

Protocolo ante brechas de seguridad de datos personales

Qué hacer cuando se pierden, se filtran o se usan sin autorización datos de residentes, familias o trabajadores: contener, avisar, evaluar, comunicar, registrar y corregir. Normativa de referencia: Ley 21.719 (Ley 19.628 modificada, artículos 14 quinquies, 14 sexies y 15 bis); Decreto 20 de 2021 del Ministerio de Salud, artículos 29 letra e) y 30.

Establecimiento	Código	Versión	Fecha de aprobación	Próxima revisión
	MACA-DAT-08			

Documento referencial de MACA, basado en la normativa chilena vigente. Adáptalo y válidalo con tu director(a) técnico(a) y tu asesor legal antes de usarlo.

1. Objetivo y alcance

Actuar rápido y en orden ante una brecha de seguridad de datos personales, para limitar el daño a las personas afectadas, hacer las comunicaciones que exige la ley y evitar que se repita. Aplica al personal, practicantes, voluntarios y proveedores que tratan datos por encargo de la residencia, en papel y en formato digital: carpetas, registros, computadores, celulares, correo, mensajería, sistemas y respaldos.

2. Responsables

- **Coordinador(a) de protección de datos (_____):** coordina la respuesta, evalúa el riesgo, prepara las comunicaciones y lleva el registro de incidentes.
- **Dirección de la residencia:** aprueba las comunicaciones a la Agencia y a las personas afectadas, y asigna los recursos para corregir.
- **Todo el personal:** avisa de inmediato cualquier brecha o sospecha. No la oculta ni intenta resolverla solo.
- **Proveedores que tratan datos por encargo:** la Ley 21.719 los obliga a reportar a la residencia las brechas que detecten. El proveedor de informática o de software ayuda a contenerlas y entrega la información técnica que se le pida.

3. Qué es una brecha de seguridad

Es cualquier falla de seguridad en que datos personales se pierden, se destruyen, se alteran, se filtran o quedan al alcance de alguien que no debía verlos, ya sea por un error, un robo o un ataque. Puede ocurrir en papel o en formato digital. Algunos ejemplos:

En papel	En formato digital
Se pierde una carpeta personal o queda olvidada en un vehículo, un hospital o una sala de espera.	Roban o se pierde un celular con fotos, chats o contactos de residentes.
Una lista con diagnósticos o medicamentos queda pegada en un pasillo, a la vista de las visitas.	Un correo con información de un residente se envía a la persona equivocada.
Documentos con datos se botan a la basura sin triturar.	Un virus o un secuestro de datos bloquea el computador o el sistema y pide un rescate.
Alguien sin autorización revisa, fotografía o fotocopia una carpeta.	Un trabajador entra al sistema con la clave de otro o revisa fichas que no le corresponden.
Un informe de salud se entrega a un familiar que no está autorizado.	Se filtra por WhatsApp una foto o un dato clínico de un residente fuera del equipo.
Una inundación o un incendio destruye el archivo.	Un proveedor avisa que su sistema sufrió un ataque.

Ante la duda, trátalo como brecha y avisa. Recomendamos que avisar a tiempo nunca sea motivo de sanción: lo grave es ocultar el incidente.

4. Qué hacer, paso a paso

1. **Contén el daño.** Recupera la carpeta o el equipo si puedes, pide a quien recibió un correo o mensaje por error que lo borre y lo confirme por escrito, cambia las claves comprometidas y bloquea o borra a distancia el celular perdido.
2. Si es un virus o un secuestro de datos, **desconecta el equipo de internet y de la red**, no pagues rescates y llama de inmediato al proveedor de informática.
3. **Avisa de inmediato al coordinador(a) de protección de datos** (_____, teléfono _____), aunque no tengas todos los detalles. Fuera de horario, avisa al encargado(a) de turno y a la dirección.
4. **No borres evidencia.** Guarda los mensajes, correos y capturas de pantalla que ayuden a entender qué pasó.
5. **Evalúa la brecha** con las preguntas de la sección 5: qué datos, de cuántas personas, si hay datos sensibles y qué riesgo hay para ellas.
6. **Comunica** la brecha a la Agencia de Protección de Datos Personales si hay un riesgo razonable para las personas y, si afecta datos de salud u otros datos sensibles, también a cada persona afectada (sección 6).
7. Si hubo un robo u otro delito, **haz la denuncia** en Carabineros (133) o en la Policía de Investigaciones.
8. **Registra** la brecha en el formulario de reporte y en el registro de incidentes (secciones 8 y 9).
9. **Aprende y corrige** para que no vuelva a pasar (sección 7).

Completa estos contactos y déjalos a mano del equipo, junto a los teléfonos de emergencia.

Contacto	Nombre	Teléfono o canal
Coordinador(a) de protección de datos		
Reemplazante		
Director(a) técnico(a)		
Asesor(a) legal		
Proveedor de informática o software		
Agencia de Protección de Datos Personales		
Carabineros		133

5. Cómo evaluar la brecha

Responde estas preguntas lo antes posible. Te ayudan a medir el riesgo para las personas y a decidir qué comunicar.

- **¿Qué datos se vieron afectados?** Identificación, contacto, salud, imágenes, datos bancarios o claves.
- **¿De cuántas personas y quiénes son?** Residentes, familias, trabajadores o postulantes.
- **¿Hay datos sensibles?** Los datos de salud son datos sensibles: una brecha con información clínica es de mayor riesgo.
- **¿Quién pudo verlos?** No es lo mismo un colega que devolvió el documento sin leerlo que un desconocido o una publicación en internet.
- **¿Estaban protegidos?** Un celular con clave o un archivo cifrado reduce el riesgo.
- **¿Qué daño puede causar?** Discriminación, vergüenza, fraude, suplantación de identidad, maltrato o una interrupción del cuidado.
- **¿Sigue ocurriendo?** Si la brecha no está contenida, vuelve al paso 1.

