Superintendencia de Industria y Comercio

GUÍA SOBRE

EL TRATAMIENTO DE DATOS PERSONALES

EN EL CONTEXTO UNIVERSITARIO

Superintendencia de
Industria y Comercio

Cielo Elainne Rusinque Urrego
Superintendente de Industria y Comercio

Juan Carlos Upegui Mejía
Superintendente Delegado para la
Protección de Datos Personales

Iván Darío Hernández Rodríguez
Jefe Oficina de Servicios al Consumidor
y Apoyo Empresarial - OSCAE

Juan Carlos Upegui Mejía
Daniel Felipe Ospina Celis
Autores

Laura Fernanda González Rey
Diagramación

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Calle 24 No. 7 - 43, Bogotá D.C., Colombia
Línea de atención: +57 601 592 0400
Línea gratuita nacional: 01 8000 910165
Teléfono conmutador: +57 601 587 0000

www.sic.gov.co

Bogotá, julio de 2026.

CONTENIDO

1 Introducción

1. Introducción

Las Instituciones de Educación Superior (IES) adelantan tratamiento de datos personales de forma intensiva. Lo hacen respecto de información de estudiantes, aspirantes, acudientes, padres de familia, egresados, visitantes, proveedores, aliados y personal administrativo y docente. Lo hacen en y a partir de expedientes académicos, disciplinarios, laborales y crediticios; registros sobre servicios de bienestar y de salud, de inscripción a eventos y de control de acceso; listados de servicios de almacenamiento, cuentas de correo electrónico y servicios anexos, entre muchos otros.

La complejidad de las actividades de tratamiento en diversos contextos y para distintas finalidades impone altas responsabilidades jurídicas y éticas en la implementación de medidas que aseguren el debido tratamiento de datos personales, conforme a la Ley 1581 de 2012, sus decretos reglamentarios y la jurisprudencia constitucional.

Esta guía presenta recomendaciones sobre el tratamiento de datos personales en las IES y sobre cómo resolver algunas tensiones y problemas comunes relacionados con dichas actividades en el contexto universitario.

#DatosPersonales

2

El derecho al habeas data y a la protección de datos personales en el contexto universitario.

2. El derecho al habeas data y a la protección de datos

El artículo 15 de la Constitución Política de 1991 reconoce el derecho fundamental al habeas data y a la protección de datos personales en los siguientes términos:

> ***ARTÍCULO 15.*** *Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*

La Ley 1581 de 2012 desarrolla este derecho y, para ello, establece disposiciones generales que rigen el tratamiento de datos personales y que son aplicables a las IES. A continuación, se presentan algunos aspectos básicos en la materia.

2.1. Definiciones

La legislación relacionada con el derecho a la protección de datos personales hace uso de términos específicos, cuya definición se debe conocer. Los más relevantes en el contexto universitario son:

Dato personal: cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable. Los datos personales se pueden clasificar en virtud de su vocación de circulación o de su sensibilidad.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales. Incluye recolección, almacenamiento, uso, análisis, comunicación, circulación o supresión, entre otros.

Responsable del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. Es decir, quien controle los medios (cómo) y establezca los fines (para qué) del tratamiento de datos. Por lo general, las IES actúan como responsables del tratamiento.

Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. En ocasiones, las IES pueden contratar a un tercero para que realice ciertas actividades de tratamiento, como llamar a los exalumnos para invitarlos a participar en ciertas actividades.

Titular: persona natural cuyos datos personales sean objeto de tratamiento. Corresponde a cualquier persona cuyos datos personales sean recolectados, usados, circulados o analizados por una IES, a saber: aspirantes, estudiantes, padres y madres, tutores, exalumnos, proveedores, aliados, personal administrativo y docente, etc.

2.2. Categorías de datos personales

Los datos personales pueden clasificarse en virtud de su vocación de circulación o en virtud de su relación con el derecho a la intimidad y a la no discriminación. La Ley 1266 de 2008 recogió las categorías creadas por la Corte Constitucional para referirse al grado de circulación de los datos y estableció las siguientes categorías: datos públicos, datos semiprivados y datos privados.

Dato público: es aquel calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.

Dato privado: es aquel que por su naturaleza íntima o reservada sólo es relevante para el titular.

A las categorías anteriores, debe sumarse la de dato sensible, reconocida en la Ley 1581 de 2012, definición que se construye a partir de su relación funcional con la intimidad y la no discriminación, y no en relación con su grado de circulación.

Dato sensible: es aquel que guarda especial relación con la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Estas categorías permiten evaluar el nivel de protección que debería darse a la información almacenada en archivos o bases de datos de las IES.

