



UNIDAD TÉCNICO-PEDAGÓGICA
CONVIVENCIA ESCOLAR
SEDE LONDRES

PROTOCOLO DE ACCIÓN ANTE VULNERACION DE DATOS PERSONALES DE ESTUDIANTES.

OBJETIVO Y MARCO REGULATORIO

Este protocolo regula la recopilación, almacenamiento, uso, entrega y resguardo de la información académica, administrativa y de convivencia de los estudiantes matriculados en las distintas sedes del Instituto Tabancura. Se fundamenta en la Ley N° 19.628 sobre Protección de los Datos Personales, el Decreto Supremo de Educación para la Modalidad de Adultos, y los principios de confidencialidad de la Superintendencia de Educación.

La [Ley 19.628](#) sobre protección de la vida privada regula en Chile cómo los organismos públicos y los particulares deben tratar los datos personales.

Esta Ley:

- . Es la normativa general en Chile sobre el manejo y resguardo de la información personal.**

- Define qué son los datos personales y los datos sensibles (como origen racial, estado de salud u opción política).
- Exige que la recopilación y uso de datos tenga un fin lícito y, por regla general, requiera el consentimiento de la persona.

Un Protocolo de Acción ante la Vulneración de Datos Personales en un establecimiento educacional es un conjunto de pasos críticos para contener la filtración, mitigar los daños y cumplir con las normativas legales.

Cuando el origen de la filtración es un error humano (ej. envío masivo por error de un Excel con notas, diagnósticos NEE, RUN o datos socioeconómicos, o dejar carpetas sin resguardo), el enfoque debe centrarse en la contención operativa instantánea, transparencia legal y corrección de procesos administrativos.

En el marco regulatorio de nuestro país se estructura el siguiente protocolo:

1: Contención Inmediata y Mitigación Técnica:

- **Revocación y Bloqueo del Envío:** Si el error ocurrió vía correo electrónico institucional o plataformas como *Drive*, se debe intentar anular el envío (opción

deshacer de Outlook/Gmail) o revocar los accesos y permisos del enlace compartido de inmediato.

- . Solicitud de Destrucción: Enviar una comunicación urgente a los receptores erróneos solicitando la eliminación definitiva del archivo, pidiendo expresamente no reenviar, descargar ni difundir la información por Ley 19.628 y 21.719.**
- . Identificación del personal involucrado: Entrevistar al funcionario que cometió el error sin un tono punitivo, sino con el fin de mapear exactamente *qué* información se envió, a *quiénes* y a través de *qué* medio institucional.**

2: Clasificación y Reporte Obligatorio a las Autoridades
Bajo la Ley 21.719, las brechas que involucren datos sensibles o de menores de 14 años gatillan obligaciones críticas:

- a) Evaluación ante la Superintendencia de Educación:**
Si la filtración vulnera la dignidad o la vida privada de los alumnos (ej. historial psicopedagógico o vulnerabilidad socioeconómica), debe dejarse constancia del hecho en.
- b) Comunicación e Impacto en la Comunidad Escolar**

Notificación Transparente a los Apoderados: Si el error expuso datos sensibles de estudiantes menores de edad, es obligatorio notificar a los padres o tutores legales. La comunicación debe ser formal, empática y detallar:

- 1. Qué datos específicos fueron expuestos.**
- 2. Cuál fue la causa (error administrativo).**
- 3. Qué acciones concretas tomó el colegio para bloquear la información.**

c) Activación de Convivencia Escolar: El error humano puede detonar dinámicas de acoso o discriminación si se filtraron notas o diagnósticos médicos. El equipo de Convivencia Escolar debe activar de inmediato los protocolos de apoyo socioemocional y prevención del *cyberbullying*.

3. Post-Incidente y Medidas Correctivas Administrativas

Al ser un error humano, la solución de fondo no es informática, sino procedimental y cultural:

- . Centralización de Canales:** Eliminar el uso de medios informales (como grupos de WhatsApp de profesores o almacenamiento en cuentas personales de Drive) para alojar datos de alumnos. Obligar el uso exclusivo

de la plataforma de gestión académica contratada por el colegio.

- . Principio de Privacidad por Defecto y Control de Roles: Restringir los accesos dentro del personal escolar. Un docente solo debe tener visibilidad de los datos del curso que imparte; las secretarías o directivos deben contar con roles diferenciados para evitar descargas masivas de bases de datos de matrículas por error.**
- . Plan de Capacitación Obligatoria: Desarrollar talleres para todo el personal (docente, administrativo y directivo) sobre el manejo técnico de correos (uso correcto de la casilla CCO - copia oculta), la Ley de Protección de Datos Personales, y la importancia del deber de confidencialidad.**

Levantar un Registro de Actividades de Tratamiento (RAT), diseñar plantillas oficiales de consentimiento informado para los apoderados y evaluar la designación formal de un Encargado de Protección de Datos (DPO) en el colegio.

DENUNCIAS QUE INVOLUCREN A FUNCIONARIOS

Cuando una denuncia identifique a un docente, asistente, profesional, directivo o trabajador como eventual responsable, la institución deberá separar dos cuestiones: la existencia o no de una vulneración de datos y, la eventual responsabilidad laboral o disciplinaria de la persona.

La sola denuncia no constituye prueba de responsabilidad, lo que implica que el funcionario deberá ser tratado con respeto y tendrá derecho a conocer los hechos que se le imputen en la medida que ello sea compatible con la protección de los involucrados y con la integridad de la investigación.

