíz para establecer medidas preventivas.

### 2. Mejora Continua

Los análisis se utilizarán para actualizar políticas y procedimientos de seguridad, reforzando las defensas.

### 3. Capacitación y Retroalimentación

Se ofrecerá capacitación específica al personal involucrado y se actualizarán los programas de formación según sea necesario.

Los controles para mantener una base de conocimientos sobre los incidentes en la seguridad de la información son:

Creación de un registro que considere:

* Volumen de incidentes producidos
* Tipología de incidentes producidos
* Coste de la resolución de la incidencia
* Impacto de la incidencia
* Solución aplicada

## Recolección de Evidencia

### 1. Preservación de Evidencia

Ante un incidente que requiera posible acción legal, el equipo deberá recolectar y preservar toda evidencia relevante de forma adecuada.

### 2. Procedimientos Forenses

La recolección de evidencia seguirá procedimientos rigurosos para asegurar su integridad y posible uso legal.

### 3. Almacenamiento Seguro

Toda evidencia se almacenará en un entorno seguro y accesible solo para personal autorizado, respetando los protocolos de confidencialidad.

El Área de sistemas debe tener control en la conservación de la información sobre las incidencias de forma que se pueda recuperar:

* Los inicios y cierres de sesión
* Las identificaciones
* El estado de los dispositivos y de las redes
* Las evidencias de reuniones informativas, documentación sobre responsabilidades y funciones de seguridad del personal

## Revisión y Mejora de la Política

Esta política se revisará anualmente o cuando se presenten incidentes significativos, asegurando la capacidad de respuesta y el cumplimiento con la norma ISO 27001.

Esta política asegura que la empresa esté preparada para gestionar incidentes de seguridad de manera eficiente, minimizando el impacto y fortaleciendo su postura de seguridad.