

APUNTES DEL MÓDULO 1

La Ley 21.719 y los datos personales en la institución educativa

Protección de Datos Personales en Instituciones Educativas (Ley 21.719)

Material de estudio

Módulo 1

Contenido del módulo

- 1 **La Ley 21.719 en el Escenario Educativo: Objeto y Alcance**
- 2 **Conceptos Clave: Datos, Titulares y Actores en la Comunidad Educativa**
- 3 **Principios Rectores I: Licitud, Lealtad, Transparencia y Finalidad**
- 4 **Principios Rectores II: Minimización y Calidad**
- 5 **Principios de Responsabilidad Proactiva y Seguridad**
- 6 **La Agencia de Protección de Datos Personales (APDP)**

La protección de datos personales es una preocupación creciente a nivel global, y Chile no es la excepción. Con la entrada en vigencia de la Ley N°21.719, las instituciones educativas se enfrentan a un nuevo marco regulatorio que exige una gestión proactiva y consciente de la información que manejan sobre sus estudiantes, apoderados y personal. Este módulo te guiará a través de los aspectos fundamentales de esta ley, permitiéndote comprender su alcance, los conceptos clave y los principios que deben regir cada acción en tu establecimiento. Prepárate para reconocer tu rol y responsabilidades como institución educativa en la salvaguarda del derecho a la privacidad.

1 La Ley 21.719 en el Escenario Educativo: Objeto y Alcance

La Ley N°21.719 sobre Protección de Datos Personales marca un hito en la legislación chilena, buscando garantizar y proteger el derecho fundamental a la privacidad y a la protección de datos personales de las personas naturales. Esta ley aborda el tratamiento de datos tanto por organismos públicos como por entidades privadas.

Ámbito de aplicación: Su alcance es amplio, cubriendo todo tratamiento de datos personales, ya sea total o parcialmente automatizado, así como el tratamiento no automatizado de datos contenidos o destinados a ser incluidos en registros. Esto significa que desde la digitalización de expedientes hasta el manejo manual de fichas, todo está bajo su paraguas. Existen algunas excepciones, como los tratamientos exclusivamente personales o domésticos, o aquellos relacionados con la seguridad nacional, pero en general, la ley abarca tanto al sector público como al privado.

Es crucial destacar que **las instituciones educativas están plenamente alcanzadas por esta normativa**. Un colegio, jardín infantil, universidad, instituto profesional o centro de formación técnica gestiona diariamente una vasta cantidad de datos de estudiantes, apoderados y funcionarios. Por esta razón, cada establecimiento educativo es considerado un **responsable** del tratamiento de datos y debe cumplir cabalmente con las disposiciones de la ley.

La plena aplicación de esta normativa rige desde el **1 de diciembre de 2026**. A partir de esa fecha, todas las instituciones educativas deberán haber implementado las medidas necesarias para asegurar el cumplimiento íntegro de sus obligaciones. Esta ley representa un cambio de paradigma, pasando de un modelo reactivo a uno de **responsabilidad proactiva**, en línea con estándares internacionales como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Tipo de Establecimiento	Rol Frente a la Ley
Colegio particular / subvencionado	Responsable del tratamiento (entidad privada)
Colegio municipal / SLEP	Responsable del tratamiento (sector público)
Universidad estatal o privada	Responsable del tratamiento (sector público o privado, según corresponda)
Centro de Formación Técnica	Responsable del tratamiento (entidad privada)



La implementación de la Ley 21.719 requiere la colaboración y el compromiso de todo el personal de la institución.

✓ Puntos clave

- La Ley N°21.719 protege el derecho a la privacidad y a la protección de datos personales.
- Se aplica a todo tratamiento de datos, automatizado o no, en el sector público y privado.
- Las instituciones educativas son responsables del tratamiento de datos y están plenamente alcanzadas por la ley.
- La ley entrará en plena vigencia el 1 de diciembre de 2026, exigiendo un enfoque de responsabilidad proactiva.

Para reflexionar

- ¿Por qué es fundamental que una institución educativa conozca y aplique la Ley 21.719?
- ¿Qué tipo de tratamientos de datos personales se realizan en tu institución que estarían cubiertos por esta ley?
- Considerando la fecha de entrada en vigencia, ¿qué pasos iniciales debería dar tu institución para prepararse?

