

GUÍA PRÁCTICA · GESTIÓN DE CRISIS

Crisis de seguridad: las *primeras 24 horas.*

Qué debe estar decidido antes de que ocurra.

MIGUEL ÁNGEL OLMEDA MORENO

SEGURIDAD CORPORATIVA

No falla la alarma. Falla lo que *viene después.*

- ¿Quién decide?
- ¿A quién se avisa?
- ¿Qué se protege primero?
- ¿Qué se conserva?
- ¿Quién comunica?

Si nadie sabe responder a estas cinco preguntas, la crisis se improvisa.

Cuatro tiempos, un *orden.*

Secuencia orientativa: ajústala a cada incidente.

1

Inmediato

Proteger a las personas y activar el mando único.

2

Primeras horas

Asegurar el escenario y preservar las pruebas.

3

Mismo día

Avisar a las autoridades, evaluar si hay brecha de datos y informar a la plantilla.

4

Hasta 24 horas

Informar a clientes y proveedores, y registrar lo decidido.

Una persona decide. Las demás *ejecutan.*

Autoridad real, no solo un cargo en el organigrama.

Operaciones

Estabilizar y garantizar la continuidad.

Comunicación

Mensajes y portavoz único.

Jurídico

Obligaciones y relación con autoridades.

Recursos humanos

Personas afectadas y plantilla.

Tecnología

Sistemas, accesos y registros.

Suplente

Quien decide si el responsable no está.

Primero las personas, no averiguar *quién ha sido.*

1 · Personas

Si hay riesgo para trabajadores, visitantes o instalaciones: cortar el acceso, evacuar si procede y garantizar asistencia.

2 · Escenario

Asegurar la zona y estabilizar la operación.

3 · Pruebas

Conservarlas antes de limpiar, reparar o reiniciar.

4 · Comunicación

Avisar a quien corresponde, en el orden y con el mensaje previstos.

Conservar bien: lo que *sí* y lo que no.

Una prueba destruida por buena intención no se recupera.

SÍ

- ✓ Custodiar las grabaciones relevantes
- ✓ Anotar hora, qué se ha tocado y quién
- ✓ Dejar intactas las cerraduras forzadas
- ✓ Limitar quién accede a las imágenes

NO

- ✗ Borrar vídeos para «limpiar»
- ✗ Reiniciar sistemas o equipos
- ✗ Reenviar capturas por mensajería
- ✗ Guardar todo indefinidamente

Conservar las pruebas no es guardar todas las grabaciones: se custodia lo relevante y el resto sigue su plazo.

Cuatro plazos que conviene tener *presentes.*

Inmediato	Comunicar a las Fuerzas y Cuerpos de Seguridad los hechos delictivos conocidos (deber de la seguridad privada).
72 horas	Notificar a la AEPD una brecha de datos personales, cuando proceda, sin dilación indebida y si es posible en ese plazo.
72 horas	Poner a disposición de la autoridad las grabaciones relacionadas con un delito, según indica la AEPD.
1 mes	Plazo general máximo de conservación de imágenes de videovigilancia.

Orientativo. Confirma cada caso con asesoría jurídica y con el delegado de protección de datos.

Tres mensajes, *preparados* de antemano.

Ni contarlo todo ni callar: quién habla, qué se dice y cuándo.

Empleados

Qué ha pasado, qué se les pide y quién les informará.

Clientes y proveedores

Impacto en el servicio y próximos pasos.

Autoridades y medios

Hechos verificados y un único portavoz.

La verdad, lo verificable y lo necesario.

Llama a tu responsable de seguridad un martes a las *seis de la tarde.*

- ¿Quién decide?
- ¿A quién avisa?
- ¿Dónde están las llaves de emergencia?
- ¿Qué grabaciones se preservan?
- ¿Quién se encarga de la comunicación?
- ¿El teléfono de guardia sigue siendo el correcto?

Si la respuesta es «ya lo veremos», hay trabajo por delante.

Si no se ha ensayado, tienes un documento, no un *plan.*

1
Mando único y suplente designados

2
Contactos de emergencia verificados

3
Procedimiento de preservación de pruebas

4
Tres mensajes base redactados

5
Responsable de notificaciones legales

6
Ensayo al menos una vez al año

¿Cuánto hace que tu empresa no ensaya una crisis de seguridad de verdad?