Riesgo	Ejemplos	Qué hacer
Bajo	Correo con datos de contacto enviado a un colega de la residencia, que lo borró de inmediato.	Sin riesgo razonable para las personas: registra la brecha y corrige la causa.

Riesgo	Ejemplos	Qué hacer
Medio	Carpeta administrativa extraviada y recuperada al día siguiente, sin señales de que alguien la revisó.	Registra, corrige y define con tu asesor si hay un riesgo razonable. Si lo hay, reporta a la Agencia.
Alto	Datos clínicos o fotos difundidos, celular sin clave robado o secuestro de datos del sistema.	Reporta sin demora a la Agencia y comunica a cada persona afectada o a su representante. Registra y corrige.

Esta tabla es una orientación. La decisión la toma la dirección con el coordinador(a) de protección de datos y, si hay dudas, con su asesor. Ante la duda, reporta: omitir deliberadamente la comunicación de una brecha es una infracción gravísima de la Ley 21.719.

6. Comunicar la brecha

Desde el 1 de diciembre de 2026, la Ley 21.719 exige:

- **Reportar a la Agencia de Protección de Datos Personales**, por los medios más rápidos posibles y sin demoras indebidas, toda brecha que signifique un **riesgo razonable para los derechos de las personas**. Usa el canal que la Agencia tenga habilitado y anótalo en la tabla de contactos.
- **Comunicar a cada persona afectada**, o a su representante, cuando la brecha afecte **datos sensibles, como los de salud, o datos económicos, financieros o bancarios**. Se hace en lenguaje claro y sencillo, indicando qué datos se afectaron, sus posibles consecuencias y las medidas tomadas. Si no es posible avisar a cada persona, la ley exige publicar un aviso en un medio de comunicación masivo de alcance nacional.
- **Registrar las comunicaciones**, con la naturaleza de la brecha, sus efectos, el tipo de datos, el número aproximado de personas afectadas y las medidas tomadas para gestionarla y evitar que se repita.

Recomendamos que el reporte a la Agencia indique qué pasó, cuándo ocurrió y cuándo se detectó; qué datos y cuántas personas se afectaron; sus posibles consecuencias; las medidas tomadas y por tomar, y un contacto de la residencia.

Con las personas afectadas, si es posible, habla primero en persona o por teléfono. Si el residente no puede comprender la información, comunícala a su representante. Explícales qué pueden hacer para protegerse, por ejemplo, cambiar una clave o desconfiar de llamadas que pidan datos.

No esperes a tener toda la información para comunicar a la Agencia: informa lo que sabes y completa después. Guarda copia de cada comunicación, con fecha y hora.

7. Aprender y corregir

- Dentro de _____ días, el coordinador(a) de protección de datos y la dirección revisan qué pasó, por qué pasó y qué se debe cambiar.
- Corrige la causa: ajusta permisos, cambia procesos, repara equipos, refuerza la capacitación o revisa el contrato con el proveedor.
- Comparte lo aprendido con el equipo, sin exponer a las personas involucradas.
- Revisa este protocolo al menos una vez al año y después de cada brecha de riesgo medio o alto.

8. Formulario de reporte de brecha

Quien detecta la brecha, o el coordinador(a) de protección de datos, completa este formulario apenas pueda. Si falta información, anota lo que sepas y complétalo después.

FECHA Y HORA DEL INCIDENTE

FECHA Y HORA EN QUE SE DETECTÓ

QUIÉN REPORTA (NOMBRE Y CARGO)

TELÉFONO

LUGAR, EQUIPO O SISTEMA AFECTADO

QUÉ PASÓ

DATOS AFECTADOS

N° APROXIMADO DE PERSONAS

MEDIDAS TOMADAS PARA CONTENER LA BRECHA Y EVITAR QUE SE REPITA

COMUNICACIÓN A LA AGENCIA (FECHA, HORA Y MEDIO)

COMUNICACIÓN A LOS AFECTADOS (FECHA Y MEDIO)

DENUNCIA, SI HUBO DELITO (INSTITUCIÓN Y NÚMERO)

Soporte: ☐ Papel ☐ Computador o sistema ☐ Celular ☐ Correo o mensajería ☐ Proveedor

Tipo: ☐ Pérdida o robo ☐ Envío por error ☐ Acceso indebido ☐ Virus o secuestro de datos ☐ Otro

Personas afectadas: ☐ Residentes ☐ Familias ☐ Trabajadores ☐ Otras

¿Hay datos de salud u otros datos sensibles? ☐ Sí ☐ No ☐ No se sabe

Nivel de riesgo: ☐ Bajo ☐ Medio ☐ Alto

Quien reporta

Coordinador(a) de protección de datos

Fecha

9. Registro de incidentes

La Ley 21.719 exige registrar las brechas que se comunican. Recomendamos registrar **todas**, aunque no se reporten a la Agencia: el registro demuestra que la residencia actúa con cuidado y ayuda a detectar problemas que se repiten.

N°	Fecha	Qué pasó y sus efectos	Datos y N° de personas afectadas	Riesgo	Medidas tomadas	¿Se comunicó? Agencia / afectados	Responsable

Aprobación y control de cambios

	Nombre y cargo	Firma	Fecha
Elaborado por			
Revisado por			
Aprobado por (dirección técnica)			