Conceptos Clave: Datos, Titulares y Actores en la Comunidad Educativa

Para una correcta aplicación de la Ley 21.719 en el entorno educativo, es indispensable comprender su terminología. A continuación, definiremos los conceptos más importantes y su relevancia en el día a día de un establecimiento.

- **Dato personal:** Es toda información que se refiera a una persona natural identificada o identificable. En una institución educativa, esto incluye, pero no se limita a: nombre completo, RUT, dirección, correo electrónico, número de teléfono, notas y calificaciones, registros de asistencia, fotografías, videos de vigilancia, e información de contacto de emergencia de estudiantes y apoderados. También se consideran datos personales los registros de desempeño laboral de los funcionarios.
- **Dato sensible:** Se refiere a aquellos datos personales que revelan aspectos íntimos de una persona, como el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos, datos de salud, vida sexual u orientación sexual. En el contexto educativo, los datos sensibles más frecuentes son los **datos de salud** (alergias, condiciones médicas), **diagnósticos relacionados con Programas de Integración Escolar (PIE) o necesidades educativas especiales**, información sobre **discapacidad** y, en algunos casos, **situación socioeconómica** cuando esta revela aspectos de vulnerabilidad. El tratamiento de este tipo de datos exige mayores salvaguardias y, generalmente, el consentimiento explícito del titular.
- **Titular:** Es la persona natural a la que se refieren los datos personales. En la comunidad educativa, los titulares son los estudiantes, los apoderados (en relación con sus propios datos) y los funcionarios.
- **Responsable del tratamiento:** Es la persona natural o jurídica, pública o privada, que determina los fines y medios del tratamiento de datos personales. En la práctica, **la institución educativa** (el sostenedor, la universidad, el centro de formación técnica) actúa como responsable. Es quien decide qué datos se recopilan, con qué propósito y cómo se gestionan.
- **Encargado del tratamiento:** Es la persona natural o jurídica, pública o privada, que trata datos personales por cuenta del responsable. Por ejemplo, un **proveedor de una plataforma de libro de clases digital**, un sistema de gestión de aprendizaje (LMS), un servicio de correo institucional o una empresa de alimentación que maneja información sobre alergias de estudiantes, actúan como encargados. Estos solo pueden tratar los datos según las instrucciones del responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales. Esto abarca desde la recolección de una ficha de matrícula, el registro de notas en un sistema, la comunicación de información académica a un apoderado, la conservación de expedientes, la consulta de historiales, hasta la modificación, bloqueo o supresión de registros.

✓ Puntos clave

- Dato personal es toda información que identifica a una persona (nombre, RUT, notas, fotos).
- Dato sensible revela aspectos íntimos (salud, diagnóstico PIE) y requiere mayor protección.
- El titular es la persona a quien corresponden los datos (estudiante, apoderado, funcionario).
- La institución educativa es el responsable del tratamiento, decidiendo fines y medios.
- El encargado trata datos por cuenta del responsable (ej. proveedor de software educativo).
- Tratamiento es cualquier operación sobre los datos (recolección, registro, comunicación, etc.).

Para reflexionar

- Identifica tres ejemplos de datos personales y dos de datos sensibles que tu institución recopila habitualmente. ¿Cómo los gestionan actualmente?
- ¿Quién sería el responsable del tratamiento en tu institución? ¿Podrías identificar a algún encargado del tratamiento con el que trabajen?
- ¿Qué implicaciones tiene para tu rol que una fotografía de un estudiante sea considerada un dato personal?

3 Principios Rectores I: Licitud, Lealtad, Transparencia y Finalidad

La Ley 21.719 establece una serie de principios que deben guiar todas las acciones de tratamiento de datos personales. Estos principios no son meras recomendaciones, sino directrices obligatorias que aseguran un manejo ético y legal de la información. A continuación, exploramos los primeros cuatro principios esenciales:

