

ANEXO C

Guía para la gestión de incidentes de seguridad de la información

CTIC-SE-P1-v.1.0



AGETIC

agencia de gobierno electrónico y
tecnologías de información y comunicación

GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1 . Introducción

Al implementar el Plan Institucional de Seguridad de la Información, la entidad debe planificar las acciones para responder ante incidentes que afecten a la seguridad de la información, fruto de errores intencionados o vulnerabilidades no contempladas en la evaluación de riesgos.

La gestión de incidentes llega a ser un control más para la seguridad de la información, porque entra en escena cuando los controles preventivos son ineficaces o están ausentes, sobre todo en aquellos riesgos, que luego de la valoración estos han sido asumidos, conscientes del riesgo que ello implica. Sobre los cuales se tienen que realizar monitoreos para mantener la seguridad en niveles aceptables.

Esta guía está basada en buenas prácticas de gestión de incidentes de la norma ISO/IEC 27035, pero la misma no obliga su adopción y la entidad o institución pública es libre de utilizar otro marco de trabajo.

2 . Objetivo

Orientar sobre la planificación y organización del proceso de gestión de incidentes en seguridad de la información.

3 . Referencias

La presente guía toma como referencia buenas prácticas en gestión de incidentes del estándar ISO/IEC 27035.

4 . Documentos relacionados

La presente guía tiene relación con los siguientes documentos:

- Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.
- Anexo A – Controles de Seguridad de la Información.

5 . Términos y definiciones

Responsable de Seguridad de la Información.- Servidor público que tiene asignadas las funciones de desarrollar e implementar el Plan Institucional de Seguridad de la Información, que entre las responsabilidades está la de gestionar incidentes.

Evento de seguridad de la información.- Ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información o la falla de controles o una situación previamente desconocida, que pueda ser relevante para la seguridad.¹

Incidente de seguridad de la información.- Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.²

6 . Gestión de incidentes

La gestión de incidentes comprende la asignación de roles y responsabilidades para el desarrollo de actividades ante la ocurrencia de incidentes.

Una de las funciones del Responsable de Seguridad de la Información es la coordinación de acciones conjuntas con las partes interesadas para atención de incidentes.

El proceso de gestión de incidentes debe estar enmarcado en la mejora continua, que permita mejorar actividades para futuros incidentes. Los resultados de la gestión de incidentes deben ser documentados; esto permitirá analizar y realizar mejoras a controles existentes o implementar nuevos.

6.1 . Planificación y preparación

Durante la planificación y preparación se debería considerar conformar un equipo de respuesta ante incidentes al interior de la entidad, liderado por el Responsable de Seguridad de la Información.

La planificación debe identificar y definir los elementos y recursos necesarios para cubrir actividades de gestión de incidentes. Una buena práctica es establecer procedimientos adecuados para el reporte por parte de los servidores públicos, seguido de programas de capacitación.

Contemplar actividades preventivas en la gestión de incidentes es una práctica que viene a minimizar la ocurrencia de los mismos, en la planificación se debería asegurar que los procedimientos para actividades críticas como respaldos, prevención de código malicioso, gestión de vulnerabilidades técnicas y otros se hagan efectivos, sobre todo la concientización y sensibilización al personal.

1 Términos y Definiciones NB/ISO/IEC 27000:2010

2 Términos y Definiciones NB/ISO/IEC 27000:2010

El RSI debe realizar el seguimiento de las actividades descritas anteriormente, para que cuando un evento ocurra, sea posible reanudar la continuidad de las operaciones en un tiempo oportuno.

Se deben definir canales de comunicación y puntos de contacto para reporte de incidentes y posterior atención, establecer procedimientos para el escalamiento de incidentes y su pronta resolución, además de elaborar directrices claras y entendibles para diferenciar entre un evento de seguridad y soporte técnico.

Una buena práctica en esta fase es clasificar los incidentes de acuerdo a las amenazas identificadas en el inventario de activos de información. La clasificación permite preparar acciones en caso de ocurrencia.

Algunos ejemplos de incidentes pueden relacionarse con:

- Accesos no autorizados
 - Acceso físico a instalaciones de procesamiento de información o áreas seguras.
 - Acceso lógico a información, servicios, sistemas, bases de datos y otros.
 - Inyección de contenido.
 - Puertas traseras.
 - Elevación de privilegios.
- Denegación de servicios
 - Ataques de fuerza bruta.
 - Ataques de denegación de servicio distribuido.
 - Inundación SYN, ICMP, UDP, HTTP.
- Divulgación y pérdida de información
 - Ingeniería social.
 - Intencionada.
 - No intencionada.
 - Robo de documentación.
- Infección de malware
 - Virus.
 - Puertas traseras.
 - Ransomware.
 - Gusanos.
- Desfiguración de sitios
 - Cambio parcial o total del sitio web, sistemas y/o aplicaciones.
- Violación de la Política de Seguridad
 - Incumplimiento de la normativa.
 - Acciones premeditadas.
- Pérdida o robo de equipamiento

- Dispositivos de red.
 - Periféricos.
 - Estaciones de trabajo.
- Correo electrónico
 - Suplantación de correo.
 - Spam.
- Otros Incidentes

6.2 . Detección y reporte

En esta fase el Responsable de Seguridad de la Información, junto con los responsables de activos de información, deben establecer criterios que permitan detectar un posible evento de seguridad e implementar mecanismos de registro del suceso para posterior análisis.

