Plan de Respuesta a Brechas de Datos

Plantilla para gestionar incidentes de seguridad que involucren datos personales. La Ley 21.719 exige notificación a la autoridad competente dentro de **72 horas** desde que se detecta la brecha.

Elaborado por Ethoz · ethoz.cl · Complete los campos [en corchetes] con datos de su establecimiento

---

1 Equipo de Respuesta a Incidentes

Rol	Nombre	Teléfono	Correo
Responsable principal (DPO)	[Nombre]	[Teléfono]	[Email]
Director(a)	[Nombre]	[Teléfono]	[Email]
Encargado TI / Proveedor	[Nombre]	[Teléfono]	[Email]
Asesor legal	[Nombre / Firma]	[Teléfono]	[Email]
Comunicaciones	[Nombre]	[Teléfono]	[Email]

2 Clasificación de Brechas

LEVE Notificación interna. Sin obligación de notificar a autoridad si no hay riesgo significativo.

Acceso no autorizado a datos básicos de identificación por un tiempo muy limitado, sin evidencia de exfiltración. Ej: un funcionario accede por error a datos de otro curso. Contención posible en horas.

GRAVE Notificación a autoridad en 72 horas. Posible comunicación a afectados.

Acceso no autorizado a datos académicos o de contacto de un grupo de alumnos o apoderados. Posible exfiltración de datos. Ej: ataque de phishing que compromete credenciales de un docente. Riesgo de discriminación o fraude.

GRAVÍSIMA Notificación urgente en 72 horas. Comunicación inmediata a afectados y medios si es masiva.

Exposición masiva de datos sensibles (médicos, judiciales, emocionales) o datos de menores. Ransomware con cifrado de todos los datos. Publicación pública de datos personales. Riesgo de daño físico o psicológico a alumnos.

3 Procedimiento de Notificación en 72 Horas (Art. 30 Ley 21.719)

Hora 0 — Detección y alerta interna

El incidente es detectado por el sistema, un funcionario o un tercero. Se activa inmediatamente el equipo de respuesta. Se documenta la hora exacta de detección. CRÍTICO: El plazo de 72 horas comienza desde este momento.

H+2 — Evaluación inicial

El DPO y el encargado TI evalúan el alcance preliminar: qué datos están comprometidos, cuántos titulares afectados, si la brecha está activa o contenida. Se clasifica el nivel de gravedad.

H+4 — Contención

Se toman medidas para detener la brecha: desconexión de sistemas afectados, revocación de credenciales comprometidas, bloqueo de accesos. Se preservan evidencias forenses (no eliminar logs).

H+12 — Evaluación de impacto

Análisis detallado: categorías de datos afectados, número de titulares, probabilidad y gravedad del daño. Determina si es obligatorio notificar a la autoridad y a los afectados.

H+24 — Notificación al Director y Sostenedor

Informe ejecutivo al director y sostenedor con resumen del incidente, medidas tomadas y plan de acción. Si hay menores involucrados, se evalúa notificación a SENAME o tribunales.

H+48 — Preparación de notificación a autoridad

Se redacta el reporte oficial usando la plantilla de la sección 7. Se incluye: descripción de la brecha, datos afectados, medidas de contención, riesgos identificados, medidas correctivas.

H+72 — Notificación a la Agencia de Protección de Datos

Envío del reporte oficial a la autoridad competente dentro del plazo legal. Si la Agencia aún no está operativa, se documenta el intento y se notifica en cuanto sea posible. Se guarda acuse de recibo.

4 Evaluación de Impacto

Para determinar la gravedad de la brecha, evalúe los siguientes factores:

Factor	Bajo (1)	Medio (2)	Alto (3)
Tipo de datos	Datos básicos de identificación	Datos académicos, contacto	Datos sensibles, médicos, menores
Número de afectados	Menos de 10 personas	Entre 10 y 100 personas	Más de 100 personas
Daño potencial	Molestia menor, sin consecuencias	Discriminación, impacto reputacional	Daño físico, psicológico o económico grave
Reversibilidad	Totalmente reversible	Parcialmente reversible	Irreversible (datos ya publicados)

Puntaje total 4-6: Leve · 7-9: Grave · 10-12: Gravísima

5 Comunicación a los Afectados

Cuando la brecha represente un alto riesgo para los derechos de los titulares, se les comunicará sin dilación indebida. La comunicación debe incluir:

- Descripción clara de la naturaleza de la brecha (qué ocurrió, cuándo).
- Datos personales afectados (sin entrar en detalles que puedan agravar el riesgo).
- Medidas adoptadas para contener el incidente.
- Recomendaciones para que los afectados protejan sus datos (cambio de contraseñas, alertas de fraude).
- Datos de contacto del DPO para consultas.
- Vías de reclamación disponibles.

6 Documentación y Lecciones Aprendidas

Todo incidente debe quedar documentado en el registro de brechas del establecimiento, independientemente de su gravedad:

Fecha y hora de detección: _____

Fecha y hora de contención: _____

Causa raíz identificada: _____

Sistemas/personas afectadas: _____

Medidas correctivas implementadas: _____

Medidas preventivas para evitar recurrencia: _____

¿Se notificó a la autoridad? Fecha: _____

¿Se notificó a los afectados? Fecha: _____

Responsable del cierre del incidente: _____

7 Plantilla de Reporte a la Autoridad

NOTIFICACIÓN DE BRECHA DE SEGURIDAD
Conforme Art. 30, Ley 21.719

1. Identificación del responsable:
[Nombre del establecimiento], RUT [___], DPO: [Nombre], Email: [___], Tel: [___]

2. Fecha y hora de detección de la brecha:
[DD/MM/AAAA] a las [HH:MM]

3. Descripción de la brecha:
[Descripción objetiva: qué ocurrió, cómo se detectó, sistemas involucrados]

4. Categorías de datos personales afectados:
[Ej: datos de identificación de alumnos, datos académicos, datos de salud]

5. Número aproximado de titulares afectados:
[Número estimado o exacto]

6. Consecuencias probables de la brecha:
[Riesgos identificados para los titulares: discriminación, fraude, daño físico, etc.]

7. Medidas adoptadas para hacer frente a la brecha:
[Medidas de contención, corrección y prevención implementadas]

8. ¿Se ha comunicado a los titulares afectados?
□ Sí, con fecha: [___] □ No (justificación: [___])

9. Firma y fecha:

_____