- **1. Licitud:** Este principio exige que todo tratamiento de datos personales debe tener un fundamento legal claro. No basta con poseer los datos; se debe contar con una base de legitimación válida para procesarlos. Las bases de legitimación incluyen el consentimiento del titular, la ejecución de un contrato (como el contrato de prestación de servicios educativos), el cumplimiento de una obligación legal (ej. informar al Ministerio de Educación), la protección de intereses vitales, el cumplimiento de una misión en interés público o el interés legítimo del responsable, siempre que no prevalezcan los derechos del titular.
- **2. Lealtad:** El tratamiento de datos debe ser realizado de manera leal, evitando cualquier engaño, fraude o abuso de confianza. Implica actuar con buena fe en la relación con los titulares de los datos. Por ejemplo, no se pueden obtener datos de estudiantes o apoderados bajo pretextos falsos o mediante prácticas desleales que manipulen su voluntad.
- **3. Transparencia:** Los titulares de los datos (estudiantes, apoderados, funcionarios) tienen el derecho a ser informados de forma clara, concisa y en lenguaje sencillo sobre el tratamiento de sus datos. Esto incluye saber quién es el responsable, para qué fines se utilizan sus datos, por cuánto tiempo se conservarán, con quién se comparten y cuáles son sus derechos (acceso, rectificación, supresión, etc.). Este principio se materializa a menudo a través de un **aviso o política de privacidad** visible y accesible en el establecimiento.
- **4. Finalidad:** Los datos personales deben ser recolectados con fines específicos, explícitos y legítimos. Esto significa que la institución educativa debe tener un propósito claro y justificado para cada dato que solicita y procesa (por ejemplo, la gestión académica, la seguridad escolar, la comunicación con apoderados). Una vez recolectados para una finalidad determinada, los datos no pueden ser tratados posteriormente de forma incompatible con dicho propósito original. Si la institución decide utilizar los datos para un fin diferente al inicial, en la mayoría de los casos, necesitará obtener un nuevo consentimiento del titular.

Principio	Descripción en el Contexto Educativo	Pregunta Clave para la Institución
Licitud	Todo tratamiento de datos debe tener una base legal (consentimiento, contrato educativo, obligación legal, etc.).	¿Tenemos una base legal válida para cada tratamiento de datos que realizamos?
Lealtad	Tratar los datos de forma honesta, sin engaño ni abuso de confianza hacia la comunidad educativa.	¿Estamos siendo honestos y transparentes en cómo obtenemos y usamos los datos de estudiantes y apoderados?
Transparencia	Informar claramente a los titulares sobre quién trata sus datos, para qué y por cuánto tiempo.	¿Nuestro aviso de privacidad es fácil de entender y accesible para todos los miembros de la comunidad?

Principio	Descripción en el Contexto Educativo	Pregunta Clave para la Institución
Finalidad	Recolectar datos solo para fines específicos y legítimos, sin utilizarlos para propósitos incompatibles.	¿Para qué propósito específico recolectamos cada dato y se está utilizando solo para eso?



La gestión de datos digitales y la seguridad de la información son aspectos clave en la protección de datos personales en el entorno educativo.

✓ Puntos clave

- Licitud: requiere una base legal para todo tratamiento de datos (consentimiento, contrato, obligación legal, etc.).
- Lealtad: prohíbe el engaño y el abuso de confianza en la obtención y uso de datos.
- Transparencia: exige informar claramente a los titulares sobre el tratamiento de sus datos.
- Finalidad: los datos deben recolectarse para fines explícitos y no usarse de forma incompatible posteriormente.

 Para reflexionar

- Imagina que tu institución quiere enviar publicidad de un campamento de verano a los apoderados. ¿Qué principio o principios deberían considerar y cómo lo aplicarían?
- ¿De qué manera pueden asegurar que la política de privacidad de su institución sea realmente transparente y comprensible para todos los apoderados?
- Si su institución recolecta datos de salud de los estudiantes, ¿cuál sería la finalidad legítima para ese tratamiento y qué base de legitimación usarían?

4 Principios Rectores II: Minimización y Calidad

Continuando con los principios rectores de la Ley 21.719, la minimización y la calidad son fundamentales para asegurar que los datos manejados por la institución educativa sean no solo relevantes, sino también precisos y actualizados. Ambos principios buscan la eficiencia y la pertinencia en el manejo de la información.

- **Principio de minimización (proporcionalidad):** Este principio establece que los datos personales deben ser adecuados, pertinentes y **no excesivos** en relación con la finalidad para la que se tratan. Una institución educativa debe solicitar y conservar solo aquellos datos estrictamente necesarios para cumplir con sus objetivos educativos y administrativos.

En la práctica: Antes de diseñar o actualizar un formulario de matrícula o admisión, el equipo responsable debería revisar cada campo y preguntarse: “¿*Realmente necesito este dato para prestar el servicio educativo o para cumplir con una obligación legal?*”. Si la respuesta es no, ese campo debe eliminarse o hacerse opcional, requiriendo un consentimiento explícito si es que se decide mantenerlo. Por ejemplo, solicitar información sobre la religión de la familia o los ingresos económicos del hogar sin una finalidad clara, justificada y una base legal específica, podría ser considerado un exceso y una violación de este principio.

- **Principio de calidad (exactitud):** Este principio exige que los datos personales deben ser exactos y, cuando sea necesario, estar actualizados. Los datos inexactos o desactualizados pueden llevar a decisiones erróneas y, potencialmente, causar perjuicios reales a los titulares. Un número de contacto de emergencia incorrecto, una alergia no registrada o una nota académica mal ingresada son ejemplos de cómo la falta de calidad puede tener consecuencias negativas.

En la práctica: Las instituciones deben implementar rutinas y procedimientos para verificar y actualizar periódicamente los datos. Esto podría incluir solicitar a los apoderados que confirmen o actualicen sus datos de contacto al inicio de cada año escolar, establecer protocolos para la corrección de errores en registros académicos o administrativos, y facilitar el ejercicio del derecho de rectificación por parte de los titulares.

✓ Puntos clave

- Minimización (proporcionalidad): recolectar solo los datos adecuados, pertinentes y no excesivos para la finalidad.
- En la práctica, revisar formularios para eliminar datos no estrictamente necesarios.
- Calidad (exactitud): asegurar que los datos sean exactos y actualizados.
- En la práctica, implementar rutinas de verificación y facilitar la rectificación de datos.

 Para reflexionar

- Revisa la ficha de matrícula de tu institución. ¿Existe algún dato que se solicite que no sea estrictamente necesario según el principio de minimización?
- ¿Qué consecuencias podría tener para un estudiante o su apoderado si la información de contacto de emergencia está desactualizada en tu institución?
- ¿Qué medidas concretas podría implementar tu institución para asegurar la calidad y actualización de los datos de salud de los estudiantes?

5 Principios de Responsabilidad Proactiva y Seguridad

Estos dos principios constituyen el núcleo del nuevo enfoque que la Ley 21.719 introduce en la gestión de datos personales. Ya no basta con cumplir; las instituciones deben ser capaces de demostrar su cumplimiento y anticiparse activamente a los riesgos.

- **Responsabilidad proactiva (Accountability):** Este principio fundamental implica que el responsable del tratamiento (la institución educativa) no solo debe cumplir con los principios y disposiciones de la ley, sino que debe ser capaz de **demostrar** dicho cumplimiento. Esto significa que la carga de la prueba recae en la institución. Para ello, se deben implementar una serie de medidas y herramientas, como el desarrollo de políticas internas claras sobre protección de datos, la adopción de medidas técnicas y organizativas adecuadas, la realización de evaluaciones de impacto sobre la privacidad para tratamientos de alto riesgo, el mantenimiento de un registro de las actividades de tratamiento, la capacitación constante del personal y la documentación exhaustiva de todas estas acciones. Este principio representa un cambio radical de un modelo reactivo (esperar una denuncia o fiscalización) a un enfoque **preventivo y documentado**.
- **Seguridad:** La ley exige que el responsable del tratamiento implemente medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra accesos no autorizados, la pérdida, alteración, destrucción o cualquier forma de tratamiento ilícito. Las medidas deben ser proporcionales al riesgo que representa el tratamiento de datos.

En la práctica: En un colegio, esto podría incluir controles de acceso físico a los archivos en papel (fichas bajo llave), controles de acceso lógico a los sistemas informáticos (contraseñas robustas para el sistema de notas), la implementación de respaldos periódicos de la información digital, el cifrado de datos sensibles, la actualización constante de software de seguridad y la elaboración de protocolos para el manejo de incidentes de seguridad.

- **Confidencialidad:** Todas las personas que, por razón de sus funciones, intervengan en el tratamiento de datos personales (docentes, inspectores, personal administrativo, psicólogos, etc.) están obligadas a guardar secreto sobre ellos. Este deber de confidencialidad no termina con la finalización de la relación laboral o contractual con la institución, sino que subsiste indefinidamente.

