PLANTILLA DE RESPUESTA ANTE BRECHAS DE DATOS (RGPD)

a

PRIVALEX

guide

LO PRIMERO ES LO PRIMERO...

Una brecha de datos es la peor pesadilla de cualquier empresa. Según el RGPD, debes:

✓ Detectar y evaluar las brechas con rapidez.
✓ Notificar a la autoridad de control en un plazo de 72 horas si la brecha supone un riesgo para las personas.
✓ Comunicar la brecha a los usuarios afectados si el riesgo es alto.

Esta plantilla te ofrece una estructura lista para usar para documentar, escalar y gestionar brechas de seguridad.

1 IDENTIFICACIÓN DEL INCIDENTE E INFORME INICIAL

Registro del incidente (plantilla):

- **Fecha/hora de detección:** *Indicar fecha y hora*
- **Reportado por:** *Nombre / Departamento*
- **Cómo se detectó:** *Sistema de monitorización, aviso de un empleado, notificación de un cliente, etc.*
- **Descripción del incidente:** *Breve explicación de lo ocurrido*
- **Sistemas/datos afectados:** *por ejemplo, CRM, correo electrónico, base de datos de pagos*

2 CONTENCIÓN Y MITIGACIÓN

Lista de verificación:

- [ ] Aislar los sistemas afectados.
- [ ] Desactivar cuentas o puntos de acceso comprometidos.
- [ ] Conservar las evidencias (registros, capturas de pantalla, alertas).
- [ ] Involucrar a IT/seguridad para confirmar el alcance del incidente.

Nota: ***Describe las medidas inmediatas adoptadas para detener o reducir el impacto.***

3

EVALUACIÓN DE LA BRECHA

Preguntas a responder:

¿Qué tipo de datos personales están involucrados?

¿Cuántos interesados se han visto afectados?

¿Se trata de datos sensibles?

¿Los datos están cifrados u protegidos de otro modo?

¿Cuáles son las posibles consecuencias para las personas?

(robo de identidad, pérdidas económicas, daño reputacional)

NIVEL DE RIESGO *(marcar una opción):*

☐ BAJO
Es poco probable que el incidente cause daños a las personas. Los datos eran limitados, estaban bien protegidos (por ejemplo, cifrados) o el incidente se contuvo rápidamente, sin un impacto real previsto para los interesados.

☐ MEDIO
El incidente podría causar molestias o un perjuicio limitado a las personas. Los datos son personales pero no especialmente sensibles, o las medidas de mitigación reducen la probabilidad de un impacto grave.

☐ ALTO
Es probable que el incidente cause un perjuicio significativo a las personas, como robo de identidad, pérdidas económicas o un daño reputacional grave. Hay datos sensibles implicados o los datos han quedado expuestos sin una protección eficaz.

DECISIÓN SOBRE LA NOTIFICACIÓN (REGLA DE LAS 72 HORAS)

1.

¿Notificar a la autoridad de control?

☐ Sí ☐ No

Obligatorio si la brecha puede suponer un riesgo para los derechos y libertades de las personas. La notificación debe realizarse en un plazo máximo de 72 horas desde que se tenga conocimiento de la brecha.

2.

¿Notificar a los interesados?

☐ Sí ☐ No

Obligatorio si la brecha afecta directamente a las personas y a sus derechos de protección de datos. La comunicación debe realizarse sin dilación indebida y en un lenguaje claro y sencillo.

Nivel de riesgo:

BAJO
No es necesaria ninguna notificación

MEDIO
Solo notificación a la autoridad de control

ALTO
Notificación a la autoridad de control y a los interesados

PLANTILLA DE NOTIFICACIÓN

A LA AUTORIDAD DE CONTROL

- ✓ Naturaleza de la brecha
- ✓ Categorías y número aproximado de interesados afectados
- ✓ Categorías y número aproximado de registros de datos personales afectados
- ✓ Consecuencias probables de la brecha
- ✓ Medidas adoptadas o propuestas para abordar y mitigar la brecha
- ✓ Datos de contacto del DPO o de la persona responsable

A LOS INTERESADOS

Asunto: *Aviso importante sobre sus datos personales*

Mensaje: *Hemos identificado recientemente un incidente de seguridad que puede haber afectado a sus datos personales. La información implicada fue *describir las categorías de datos*.*

*Hemos adoptado medidas inmediatas para contener el incidente y evitar que vuelva a producirse, incluyendo *describir las medidas adoptadas*.*

*Qué puede hacer usted: *por ejemplo, restablecer su contraseña, vigilar sus cuentas*.*

*Si tiene alguna pregunta, puede ponerse en contacto con nuestro Delegado de Protección de Datos en *correo electrónico / contacto del DPO*.*

Lamentamos sinceramente las molestias ocasionadas y nos tomamos muy en serio nuestra responsabilidad de proteger sus datos personales.

REVISIÓN POSTERIOR AL INCIDENTE

Campos de la plantilla:

Análisis de la causa principal: *Explicar*

Lecciones aprendidas: *Indicar los principales aprendizajes*

Acciones correctivas: *Actualizar políticas, formación o controles técnicos*

Responsable: *Persona o equipo asignado*

Plazo para las acciones: *Indicar fecha*

LISTA DE VERIFICACIÓN RÁPIDA

- [ ] Detectar y documentar la brecha
- [ ] Contener y mitigar los daños
- [ ] Evaluar el riesgo para las personas
- [ ] Notificar a la autoridad de control en un plazo de 72 horas (si procede)
- [ ] Notificar a los interesados sin dilación indebida (si el riesgo es alto)
- [ ] Documentar todo (incluso si no es necesaria ninguna notificación)
- [ ] Realizar una revisión posterior al incidente

PRÓXIMOS PASOS

La mayoría de las empresas pierde un tiempo valioso durante una brecha porque no tiene claro quién debe hacer qué. Contar con una plantilla clara evita el pánico y demuestra a los reguladores que el cumplimiento se toma en serio.

No esperes a que ocurra una brecha. Contacta con nosotros para obtener un plan de respuesta ante brechas personalizado y alineado con tu sector y tus riesgos.

CONTÁCTANOS

PRIVALEX