CATEGORÍA	EJEMPLOS EN EL CONTEXTO UNIVERSITARIO	NIVEL DE PROTECCIÓN
Público	Vinculación, título otorgado.	Bajo
Semiprivado	Notas, promedios, historial y estatus académico, cartera y saldos financieros, situación socioeconómica.	Intermedio
Privado	Datos de contacto personales, correspondencia privada, expedientes disciplinarios.	Elevado
Sensible	Datos de salud (física y mental), datos biométricos, que revelen pertenencia a grupos étnicos, identidad racial y de género, convicciones religiosas o filosóficas, orientación política y los relativos a la vida sexual.	Reforzado

2.3. Principios del tratamiento de datos personales

El tratamiento de datos personales es una actividad reglada que debe realizarse conforme a los principios establecidos en la Ley 1581 de 2012. En esta guía se indican los más relevantes en el ámbito universitario sin que esto implique que los demás dejen de ser plenamente aplicables.

- **Principio de finalidad.** El tratamiento debe realizarse con un fin u objetivo constitucionalmente legítimo. Algunos fines constitucionalmente legítimos en el contexto universitario son: el cumplimiento de los deberes legales y constitucionales asociados a la prestación del servicio público de educación, la debida ejecución de las obligaciones nacidas del contrato de matrícula, la comunicación con la comunidad estudiantil para el ejercicio de sus derechos, y la satisfacción de derechos de terceros, en especial, de madres, padres o acudientes a ser informados sobre circunstancias excepcionales, etc.

- **Principio de libertad.** El tratamiento solo es válido si se realiza al amparo del cumplimiento de un deber constitucional o legal, es indispensable para el cumplimiento del contrato de matrícula, o se cuenta con el consentimiento previo, libre, informado y expreso del titular.

- **Principio de acceso y circulación restringida.** El tratamiento y sobre todo la circulación deben sujetarse a la naturaleza de los datos personales (públicos, semiprivados, privados) y a lo establecido en la ley. En principio, las IES no deberían circular o comunicar a terceros los datos personales de los titulares sin que exista habilitación legal o autorización de la o el titular.

- **Principio de confidencialidad.** Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información personal.

El tratamiento de datos personales en el contexto universitario debe adelantarse conforme a estos y a los demás principios contenidos en **el artículo 4 de la Ley 1581 de 2012** y en la Jurisprudencia constitucional.

2.4. Deberes de los responsables y encargados del tratamiento

Como una medida para proteger los derechos fundamentales de los titulares, las IES como responsables del tratamiento deben cumplir con ciertos deberes al realizar cualquier operación sobre datos personales. Dichos deberes constituyen uno de los aspectos más relevantes de la Ley 1581 de 2012 y determinan qué debe, qué puede y qué no puede hacer una IES con los datos personales que recolecte.

En su labor de tratamiento de datos personales las IES deben cumplir con los deberes contenidos en **los artículos 17 y 18 de la Ley 1581 de 2012.** Aunque se trata de deberes generales que se orientan a determinar la conducta de los responsables y encargados del tratamiento, las IES pueden encontrar dificultades para cumplir simultáneamente con dichos deberes y con las otras obligaciones legales que pesan sobre ellas.

En la siguiente sección se presentan algunas recomendaciones para el tratamiento de datos personales en contextos universitarios.

#DatosPersonales

3

Recomendaciones sobre el tratamiento de datos personales en contextos universitarios.

3. Recomendaciones sobre el tratamiento de datos

En el contexto universitario pueden surgir conflictos (de derechos, de intereses, de normas) relacionados con el tratamiento de datos personales. Por ejemplo, algunas IES y sobre todo las de naturaleza pública, experimentan retos relacionados con el encuentro de dos regímenes jurídicos: el de la transparencia y el de la protección de datos personales. En ocasiones, se solicita a las instituciones que prestan el servicio público de educación acceso a información pública que contiene datos de personas naturales.

Asimismo, las IES tanto públicas como privadas acogen, dentro del ecosistema de tratamiento de datos personales, a personas y actores que pueden tener diferentes intereses y derechos: madres, padres, acudientes o responsables económicos, otros miembros de la comunidad, periodistas, autoridades públicas, etc., por un lado, y la comunidad estudiantil, egresados y docentes, por el otro.

En ocasiones, por ejemplo, quienes financian el servicio público de educación tienen interés en conocer el desempeño (y otra información) de quien se beneficia de dicho financiamiento. También es posible que ante ciertos hechos que involucren estudiantes, docentes o egresados pueda surgir un interés público en su develación (casos de accidentes, comisión de delitos, escrutinio público de egresados con poder o con vocación de poder, asuntos de interés público, etc.).