En la práctica: La institución debe asegurar que su personal firme acuerdos de confidencialidad o que esta obligación quede explícitamente establecida en sus contratos de trabajo y reglamentos internos. Es fundamental concientizar y capacitar al personal sobre la importancia de no divulgar información personal de estudiantes o apoderados, incluso en conversaciones informales.

✓ Puntos clave

- Responsabilidad proactiva (Accountability): la institución debe demostrar el cumplimiento de la ley con políticas, capacitaciones y documentación.
- Este principio transforma el enfoque de reactivo a preventivo y documentado.
- Seguridad: implementar medidas técnicas y organizativas para proteger los datos contra accesos no autorizados, pérdida o daño.
- Confidencialidad: todo el personal que trate datos está obligado a guardar secreto, incluso después de terminar su relación con la institución.

Para reflexionar

- ¿Cómo podría tu institución documentar que está cumpliendo con los principios de protección de datos (responsabilidad proactiva)?
- Identifica al menos tres medidas de seguridad que tu institución ya implementa o podría implementar para proteger los datos personales.
- ¿Qué tipo de capacitación o sensibilización sería necesaria para el personal docente y administrativo respecto al deber de confidencialidad?

Con la Ley 21.719, Chile establece una autoridad de control especializada en la protección de datos personales: la Agencia de Protección de Datos Personales (APDP). Esta entidad es el nuevo guardián de la privacidad y tiene un rol crucial en la fiscalización y el cumplimiento de la normativa en todos los ámbitos, incluyendo el educativo.

La **Agencia de Protección de Datos Personales (APDP)** es un servicio público descentralizado, lo que le otorga autonomía para ejercer sus funciones. Posee personalidad jurídica y patrimonio propio, y está bajo la supervigilancia del Presidente de la República a través del Ministerio de Justicia y Derechos Humanos.

Entre sus **principales funciones** se encuentran:

- **Fiscalizar el cumplimiento de la normativa:** La APDP tiene la potestad de investigar y verificar si las instituciones (públicas y privadas, incluyendo las educativas) están respetando las disposiciones de la Ley 21.719. Esto puede hacerlo de oficio (por iniciativa propia) o a petición de parte (por ejemplo, ante el reclamo de un apoderado que considere que sus datos fueron mal tratados).
- **Instruir procedimientos sancionatorios y aplicar sanciones:** En caso de detectar incumplimientos a la ley, la APDP está facultada para iniciar procedimientos administrativos que pueden culminar en la imposición de sanciones. Estas sanciones pueden variar en gravedad, incluyendo multas que pueden alcanzar hasta 15.000 UTM (Unidades Tributarias Mensuales) en los casos más graves.
- **Conocer y resolver reclamaciones:** La Agencia actuará como instancia para que los titulares de datos (estudiantes, apoderados, funcionarios) puedan presentar reclamos cuando consideren que sus derechos han sido vulnerados o que sus datos han sido tratados de forma indebida.
- **Dictar normas e instrucciones:** Para facilitar el cumplimiento de la ley y aclarar su aplicación en diversos sectores, la APDP podrá emitir reglamentos, instructivos y guías técnicas.
- **Promover la educación y concientización:** Un rol importante de la Agencia es difundir el conocimiento sobre los derechos en materia de protección de datos y las obligaciones de los responsables, contribuyendo a una cultura de respeto a la privacidad.
- **Colaborar con otras autoridades:** Podrá establecer alianzas y cooperar con otras instituciones, tanto nacionales como internacionales, en materias relacionadas con la protección de datos.

Para las instituciones educativas, la existencia de la APDP significa que habrá un organismo vigilante y con capacidad sancionatoria, lo que subraya la importancia de implementar medidas robustas de cumplimiento y de estar preparados para eventuales fiscalizaciones. La proactividad en la adaptación a la ley será clave para evitar sanciones y construir confianza con la comunidad educativa.

✓ Puntos clave

- La APDP es la autoridad de control encargada de fiscalizar la Ley 21.719.
- Tiene funciones de fiscalización, sanción (multas de hasta 15.000 UTM), resolución de reclamos y emisión de normas.
- Promueve la educación y concientización sobre la protección de datos.
- Su existencia subraya la necesidad de que las instituciones educativas sean proactivas en el cumplimiento de la ley.

