Fuga o exposición de datos

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Responsables de TI, de datos, legal y gerencia.

Qué hacer cuando información personal o confidencial queda expuesta, fue copiada sin autorización o aparece publicada. El objetivo es cerrar la exposición, saber con precisión qué se filtró y avisar con honestidad a los afectados.

Señales de que está ocurriendo

- Base de datos, respaldo o carpeta accesible desde internet sin contraseña.
- Datos de la organización a la venta o publicados en un foro.
- Aviso de un investigador, cliente o periodista sobre información expuesta.
- Descargas o consultas masivas inusuales en un sistema interno.
- Dispositivo extraviado o robado que contenía información sin cifrar.

Qué tan grave es

Crítica	Datos sensibles de muchas personas (salud, financieros, menores) o ya publicados.
Alta	Datos personales o credenciales expuestos, sin confirmar su publicación.
Media	Información interna no sensible o exposición breve sin evidencia de acceso.

Primera hora

- [ ] **1.** Cierra el acceso: quita el recurso de internet o restringe sus permisos.
- [ ] **2.** No borres nada: conserva el estado y los registros de acceso del recurso expuesto.
- [ ] **3.** Cambia las contraseñas y llaves que aparecen dentro de los datos expuestos.
- [ ] **4.** Guarda evidencia de la publicación (captura, dirección, fecha) si los datos están en línea.
- [ ] **5.** Convoca a TI, legal y gerencia; define quién toma las decisiones.
- [ ] **6.** Empieza el inventario: qué datos, de cuántas personas y de qué fechas.

Preparación (antes del incidente)

- Mantén un inventario de qué datos personales guardas y dónde.
- Guarda sólo lo necesario y borra lo que ya no se usa.
- Cifra los datos en reposo y los dispositivos portátiles.
- Revisa periódicamente qué recursos de nube son públicos.
- Ten redactada una plantilla de aviso a personas afectadas.

Detección y análisis

- Confirma que los datos son auténticos y de qué sistema provienen.
- Determina la ventana de exposición: desde cuándo y hasta cuándo.
- Revisa los registros para saber si alguien accedió y qué se llevó.
- Clasifica los datos: identificación, contacto, financieros, salud, credenciales.

Contención

- Revoca accesos, llaves de API y tokens relacionados.
- Solicita el retiro del contenido al sitio o plataforma donde esté publicado.
- Fuerza el cambio de contraseña si se expusieron credenciales de usuarios.

Erradicación

- Corrige la causa: configuración, vulnerabilidad o cuenta comprometida.
- Busca la misma falla en sistemas similares.
- Pide a los buscadores retirar las copias en caché.

Recuperación

- Restablece el servicio con los controles corregidos y verificados.
- Vigila el uso indebido de los datos: fraudes, suplantación, phishing dirigido.
- Ofrece a los afectados un canal de consulta y orientación concreta.

Lecciones aprendidas

- Documenta causa, alcance y decisiones, con fechas.
- Reduce los datos almacenados que no eran necesarios.
- Agrega la revisión de exposición a los controles periódicos.

Evidencia que debes conservar

- Registros de acceso del recurso expuesto.
- Copia o muestra de los datos filtrados, resguardada con acceso restringido.
- Capturas de la publicación, con dirección y fecha.
- Comunicaciones recibidas de terceros sobre la fuga.

Qué no hacer

- Negar o minimizar la fuga antes de conocer el alcance.
- Borrar el recurso expuesto sin haber guardado los registros.
- Avisar a los afectados con información vaga o sin indicar qué hacer.
- Negociar con quien ofrece “devolver” los datos.

A quién avisar

- Personas afectadas: qué datos, desde cuándo, qué riesgo tienen y qué deben hacer.
- Gerencia y asesoría legal, para evaluar obligaciones contractuales y regulatorias.
- Regulador de tu sector, si aplica.
- Ministerio Público, si hubo acceso ilícito.
- cert.gt, para orientación y coordinación.

Cuándo dar por cerrado el incidente

- La exposición está cerrada y verificada desde fuera de la red.
- El alcance está documentado: datos, personas y fechas.
- Los afectados fueron notificados.
- La causa raíz está corregida en todos los sistemas similares.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).