

# Claves para la gestión de ciberincidentes



1

**Disponer de herramientas, mecanismos, y procedimientos de detección** que alerten al organismo de comportamientos anómalos en sus sistemas y redes. Para ello, se recomienda la adhesión al Sistema de Alerta Temprana (SAT) del CCN-CERT.

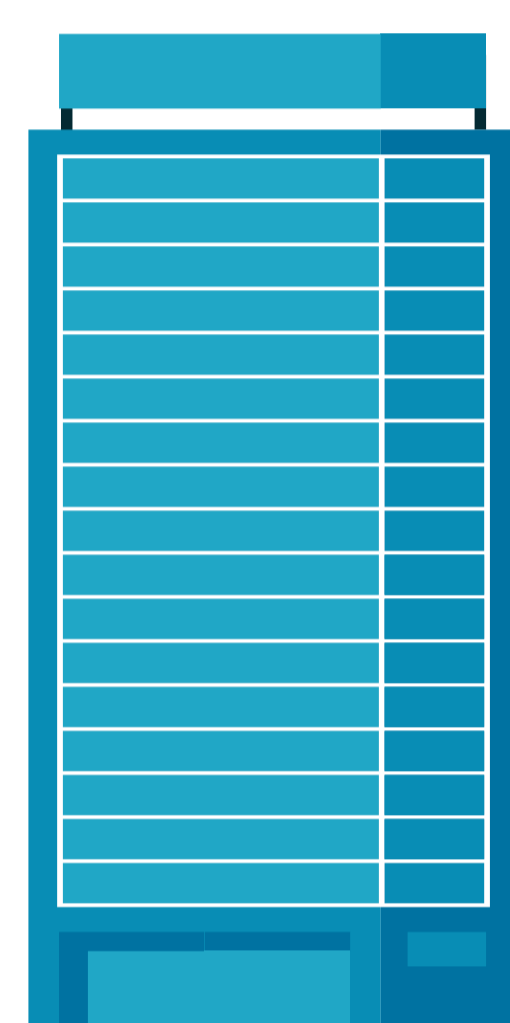
2

Es fundamental **identificar la amenaza, la peligrosidad potencial y prevenir** de esta manera **el posible impacto** sobre el servicio.



3

**El organismo debe conocer su grado de madurez** para responder al incidente en base a la tipología y peligrosidad definidos en la guía CCN-STIC 817.



4

**Actuar con prontitud**, sin dilación indebida. **Notificar el incidente a la autoridad competente** a través del CSIRT de referencia para establecer una comunicación directa. En el caso del sector Público, los organismos víctimas de posibles ciberincidentes deberán notificar al CCN-CERT. La notificación es un paso fundamental: el incidente puede estar afectando a otro organismo de forma simultánea.