Para reflexionar

- ¿Cómo crees que la existencia de la APDP impactará la forma en que tu institución maneja los datos personales?
- Si un apoderado presenta un reclamo ante la APDP por un supuesto mal uso de sus datos, ¿qué preparación debería tener tu institución para afrontar este escenario?
- ¿De qué manera podría tu institución utilizar las orientaciones o guías que emita la APDP para mejorar sus prácticas de protección de datos?

Esquema del Módulo: La Ley 21.719 y los Datos Personales en la Institución Educativa

Introducción a la Ley 21.719	Objeto y ámbito de aplicación de la ley en instituciones educativas, destacando la responsabilidad proactiva.
Conceptos Clave	Definición de dato personal, dato sensible, titular, responsable y encargado del tratamiento en el ámbito educativo.
Principios Rectores (Parte I)	Análisis de licitud, lealtad, transparencia y finalidad como pilares del tratamiento de datos.
Principios Rectores (Parte II)	Exploración de la minimización (proporcionalidad) y la calidad (exactitud) de los datos.
Responsabilidad y Seguridad	Profundización en la responsabilidad proactiva, medidas de seguridad y el deber de confidencialidad.
Agencia de Protección de Datos Personales (APDP)	Funciones y rol de la autoridad de control en la fiscalización y aplicación de la ley.

Para repasar

¿Qué concepto es?

Concepto	Respuesta
El nombre, el RUT y la dirección de un estudiante	Dato personal: información de una persona natural identificada o identificable.
El diagnóstico PIE o la situación socioeconómica de un estudiante	Dato sensible: su tratamiento exige mayores garantías.
El apoderado o el funcionario a quien se refieren los datos	Titular de los datos.

Concepto	Respuesta
El sostenedor que decide qué datos pedir y para qué	Responsable del tratamiento: determina los fines y los medios.
El proveedor del libro de clases digital o del LMS	Encargado del tratamiento: trata los datos por cuenta del responsable.
Registrar notas, conservar expedientes o suprimir registros	Tratamiento: cualquier operación sobre los datos.

Aplicar minimización y calidad en la ficha de matrícula

1. **Revisa cada campo.** Antes de diseñar el formulario de matrícula o admisión, analiza los campos uno por uno.
2. **Pregunta por la necesidad.** ¿Necesito este dato para prestar el servicio educativo?
3. **Elimina o haz opcional.** Si no es necesario, elimínalo o déjalo opcional con consentimiento explícito.
4. **Verifica al inicio del año.** Confirma el teléfono del apoderado y los contactos de emergencia.
5. **Corrige y facilita la rectificación.** Corrige las notas mal ingresadas y facilita que el apoderado ejerza su derecho de rectificación.

Preguntas frecuentes sobre la APDP en el establecimiento

¿Qué pasa si un apoderado reclama ante la APDP? La Agencia puede fiscalizar a petición de parte y conoce y resuelve los reclamos de los titulares por vulneración de sus derechos.

¿Puede sancionar al establecimiento? Sí. Instruye procedimientos sancionatorios y aplica multas de hasta 15.000 UTM en casos graves.

¿Importa si nuestra plataforma está alojada en el extranjero? Sí. La APDP autoriza las transferencias internacionales de datos cuando corresponde.

¿Qué obligaciones tenemos frente a la Agencia? Responder sus requerimientos en plazo, notificar las brechas de seguridad y seguir sus directrices sobre datos de niños, niñas y adolescentes.

¿De quién depende la APDP? Es un servicio público descentralizado, supervigilado por el Presidente de la República a través del Ministerio de Justicia y Derechos Humanos.

En síntesis. Hemos completado un recorrido fundamental por la Ley N°21.719, comprendiendo su objeto, los conceptos esenciales y los principios que deben guiar cada acción en su institución educativa. Recuerde que el cumplimiento de esta ley no es solo una obligación legal, sino una oportunidad para fortalecer la confianza de su comunidad y asegurar un entorno educativo que valore y proteja la privacidad de cada individuo. La responsabilidad proactiva es el camino a seguir, anticipándose a los desafíos y construyendo una cultura de respeto por los datos personales. ¡Su rol es crucial en este nuevo escenario!