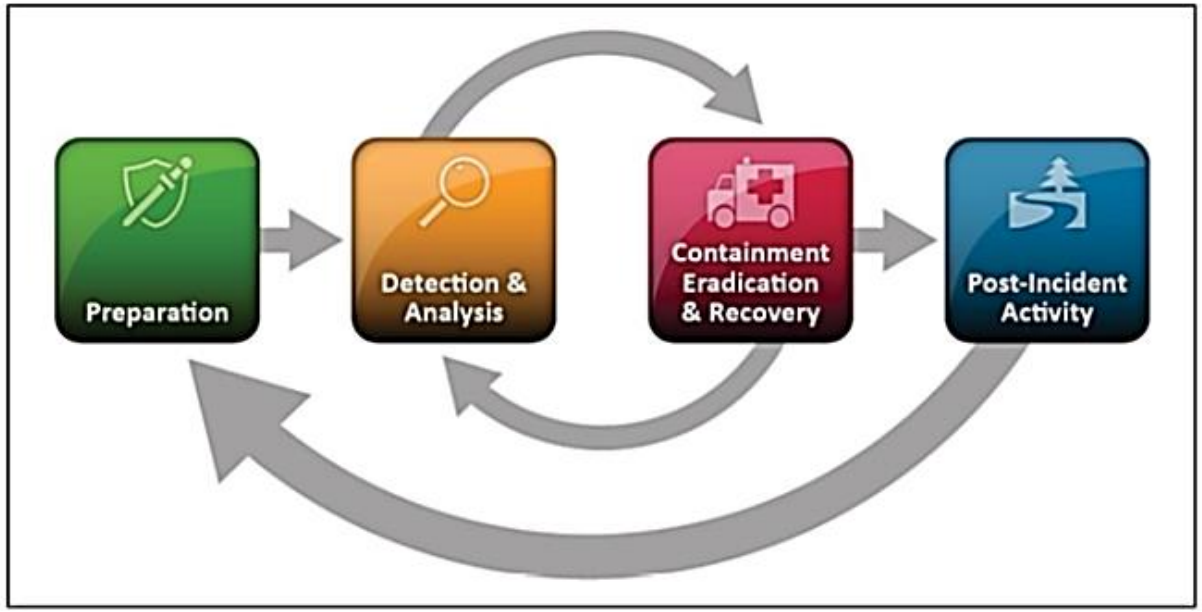
Ciclo de vida de la gestión de un incidente

La mayoría de los estándares de referencia para la gestión de incidentes describen una serie de etapas a seguir para un manejo adecuado de los mismos, que se resume en una etapa de preparación (preincidente), una etapa de detección del incidente, otra etapa en la que se toman las decisiones correspondientes a la contención, erradicación y recuperación ante el incidente, y por último una etapa de actividad postincidente.



Ciclo de vida de la gestión de un incidente de seguridad según la guía SP 800-61 publicada por el NIST

Ciclo de vida de la gestión de un incidente

En este capítulo es reseñable mencionar el siguiente párrafo del Esquema Nacional de Seguridad:

> *"La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan."*

Tomando como referencia la norma ISO/IEC 27035, la gestión de incidentes de seguridad de la información consta de cinco fases y a las que sería interesante añadir una sexta etapa que consistiría en el cierre del incidente, dándole de esta forma un peso excepcional no dando finalizando el ciclo hasta haber llevado a cabo todas las iniciativas en curso. Por tanto, el ciclo de vida de la gestión de un incidente podría resumirse en:

Ciclo de vida de la gestión de un incidente

1. **Planificación y preparación.** Esta fase se centra en llevar a cabo todas las acciones necesarias para la preparación ante un incidente de seguridad. En líneas generales esta etapa engloba:
    - Plan de gestión de incidentes. Procedimientos de actuación.
    - Política de seguridad de la información.
    - Establecimiento del equipo de respuesta a incidentes de seguridad.
    - Concienciación y formación sobre la gestión de incidentes.
    - Implantación y mantenimiento de los elementos de monitorización de eventos de seguridad.
    - Simulacros del plan de gestión de incidentes.
    - Definición de la taxonomía de incidentes de seguridad.
    - Plan de intercambio de información y comunicación con terceros.
    - Formación permanente del equipo humano.

Ciclo de vida de la gestión de un incidente

2. **Detección y reporte.** Fundamentalmente esta fase consta de:
    - Recopilación de información, tanto interna como externa a través de los mecanismos establecidos en la etapa anterior.
    - Identificar actividad anómala.
    - Registrar y notificar el incidente en caso de confirmarse.

3. **Valoración y decisión** sobre la información recopilada que determina si se está o no ante un incidente de ciberseguridad y cómo se debería abordar. En este punto se hace una primera clasificación del incidente de acuerdo a la taxonomía definida y se estima el impacto que está ocasionando o podría ocasionar dicho incidente. No obstante, estos parámetros podrán ser reevaluados más adelante.

4. **Respuesta.** Se continúa con la investigación del incidente siendo necesario en ocasiones llevar a cabo una recopilación y análisis de evidencias para ampliar la información de la que se dispone, de forma que las decisiones que se tomen en esta etapa sean las más adecuadas, proporcionadas y ágiles. A más rapidez de

Ciclo de vida de la gestión de un incidente

actuación en la respuesta, menor impacto ocasionará el incidente. Esta fase pasa por las siguientes subetapas:

- Contención del incidente.
- Erradicación del incidente.
- Recuperación tras el incidente.

5. **Lecciones aprendidas.** Esta etapa es imprescindible para la mejora continua del ciclo de vida de la gestión de incidentes porque nos ayuda a identificar tanto las carencias como los puntos fuertes de las etapas llevadas a cabo, así como nos pone de manifiesto posibles mejoras en protección y ciberdefensa de la organización. Entre otros, sus objetivos son:
   - Identificación de mejoras ante los planes, políticas, procedimientos, etc.
   - Evaluación de la efectividad, agilidad y desempeño del equipo de respuesta ante incidentes.
   - Identificación de mejoras ante los sistemas de monitorización y obtención de información.

Ciclo de vida de la gestión de un incidente

6. **Cierre del incidente.** Actividad post-incidente. El incidente de seguridad no se dará por finalizado hasta haber identificado las lecciones aprendidas y haya un plan para llevarlas a cabo.

Un diagrama de flujo del ciclo de vida de la gestión de incidentes de seguridad se muestra gráficamente a continuación:

Ciclo de vida de la gestión de un incidente