# Implementación de medidas de ciberseguridad (Incidentes de ciberseguridad)

## Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes

A pesar de que las medidas de mitigación dependen del tipo de ciberincidente y la afectación que haya tenido, algunas recomendaciones en esta fase son:

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes.
- Recuperación de la última copia de seguridad limpia.
- Identificar servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.

Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece: las lecciones aprendidas.

Conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación
similar se pueda volver a repetir, además de mejorar los procedimientos.

Por último se realizará un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

---

**Más información**

- http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf

---

# Implantar capacidades de ciberresiliencia

La ciber-resiliencia, es la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes.

Las empresas, en general están poco preparadas para resistir frente a este tipo de ataques, debido principalmente a:

- Falta de medidas técnicas para mitigarlos,
- poca preparación de los sistemas para detener este tipo de ataques,
- falta de formación o de recursos para hacerles frente o
- falta de pruebas para evaluar la capacidad real de la organización ante cualquier tipo de ataque externo.

Las organizaciones, deben estar preparadas para dar respuestas rápidas a este tipo de ataques, permitiendo que los servicios que prestan no se vean interrumpidos, fortaleciendo sus capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua contra las ciberamenazas.

---

**Más información**

- https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf

---

# Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses.

- Daño potencial y hurto de activos.
- Necesidades para la preservación de evidencia.
- Disponibilidad del servicio.
- Tiempo y recursos para implementar la estrategia.
- Efectividad de la estrategia para contener el incidente (parcial o total).
- Duración de la solución.

# Tareas para reestablecer los servicios afectados por incidentes

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes.

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.

Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece: las lecciones aprendidas.

# Documentación

Conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir, además de mejorar los procedimientos.

Por último se realizará un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

## Seguimiento de incidentes para evitar una situación similar

Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier signo de actividad sospechosa, definiendo un periodo de tiempo con medidas adicionales de monitorización.