5

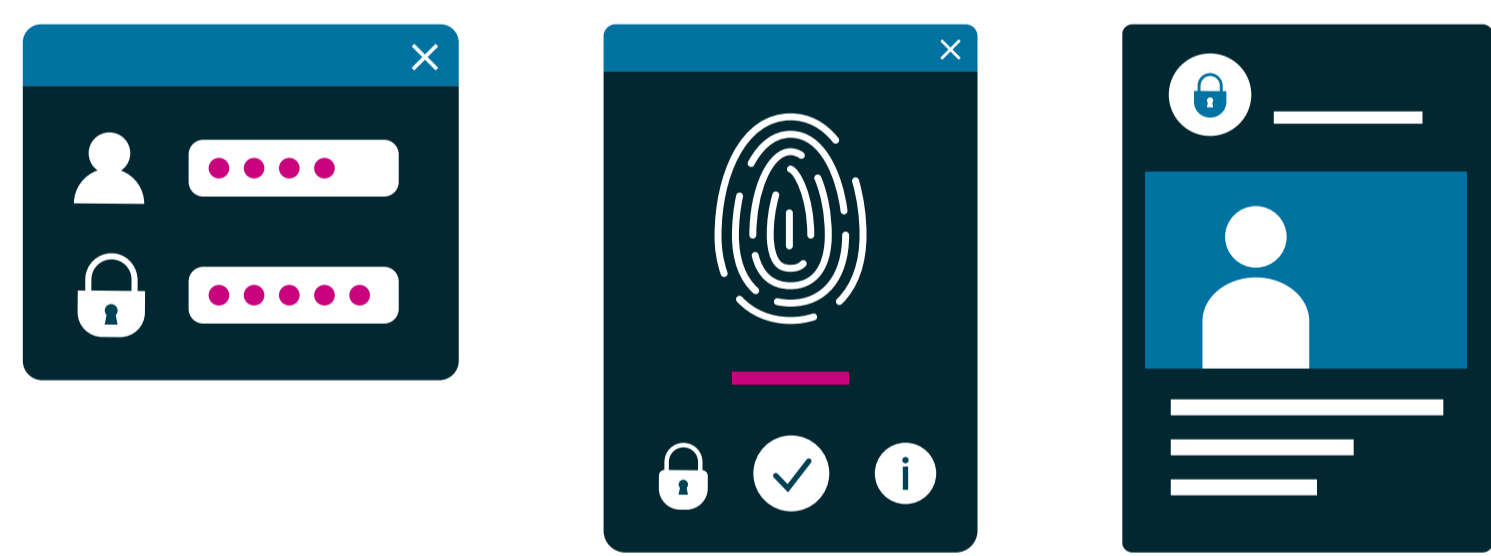
**Priorización y ejecución de procedimientos y medidas para evitar la propagación del incidente.**

El procedimiento de notificación de incidentes tiene que ser una realidad dentro del marco normativo que desarrolla el plan de implantación para dar respuesta a la política de seguridad del organismo.



6

**Recopilar toda la información del incidente.** Revisar los eventos de seguridad y determinar los activos internos que han sufrido el intento de ataque y lo que es más importante priorizar en base a la peligrosidad y el contexto (triaje).

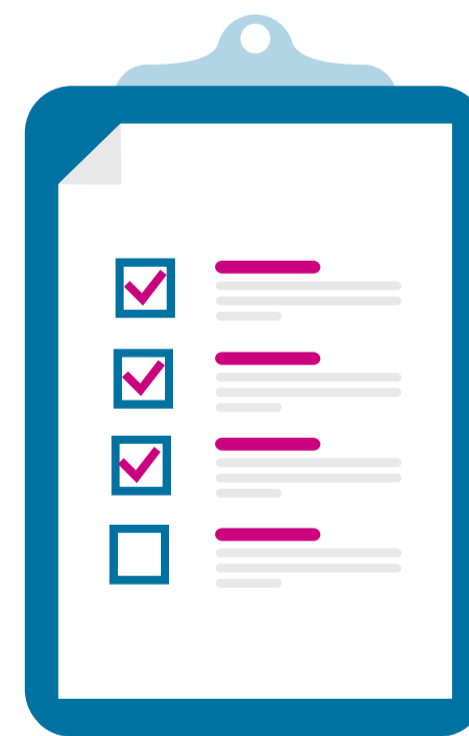


8

**Contener y mitigar la amenaza.** Llevar a cabo labores de investigación, auditoría, bastionado, análisis forense e ingeniería inversa.

7

**Documentar el incidente y las acciones llevadas a cabo** en el momento de su detección.



9

**Restauración de sistemas y servicios siguiendo un plan establecido.** Se determinará técnicamente el riesgo de reconexión de un sistema indicando los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto para, en la manera de lo posible, evitar que se den de nuevo las circunstancias que lo propiciaron.



10

**Resolución y cierre del incidente.** Determinar el impacto del ciberataque y revisar y reforzar las políticas y medidas de seguridad necesarias.

