#PrimerosAuxilios Digitales

¿Qué hacer en **los primeros minutos** tras un **ciberataque**?

En 10 pasos

Como con un botiquín de primeros auxilios, lo mejor es tener todo listo antes de necesitarlo.

Prepara tu kit de emergencia digital antes del incidente:

- Manual de actuación
- Contactos de emergencia
- Copias de seguridad seguras y desconectadas
- Roles asignados y personal formado

¡Tener esta infografía siempre a mano!

1 Detecta la amenaza

Vigilar que todo funciona correctamente

- ☐ Observa comportamientos inusuales en tus sistemas (lentitud, mensajes raros, accesos sospechosos).

2 Desconecta y aísla

Evitar la propagación del ataque

- ☐ Desconecta los equipos afectados de internet y de la red interna (*WiFi*, cable de red, *bluetooth*).
- ☐ Apaga el equipo solo si no puedes aislarlo.
- ☐ No conectes ningún USB ni disco duro externo.

3 Evalúa el alcance

Saber qué ha pasado y a quién ha afectado

- ☐ Anota los sistemas o servicios afectados y qué funciones están fallando.
- ☐ Identifica los síntomas (mensajes extraños, lentitud, accesos sospechosos).
- ☐ Documenta lo que observes sin modificar archivos.
- ☐ Pregunta a otros usuarios si también notan problemas.
- ☐ Reúne la máxima información útil para los técnicos.

4 Contén la amenaza

Impedir que el ataque se extienda

- ☐ Cambia contraseñas desde un dispositivo NO afectado. Prioriza accesos críticos como correo y sistemas y no uses nuevas contraseñas en equipos comprometidos.
- ☐ Bloquea accesos no autorizados en paneles de control o cuentas online y cierra sesiones.
- ☐ Activa los protocolos de seguridad si tienes un plan de contingencia.

5 Comunica con calma

Informar sin generar pánico

- ☐ Avisa a tus empleados y responsables usando canales seguros (email cifrado, mensajería protegida).
- ☐ Designa una persona que centralice la comunicación externa.
- ☐ No hagas públicas declaraciones sin verificar antes la información.

6 Notifica a los expertos

Obtener ayuda profesional y cumplir la ley

- ☐ Reporta a INCIBE-CERT (o llama al 017).
- ☐ Si manejas datos personales, valora si debes notificar a la AEPD.
- ☐ Si el daño es grave, considera avisar a las fuerzas de seguridad.

7 Documenta todo

Ayudar a las Fuerzas y Cuerpos de Seguridad

- ☐ Relato cronológico de los hechos.
- ☐ Pruebas visuales y electrónicas de lo sucedido.
- ☐ Descripción de los daños.

8 Analiza el *malware* (si puedes)

Saber con qué estás lidiando

- ☐ Usa un antivirus actualizado desde un equipo seguro para escanear archivos.
- ☐ No abras ni elimines archivos sospechosos y no reenvíes correos afectados.
- ☐ Documenta todo lo que encuentres (pantallazos, registros de actividad).

9 Restaura desde copias de seguridad

Recuperar la normalidad sin arrastrar el problema

- ☐ Reinstala el sistema desde *backups* que sepas que están limpios y verificados.
- ☐ No reutilices dispositivos hasta estar seguros de que no están comprometidos.
- ☐ Comprueba que todo funciona antes de volver a operar.

10 Aprende y mejora

Aprender del incidente y fortalecer tu defensa

- ☐ Haz una revisión post-incidente con tu equipo.
- ☐ Actualiza el plan de crisis según lo aprendido.
- ☐ Capacita al personal sobre nuevas amenazas.

Financiado por la Unión Europea NextGenerationEU

Ministerio de Defensa · Secretaría de Estado Digital y para la Inteligencia Artificial · Secretaría General de Administración Digital · Plan de Recuperación, Transformación y Resiliencia · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD