[Curso de Introducción a la Seguridad Informática](https://platzi.com/clases/seguridad-informatica/)

**ArtículoRecomendaciones para la atención y manejo de incidentes de seguridad**

[**atovarg**](https://platzi.com/@atovarg)

24 de Enero de 2019

En la actualidad, resulta bastante difícil asegurar con total certeza que una compañía no pueda ser víctima de incidentes relacionados con la seguridad informática. No obstante, lo que sí es posible gestionar es la forma de reaccionar ante la materialización que un riesgo específico. Tener un enfoque estructurado y bien planificado nos permitirá manejarlos adecuadamente y minimizar el impacto que estos tengan sobre determinado proceso operativo en la compañía.

De acuerdo a nuestra clase sobre la gestión de incidentes, en la que vimos las fases a tener en cuenta para la atención de los mismos, te voy a mencionar los aspectos más relevantes que deberás tener en cuenta durante cada fase para que tu gestión de incidentes tenga el mayor éxito posible.

**Fase 1: Preparación**  
Definir los roles y responsabilidades dentro de la compañía de forma clara y puntual, que permita mantener la operación, la continuidad y la disponibilidad del servicio. Esta fase suele hacerse pensando no sólo en crear un modelo que permita a la compañía estar en capacidad de responder ante estos, sino también en la forma cómo pueden ser detectadas, evaluadas y gestionadas las vulnerabilidades para prevenirse, es decir, intenta que tu proceso de gestión de incidentes pueda llegar a ser proactivo y estar en lo posible siempre un paso adelante de la amenaza.

* Ocúpate en esta fase de temas como:
* Gestión de Parches de Seguridad
* Aseguramiento de plataforma
* Prevención de malware
* Sensibilización y entrenamiento de usuarios

**Fase 2: Detección y Análisis**  
Si mantienes unos buenos indicadores y un completo monitoreo de toda tu infraestructura tecnológica, podrás detectar oportunamente señales de alerta que te permitan identificar un posible evento aislado que tenga el potencial de convertirse en un importante incidente que afecte la seguridad de tu compañía. La clave en esta fase radica en el monitoreo del performance de tu infraestructura TI, generalmente algunos de estos elementos son:

* Alertas en sistemas de seguridad
* Caídas de servidores
* Reportes de usuarios
* Software antivirus dando informes
* Otros funcionamientos fuera de lo normal del sistema

**Fase 3: Identificación**  
En esta fase ya estamos seguros que ha ocurrido un incidente de seguridad, el paso a seguir es identificar el tipo de incidente ocurrido y si ha ocurrido más de uno para posteriormente priorizarlos dependiendo de su impacto.

**Fase 4: Notificación**  
Es muy importante comunicar de forma eficiente cuando ocurre un incidente, si este paso se realiza de forma desordenada y a la ligera, estarás perdiendo tiempo muy valioso para la resolución del mismo. En esta fase debes tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones. De acuerdo a mi experiencia profesional si tu compañía es de interés público es aconsejable contar con una Política de Comunicación que pueda definir qué incidente puede ser notificado a los medios de comunicación y cuál no.

**Fase 5: Clasificación y Priorización**  
Ahora deberás clasificar el incidente dentro de una determinada categoría, esto te permitirá enfocar mejor los esfuerzos para la resolución, algunos de las categorías más comunes pueden ser:

* Accesos no autorizados a la información
* Fuga de información confidencial
* Interrupción de operaciones
* Fallas de hardware
* Ataques Informáticos

Con el fin de permitir una atención adecuada a los incidentes, debes determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad. Recuerda identificar el tipo de recurso tecnológico y el perfil del usuario afectado.

**Fase 6: Contención, Resolución y Recuperación**  
Esta fase es la encargada de evitar que el incidente afecte más infraestructura tecnológica de la que afectó inicialmente, por ejemplo si es un ataque informático deberás aislar de la red corporativa el equipo o equipos involucrados, así evitarás que sean afectados otros segmentos de la red.

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

**Fase 7: Acciones Posteriores al Cierre**  
Esta fase básicamente se compone de actividades como el reporte apropiado del incidente, la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales (de ser necesarias) así como el registro en la base de conocimiento para alimentar los indicadores.

Reportar un problema

**¿Qué es malware Tipos de malware**