MEDIDAS PREVENTIVAS TEMPORALES

- . Restricción temporal de acceso a determinados sistemas, si existe riesgo objetivo**
- . Preservación de registros electrónicos**
- . Separación funcional respecto del tratamiento de datos específicos, cuando exista un motivo necesario**
- . Medidas de resguardo para estudiantes o terceros afectados**
- . Evitar sanciones anticipadas antes de concluir el procedimiento correspondiente**

FASE DE INVESTIGACIÓN DEL HECHO.

El objetivo principal es detener la filtración y asegurar los sistemas afectados.

Una vez conocida la denuncia de filtración, se procede según el siguiente protocolo:

- a) Identificación del incidente: Determinar el tipo de brecha (acceso no autorizado, pérdida de dispositivos, ciberataque, envío erróneo de correos masivos con notas/RUT/historiales médicos)**
- b) Aislamiento de sistemas: Desconectar los servidores o plataformas comprometidas de la red de internet si se trata de un ataque informático**
- c) Bloqueo de accesos: Cambiar credenciales de forma masiva, revocar accesos temporales y suspender cuentas bajo sospecha.**
- d) Preservación de evidencia: Registrar logs de auditoría, capturas de pantalla y bitácoras técnicas para futuras investigaciones legales o forenses.**
- e) Clasificación de los datos: Identificar si la filtración incluye datos sensibles de menores (salud, psicopedagógicos, situación socioeconómica, direcciones o teléfonos).**
- f) Notificación a la comunidad escolar: Comunicar de forma transparente a los padres, madres y apoderados afectados. La comunicación debe ser clara, empática y**

especificar qué datos se vieron comprometidos y qué medidas se están tomando.

- g) Apoyo psicoeducativo: Activar al equipo de convivencia escolar si la filtración genera situaciones de acoso (*cyberbullying*) o vulnerabilidad emocional entre los estudiantes.**
- h) Entrevistar al funcionario que cometió el error sin un tono punitivo, sino con el fin de mapear exactamente *qué* información se envió, a *quiénes* y a través de *qué* medio institucional.**
- i) Entrevistar a los estudiantes del mismo y de otros cursos ,con el objetivo de recabar la mayor información posible sobre la situación ocurrida.**
- j) Concluida la revisión, se emitirá un informe interno que distinga claramente entre:**
 - 1) no se acredita vulneración;**
 - 2) se acredita incumplimiento interno sin exposición relevante;**
 - 3) se acredita tratamiento indebido;**
 - 4) se acredita brecha de seguridad;**
- k) Informar a la persona demandante**

CIERRE

SI SE ACREDITA UNA INFRACCIÓN, podrán aplicarse las medidas que correspondan conforme al contrato de trabajo, reglamento interno, normativa educacional y legislación aplicable vigente.

SI NO SE ACREDITA, deberá dejarse constancia del resultado y evitar la difusión innecesaria de la denuncia.

DENUNCIAS QUE INVOLUCREN A ESTUDIANTES O APODERADOS

Cuando el denunciante o afectado sea estudiante, el Instituto deberá considerar su edad, grado de comprensión, interés superior y necesidad de protección, evitando exposiciones innecesarias.

Los apoderados serán informados cuando corresponda según la naturaleza del hecho, las obligaciones legales, el reglamento interno y las necesidades de protección del estudiante.

RESPECTO DE LAS REGLAS DE ENTREVISTA

- . Realizar entrevistas en espacio reservado**
- . Evitar preguntas sugestivas o innecesarias**
- . Registrar hechos y expresiones relevantes de manera objetiva**
- . No circular relatos por grupos de mensajería**
- . No confrontar innecesariamente a denunciante y denunciado**
- . Derivar a las instancias de convivencia, protección o autoridad cuando corresponda.**

DE LA PROHIBICIÓN DE DIFUSIÓN INFORMAL

Ningún integrante de la comunidad educativa podrá divulgar por redes sociales, grupos de WhatsApp, correo personal u otros dispositivos de mensajería instantánea, o conversaciones informales, antecedentes de una investigación, fotografías, capturas de pantalla, nombres o documentos que permitan identificar a personas involucradas, salvo que exista fundamento jurídico o instrucción institucional válida.

MEDIDAS DISCIPLINARIAS Y SANCIONES INTERNAS

Las sanciones internas no sustituyen las competencias de las autoridades públicas. La institución aplicará las medidas que correspondan conforme a contratos, reglamento interno, estatutos, normativa laboral y educacional.

Nivel interno orientativo	Ejemplo	Medida posible
Preventivo	Error sin exposición relevante	Orientación/capacitación
Menor	Incumplimiento procedimental sin daño relevante.	Amonestación o medida interna según normativa.
Serio	Acceso indebido, divulgación o reiteración.	Investigación disciplinaria y aplicación medidas conforme al reglamento/contrato.

Muy serio	Divulgación deliberada, datos sensibles o NNA (niños, niñas y adolescents) ocultamiento.	Medidas disciplinarias y una posible y/o eventual derivación a autoridad competente.
------------------	---	---

La calificación interna no sustituye la calificación jurídica que corresponda conforme a la ley. En particular, las categorías de infracciones leves, graves y gravísimas de la Ley regidora, corresponden al régimen legal y no deben confundirse automáticamente con categorías disciplinarias laborales.