El Responsable de Seguridad de la Información debe realizar el reporte formal de eventos de seguridad y los procesos de escalamiento que se puedan tener.

Los servidores públicos deberían conocer las responsabilidades que tienen con la seguridad de la información y la obligación de reportar la ocurrencia de incidentes producto de la violación de las políticas, omisión de procedimientos e identificación de vulnerabilidades. La entidad o institución debería establecer medios como el correo electrónico, números de teléfono, personas de contacto, implementación de sistemas de atención y seguimiento de incidentes.

Identificar distintas fuentes de detección como ser: software antivirus, reporte de usuarios, alertas por correo sobre caídas de servicio y otros convenientes. Esta información a corto plazo permitirá redefinir los procedimientos para minimizar el impacto, pero no solo basta detectar el incidente, también es importante implementar mecanismos que permitan la identificación y análisis en detalle, como pueden ser los registros de logs en el caso de servidores.

6.3 . Valoración y decisión

Una vez detectado un incidente, el siguiente paso debe ser el análisis, valoración y decisión sobre las acciones a realizar. Los responsables de infraestructuras tecnológicas y responsables de procesos deben conocer la funcionalidad normal de los procesos para determinar la confirmación de un incidente.

Para la valoración se debería contar con la mayor cantidad de información posible para realizar el análisis, correlación de sucesos, patrones de comportamiento, consultar incidentes pasados y otros. La evaluación debe contar con escalas para medir el

impacto y prioridad que se le dará al incidente; se recomienda que las escalas estén en función de valores establecidos en la evaluación de riesgos.

Ejemplo 1. Escala de Impacto

Escala	Definición
Bajo	La incidencia no afecta a un servicio crítico de la institución pública.
Medio	La incidencia tiene efectos mínimos sobre sistemas críticos. La institución pública puede proporcionar servicios críticos.
Alto	La incidencia tiene efecto significativo e inmediato sobre los sistemas críticos de la institución pública.
Crítico	Graves efectos en los sistemas críticos de la institución pública que impiden la continuidad de los servicios que esta proporciona.

Se deben establecer niveles de impacto ocasionado y actuar en consecuencia; el nivel puede ser el mismo que se ha definido para la evaluación de riesgos u otro. En este punto se debe haber definido previamente la clasificación de tipos de incidentes.

Se sugiere la siguiente clasificación:

Ejemplo 2. Clasificación de Incidentes

Tipo de incidente	Descripción
Acceso no autorizado	Acceso a información protegida implícita o explícita, provocando la degradación de información y otros.
Ataques por vulnerabilidades	En esta clasificación ingresarían los ataques por inyección sql, xss, redirecciones, envenenamiento de DNS, envenenamiento ARP, ataques de día cero y otros.
Código malicioso	En esta clasificación ingresan los virus, troyanos, puertas traseras, rootkits, keyloggers, ransomware y otros.
Denegación de servicio	Ingresa toda la gama de ataques de denegación de servicios como ser : DDoS, inundación SYN, ICMP, UDP y otros.
Desfiguración de sitio	Defacement total o parcial de sitios web y otros.
Divulgación de información	Ataques de ingeniería social, espionaje, phishing y otros.
Fallas de hardware o infraestructura tecnológica	Fallas de hardware, infraestructura tecnológica y otras.

Para la adecuada respuesta a incidentes se debe establecer el nivel de prioridad para los mismos, esto permitirá atender el incidente en función de criticidad y utilizar los recursos necesarios para contener y recuperar los servicios que se vean afectados. Se sugiere utilizar la siguiente escala:

Ejemplo 3. Escala de Prioridades

Prioridad	Descripción
Baja	Sistemas o servicios que tienen un impacto potencial de poca consideración.
Media	Sistemas o servicios que tienen relación con otros y esta provoca una afectación parcial en las mismas.
Alta	Sistemas o servicios relacionados al área de infraestructura tecnológica.
Crítico	Sistemas o servicios críticos para la entidad o institución pública.

También es buena práctica establecer tiempos de respuesta para la atención de incidentes, esto dependerá de la escala de prioridades y categorización; la presente guía no pretende establecer los mismos y deja a consideración de la entidad su definición.

En esta etapa se deben establecer procedimientos para escalar el incidente al Centro de Gestión de Incidentes Informáticos.

