Gestión de Incidentes de SI

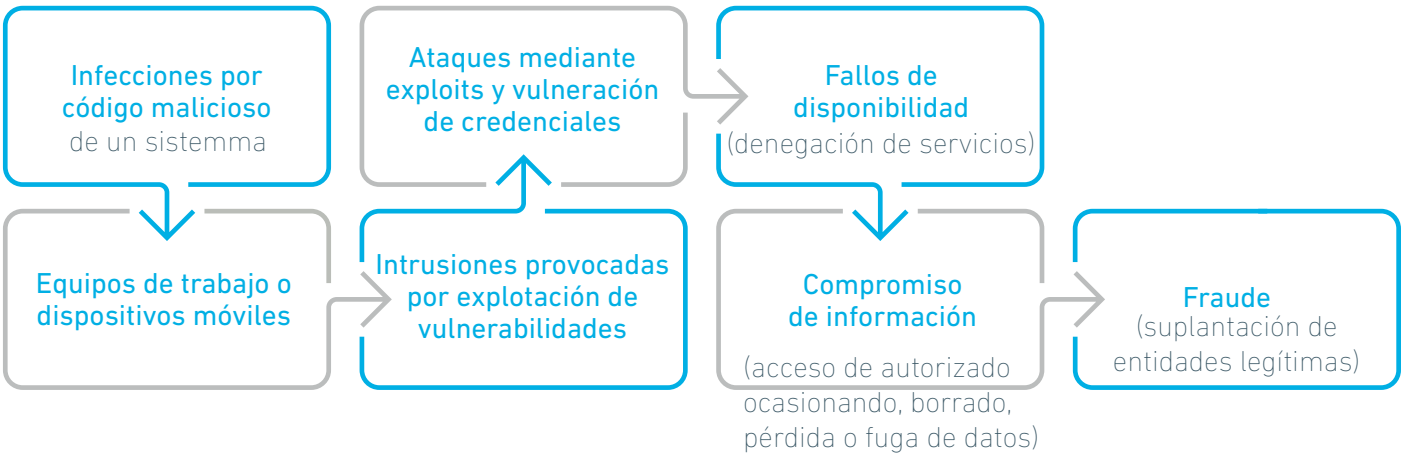
FASES DE GESTIÓN DE INCIDENTES

El propósito de la gestión de incidentes, es garantizar un proceso mediante un enfoque resistente y eficaz para su manejo, incorporando la comunicación de vulnerabilidades de cada caso con el fin de aplicar correctivos necesarios oportunamente en cada departamento de la organización. La implementación incluye los siguientes objetivos:

Detectar, informar y evaluar el incidente de información hallado.
Responder al incidente presentado.
Reportar las vulnerabilidades detectadas
Aprender de los incidentes de la seguridad de la información.

TIPOS DE INCIDENTES

Algunos incidentes que se destacan son:

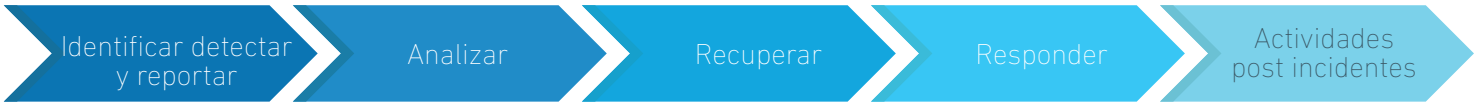


Angélica Viloria. (experta)
Ruth Berríos M. (diseñador)

CONTROLES PARA LA GESTIÓN DE INCIDENTES

La Norma ISO 27002 es el código de buenas prácticas que desarrolla los controles de seguridad de la información y en la gestión de incidentes se debe comprobar que existe un proceso en el que se incluya cómo actuar en caso de que se presente un evento, y minimizar el impacto de forma rápida ante cualquier amenaza.

CONTROLES PARA LA GESTIÓN DE INCIDENTES



Tratamiento de los procesos de la gestión de incidentes

Las responsabilidades dentro de la gestión de incidentes están ligadas a un plan específico y a la función que desempeña.
En los procedimientos, se debe tener claridad de que la gestión de la seguridad de incidentes, se entiende como el ejercicio de una consistente y efectiva proximidad de un evento o secuencia de eventos de seguridad de la información.

EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Conforme a lo que señala la ISO/IEC 27035:2016, el evento de seguridad de la información se da cuando se produce un suceso o cambio en las operaciones cuya ocurrencia indica una posible brecha de la seguridad de la información o falla en los controles.

DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Dentro de las **debilidades físicas** se encuentran:
• Inexistencia de controles para ingresar a lugares sensibles.
• Claves de seguridad pegadas en las pantallas de los computadores, papeles a un costado del escritorio, entre otros.
• Inexistencia de vigilancia en lugares de tratamiento de datos importantes.
• Inexistencia de controles de copias de documentos confidenciales
.
Las debilidades en la seguridad de la información tomando en cuenta **aspectos lógicos** pueden ser:
• Inexistencia de criptografía en las aplicaciones de la empresa.
• Network sin claves de acceso robustas.
• Softwares sin licencia y sin actualización.

EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SI

Para la evaluación y decisión, la organización debe realizar las siguientes actividades clave:

• Recolectar información que incluya test, medición y cualquier recopilación de datos sobre la detección de un evento de la seguridad de la información, el tipo y cantidad de información recolectada va a depender del tipo de evento de la seguridad de la información que ha ocurrido.
• El responsable debe realizar una evaluación que permita determinar si el evento es posible, si está confirmado, o se trata de un incidente de una falsa alarma, la falsa alarma (falso positivo) es un reporte del evento que es encontrado y que no es real o no tuvo consecuencias.
• Asegurarse de que todas las partes involucradas, en especial el SGSI, realicen un registro adecuado de todas las actividades, resultados y decisiones relacionadas para un posterior análisis.
• Asegurarse de que el régimen de control de cambios se mantenga para cubrir el rastro del incidente de seguridad de la información, las actualizaciones del reporte de incidentes, y mantener la base de datos de la seguridad de la información up-to-date.

RESPUESTA ANTE INCIDENTES DE SI

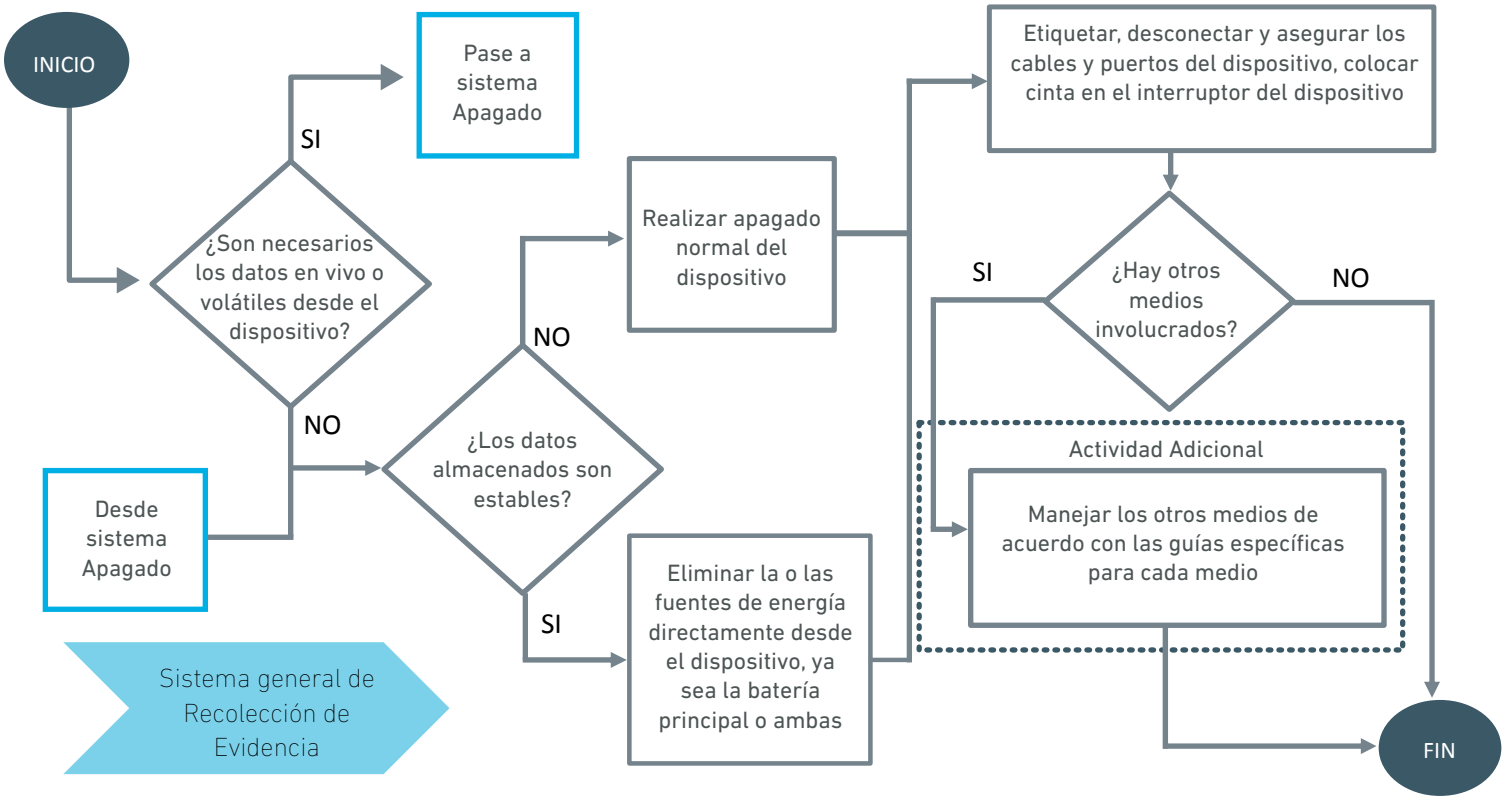
Una vez que el incidente de la seguridad de la información ha sido confirmado y las responsabilidades determinadas, se trata de controlar el proceso de resolución de incidentes en la seguridad de la información, los controles deben ser:
• Evaluar la capacidad de la organización para resolver el incidente por su sola o con ayuda de terceros.
• Mantener un registro con las evidencias de los incidentes.
• Usar guías formales de la documentación de un incidente de la información y acciones consiguientes.
• Establecer comunicación efectiva entre los usuarios y el equipo de gestión de incidentes, los cuales deben estar informados sobre las actuaciones y resolución en caso de presentarse incidencias.
• Registrar las acciones realizadas y sus resultados.
• Realizar análisis para determinar las causas del incidente.
• Cerrar evidencias formalmente luego de resueltos los incidentes reportados.

APRENDIZAJE DE INCIDENTES DE SI

Según NIST, la lección aprendida se encuentra en la actividad post incidente, en la cual es importante considerar las siguientes preguntas:

¿Qué fue lo que sucedió exactamente? ¿En qué período de tiempo?
¿Fue correcto el actuar del personal y de la gerencia cuando se lidiaba con el evento?
¿Se siguió el procedimiento documentado? ¿Fue el adecuado?
¿Qué información es necesaria pronto?
¿Qué paso o acción puede haber inhibido la recuperación?
¿Qué persona y gerencia puede hacer las cosas de manera diferente en una próxima oportunidad de un evento similar?
¿Cómo podría la información ser compartida con otras organizaciones para que realicen mejoras?
¿Qué acciones preventivas pueden realizarse en incidentes en el futuro?
¿Qué precursores o indicadores pueden ser observados en el futuro para prevenir incidentes similares?
¿Qué herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar incidentes en el futuro?

RECOLECCIÓN DE EVIDENCIAS



La evidencia digital para la ISO 27037 es "información o dato, guardado o transmitido en forma binaria desde que puede ser confiada como una evidencia", y recolección como "proceso de reunión de ítems físicos que contienen una potencial evidencia digital"
En este punto la norma establece controles para la identificación, recolección, adquisición y conservación de la información de evidencia digital. En este proceso se puede conservar información en incidencias que se puedan recuperar como: inicios y cierres de sesión, las identificaciones, el estado de los dispositivos y redes, y evidencias de reuniones informativas, documentación sobre responsabilidades y funciones de seguridad del personal.