MODELOS DE PREVENCIÓN EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN COLEGIOS: EL DESAFÍO QUE ESTÁ TRANSFORMANDO LA GESTIÓN ESCOLAR

Por Juan Eduardo Estay
Abogado, Especialista en regulación educacional y compliance

1. Introducción: los datos que los colegios tratan sin percibir los riesgos

En los establecimientos educacionales, la información circula de manera constante. Está en plataformas digitales, registros de convivencia, informes psicopedagógicos, emails y múltiples espacios de interacción cotidiana. Pero no toda esa información es equivalente.

Una cosa es una lista de asistencia; otra muy distinta es un informe psicológico, un antecedente familiar o una denuncia de maltrato. Ahí surge una distinción clave, no todos los datos son iguales, y los hay con distintos grados de riesgo.

2. De qué datos hablamos y cuál es la relevancia de su distinción

No toda la información que maneja un establecimiento tiene el mismo nivel de riesgo;

- Dato personal: cualquier información que permite identificar a una persona (nombre, RUT, curso, correo electrónico, etc.). La ley es menos exigente en su tratamiento.

- Dato sensible: información que afecta la esfera íntima o puede generar discriminación o daño si se divulga. La ley estableces exigentes estándares en su tratamiento En el contexto escolar, los datos personales sensibles incluyen: a) evaluaciones psicológicas o psicopedagógicas; b) datos sobre de salud física o mental; c) información familiar o socioeconómica; y d) denuncias de maltrato o abuso.

3. ¿Por qué esto es relevante hoy para los colegios?

La protección de datos dejó de ser una buena práctica y pasó a ser un estándar exigible:

- Ya es fiscalizado y sancionado por la Superintendencia de Educación.
- Será prontamente fiscalizado y sancionado por la Agencia de Protección de Datos (desde el 1 de diciembre de 2026).
- Exige modelos de prevención, no solo cumplimiento formal.

4. Caso concreto en que la Superintendencia de Educación sancionó por infracción en la protección datos personales sensibles.

A modo de ejemplo, la Superintendencia de Educación, mediante la Resolución Exenta N°2020/PA/13/2780, sancionó a un colegio específicamente por la exposición de la privacidad de un estudiante en un contexto de vulneración de derechos.

El hecho sancionado fue: El establecimiento no resguardó la confidencialidad de los antecedentes de un estudiante, permitiendo que información sensible fuera conocida por terceros, lo que afectó su integridad psicológica y su derecho a la vida privada.

La sanción aplicada fue: la privación temporal y parcial del 3% de la subvención general por un periodo de 4 meses.

5. Principios esenciales

La ley establece principios actúan como criterios rectores para la legitimidad en todo tratamiento. No se trata solo de "cumplir la ley", sino hacerlo de forma coherente con la finalidad del tratamiento, respetando la voluntad del titular; y minimizando riesgos:

- Principio de finalidad: los datos personales deben recolectarse y utilizarse para fines específicos, legítimos, previamente informados al titular, sin poder ser usados posteriormente para propósitos distintos o incompatibles.
- Principio de consentimiento constatable e informado: el tratamiento de datos requiere la autorización del titular, la cual debe otorgarse de manera libre, previa e informada, con un conocimiento claro sobre de qué datos se recogen, para qué y cómo serán utilizados.
- Principio de proporcionalidad: solo pueden tratarse los datos estrictamente necesarios para cumplir la finalidad declarada, evitando recopilar o usar información excesiva, irrelevante o desproporcionada respecto del objetivo perseguido.
- Principio de calidad o veracidad de los datos: la información debe ser exacta, actualizada y pertinente.
- Principio de responsabilidad: el responsable del tratamiento debe no solo cumplir la normativa, sino además demostrar la adopción de medidas efectivas para asegurar dicho cumplimiento.

Estos principios, aplicados correctamente, permiten construir un tratamiento de datos legítimo, transparente y respetuoso de los derechos fundamentales.

6. Derechos esenciales: cuando los datos vuelven a las personas

La gestión del tratamiento y protección de información personal se basa en que los datos no pertenecen al colegio, sino a sus titulares. Esto se traduce en derechos concretos que todo titular puede ejercer, los llamados derechos ARCO:

- Acceso: saber qué información existe y cómo se usa
- Rectificación: corregir datos incorrectos
- Cancelación: solicitar su eliminación cuando corresponda
- Oposición: limitar ciertos usos

Incorporar estos derechos busca transformar la relación entre la comunidad educativa, instalando un estándar de mayor transparencia y confianza.

7. Modelo de prevención: qué espera hoy la normativa de un colegio

En la vida cotidiana de un colegio, hay decisiones que parecen menores: reenviar un informe, comentar un caso en una reunión, subir información a una plataforma o compartir antecedentes con otro equipo.

La normativa actual y el nuevo estándar que introduce el modelo de prevención de infracciones obligan a dar un paso más: ya no se trata solo de reaccionar ante un incidente, sino de anticiparlo, ordenarlo y documentarlo, no siendo suficiente el “cuidar datos”, sino demostrar que se previenen riesgos.

8. Cuando el sistema empieza a ordenar la gestión de riesgos

Un componente crucial en la protección tratamiento es la matriz de riesgos, con la que el colegio puede clasificar e identificar riesgos: a) Dónde se concentran los datos más sensibles; b) Quiénes acceden a ellos; c) Qué podría pasar si se filtran; y d) Qué tan probable es que ocurra un incidente.

El modelo de prevención no busca burocratizar la escuela, sino dar coherencia a lo que ya ocurre. En la práctica, se traduce en las siguientes piezas que, integradas, hacen la diferencia:

a) Política y protocolos que establecen reglas claras (qué se usa, para qué y quién accede).
b) Encargado de protección de datos, que articula el sistema, coordina capacitaciones y gestiona incidentes.
c) Capacitación permanente, para que docentes y equipos reconozcan riesgos en su trabajo cotidiano.
d) Canales de reporte, que permitan informar a tiempo y aprender de los errores.

9. El punto más sensible: la convivencia escolar

Este aspecto más relevante es el ámbito de la convivencia escolar, que concentra información de alta sensibilidad: denuncias de maltrato, situaciones de acoso, datos familiares o procesos disciplinarios que requieren un tratamiento especialmente cuidadoso. En estos casos, la confidencialidad deja de ser una recomendación y se convierte en una obligación estricta, que debe reflejarse en:

a) Protocolos de actuación.
b) Resguardo de identidad de los involucrados.
c) Acceso restringido a la información.
d) Reglas claras en el Reglamento Interno de Convivencia Escolar (RICE).

10. Lo que viene: anticipar riesgos y necesidad de implementar desde ya

Mientras la Superintendencia de Educación ya fiscaliza y sanciona el tratamiento de datos personales por colegios, la Agencia de Protección de Datos (que comienza a fiscalizar y sancionar a los colegios el 01/12/2026) introducirá un estándar aún más exigente: no solo se evaluará el cumplimiento, sino la efectividad de modelos de prevención.

Ello plantea un nuevo desafío para los colegios: comenzar a prepararse desde ahora. Porque estos modelos no se implementan de un día para otro: requieren tiempo, adaptación y, sobre todo, un cambio cultural.

Bajo dicha inminencia, el rol del director y de los equipos de convivencia tienen una relevancia clave. No solo por su responsabilidad en la gestión institucional, sino por ser quienes pueden impulsar, de forma consciente, holística y ordenada, estos nuevos desafíos.

Santiago, abril de 2026

.