

# #PrimerosAuxilios Digitales

¿Qué hacer en los primeros minutos tras un ciberataque?

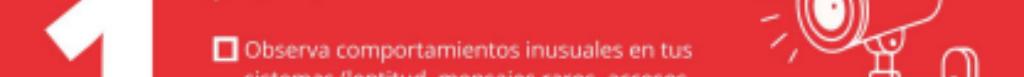
En 10 pasos

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

JTener esta infografía siempre a mano!



## Detecta la amenaza

1

- ⌚ Vigilar que todo funciona correctamente

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



## Desconecta y aísla

2

- ⌚ 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.

## Evaluá el alcance

- ⌚ Saber qué ha pasado y a quién ha afectado



3

- 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.

## 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.



## Comunica con calma

- ⌚ Informar sin generar pánico



5

- 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.

## Notifica a los expertos

- ⌚ Obtener ayuda profesional y cumplir la ley



6

- 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.

## 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.

7

## Analiza el malware (si puedes)

- ⌚ Saber con qué estás lidiando

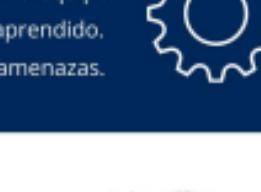


8

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

## Restaura desde copias de seguridad

- ⌚ Recuperar la normalidad sin arrastrar el problema



9

## Aprende y mejora

- ⌚ Aprender del incidente y fortalecer tu defensa



10

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