6.4 . Respuesta y erradicación

La respuesta hace efectiva las actividades previamente descritas; para esto es necesario documentar las acciones que se vayan a realizar. Las actividades adicionales a la respuesta del incidente son: analizar posibles daños colaterales por la propagación del incidente que provoque afectación a la información o infraestructura tecnológica; para esto en la planificación se debería contar con procedimientos de acción para determinado incidente aunque no siempre se puede predecir el evento, pero tomar las previsiones ya es una ventaja.

Ejemplo 4. Posibles Acciones por Tipo de Incidente

Tipo de incidente	Causas comunes	Posibles acciones de respuesta
Acceso no autorizado	Acceso físico: Las causas comunes son la permisividad e inexistencia de control de instalaciones internas. Estas pueden ser por personas internas y externas.	Identificar a la persona que infringe la normativa interna, indagar motivos por los cuales se encuentra en instalaciones sin autorización, identificar causas que permitieron su ingreso.

	<p>Acceso lógico: Configuraciones por defecto, errores de aplicación, vulnerabilidades o parches de seguridad no aplicados, entre otros.</p>	<p>Para el acceso lógico es algo más complejo; las acciones a tomar dependerán del tipo y gravedad del incidente. Revisión de registros, recuperar el servicio afectado, correlación de accesos, permisos, horas, nombres de usuario, origen y otros.</p>
Ataques por vulnerabilidades	<p>Vulnerabilidades de día cero, versiones de aplicación desactualizadas o descontinuadas, entre otros.</p>	<p>Identificar el sistema y/o servicio afectado; contar con respaldos de información; dependiendo de la gravedad, detener el servicio; restaurar configuraciones e información anteriores.</p>
Código malicioso	<p>Campañas de phishing, uso descontrolado de dispositivos de almacenamiento, acceso a páginas sospechosas, vulnerabilidades a nivel de red que faciliten la propagación.</p>	<p>Identificar el tipo de código malicioso, aislar equipos comprometidos de la red, monitoreo del tráfico de red. Analizar el comportamiento del código malicioso, entre otras acciones.</p>
Denegación de Servicio	<p>Generalmente ocurren por motivos intencionados que buscan restringir el acceso y disponibilidad de servicios, aprovechando cambios incontrolados de configuración, mal funcionamiento de hardware, incidentes no intencionados, errores incontrolados en sistemas y otros.</p>	<p>Identificar el origen del ataque y bloquear el mismo; esto si no se trata de una denegación distribuida. Para su prevención se recomienda implementar reglas para identificar y bloquear automáticamente estos ataques.</p>
Desfiguración de sitios web	<p>Debido principalmente a vulnerabilidades en aplicación y servidor, como ser contraseñas débiles.</p>	<p>Acciones preventivas: copias de respaldo del sitio completo, archivo de la página principal en texto plano html. Acciones correctivas: extraer una o varias copias completas del sitio, reemplazar el archivo en texto plano. En estos casos el objetivo principal es restablecer la página original.</p>
Divulgación de información	<p>Accesos no autorizados a instalaciones con información sensible expuestas en lugares visibles sin seguridad.</p>	<p>Este tipo de incidentes debe tener tratamiento especial, porque la finalidad no es restablecer servicios. Las acciones deberían estar orientadas al análisis de las causas, origen y responsables, para prevenir futuros incidentes.</p>

Todas las acciones deberían estar dirigidas a restablecer el servicio en los tiempos establecidos.

Después de que el incidente haya pasado y se hayan restablecido los servicios, se debería realizar la erradicación del problema adoptando estrategias de erradicación. Esto consiste en analizar las posibles consecuencias del incidente como ser: código malicioso que puede estar oculto, configuraciones del servidor y otras que, dependiendo del tipo de incidente, se pueden analizar otros servicios relacionados de forma directa o indirecta.

La respuesta al incidente debería finalizar con un informe que documente las actividades realizadas. La experiencia adquirida deberá permitir mejorar las acciones de respuesta para futuros incidentes con similar característica.

La gestión de incidentes es parte integral de la seguridad, ya que se pueden identificar debilidades en los controles y mejorar los mismos, con la modificación o la implementación de nuevos controles.

En caso de existir un incidente crítico que afecte la imagen institucional, se deberá designar un encargado de comunicar y otorgar información como portavoz autorizado.

6.5 . Mejora continua

La experiencia adquirida en la atención al incidente, así como toda la información obtenida durante la atención, deberá permitir elaborar un plan de acción de mejora continua.

Un proceso de mejora continua debe ser aplicado para la respuesta al seguimiento, evaluación y en general a la gestión de incidentes de seguridad de la información, que permita que los responsables entiendan las prioridades de la institución para manejo de incidentes.

El objetivo de este plan de acción no deberá ser en ningún caso un objetivo de auditoría o de búsqueda de responsables, más al contrario el plan deberá fortalecer la seguridad de la entidad o institución pública para evitar la repetición de incidentes similares en el futuro.