Por otro lado, pueden darse circunstancias en las que la vida o la salud de uno o varios miembros de la comunidad universitaria esté en riesgo. En tales casos, el derecho de terceros a acceder a información personal de algún miembro de la comunidad universitaria, o incluso el deber de la IES de comunicar o circular dicha información, podría entrar en tensión con el derecho a la protección de datos personales-principios de circulación restringida y confidencialidad. El reto práctico en estos casos consiste en identificar qué información se puede o no compartir, con quién, en virtud de cuál finalidad, por qué buenas razones y bajo qué garantías.

Otro tipo de retos se refiere al tratamiento de datos personales de menores de edad que integran la comunidad universitaria o quieren hacerlo. Según **el artículo 7 de la Ley 1581 de 2012**, el tratamiento de dichos datos se encuentra proscrito. Sin embargo, la Corte Constitucional en la sentencia C-748 de 2011 estableció que esta afirmación:

> *...no debe entenderse en el sentido de que existe una prohibición casi absoluta del tratamiento de los datos de los menores de 18 años, exceptuando los de naturaleza pública, pues ello, daría lugar a la negación de otros derechos superiores de esta población como el de la seguridad social en salud, interpretación ésta que no se encuentra conforme con la Constitución. De lo que se trata entonces, es de reconocer y asegurar la plena vigencia de todos los derechos fundamentales de esta población, incluido el habeas data.*
>
> *En este mismo sentido, debe interpretarse la expresión "naturaleza pública". Es decir, el tratamiento de los datos personales de los menores de 18 años, al margen de su*

naturaleza, pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, las niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes.

Por tal motivo, las IES pueden y deben realizar tratamiento de datos personales de menores de 18 años siempre que se promueva el interés superior del menor. Por ejemplo, si el tratamiento es indispensable para asegurar el acceso efectivo al servicio público de educación, el goce de su derecho a la educación o para proteger la vida o integridad física del menor de edad.

Ya sea en procesos de admisión y de oferta de servicios (ferias estudiantiles, eventos, formularios, etc.) o ya durante el transcurso de la vida universitaria de quienes acceden siendo menores de 18 años, las IES deben cumplir con los principios y deberes contenidos en la Ley 1581 de 2012, al realizar tratamiento de datos personales de menores de edad.

Teniendo en cuenta estos y otros retos que se generan en el contexto universitario, se formulan las siguientes recomendaciones.

3.1. En casos de conflictos de derechos o de intereses, ponderar el derecho a la protección de datos personales con otros derechos fundamentales e intereses constitucionales legítimos

Como cualquier derecho fundamental, el derecho al habeas data y a la protección de datos personales no es un derecho absoluto. Por eso, cuando se presenten casos difíciles en los que entran en conflicto o en tensión derechos o intereses constitucionales, las IES como responsables del tratamiento deben determinar, en el caso concreto, cuál derecho prima sobre el otro. Las herramientas de ponderación son un instrumento útil para resolver estos casos.

Por ejemplo, la Corte Constitucional ha reconocido que cuando los derechos a la intimidad y al habeas data entran en tensión con otros derechos, como el derecho de acceso a la información, se debe revisar con atención el régimen jurídico aplicable y si es del caso acudir a instrumentos de ponderación.

En la **Sentencia T-454 de 2024,** la Corte ordenó a una IES privada entregar a un periodista información personal relacionada con el título otorgado o con el estatus académico del entonces rector de una universidad pública. Para llegar a esta conclusión, la Corte realizó un ejercicio de ponderación de tres pasos[1]:

1. Corte Constitucional. Sentencia T-454 de 2024. "Test de ponderación entre la afectación a la protección de datos personales y el derecho al acceso a la información pública". Consideraciones 82 a 115. M.P. Natalia Ángel Cabo.

i. **un primer paso** en el que se determine el "grado de protección de los derechos al hábeas data y a la intimidad" del titular de los datos personales en el caso específico;

ii. **un segundo paso** en el que se determine el "grado de protección del derecho de acceso a la información" a partir de revisar tres elementos: "las características del titular de la información, la actividad que ejerce el solicitante y la relevancia pública que tiene la información" en el caso específico;

iii. **Y un tercer paso** en el que se "compar[en] el grado de protección de los derechos en juego" y a partir de lo cual "se esco[ja] el escenario que promueva una mayor realización de derechos fundamentales y principios constitucionales" en el caso específico.

Este tipo de ejercicios de ponderación es replicable en otros casos de tensión entre el derecho al habeas data y cualquier otro derecho fundamental. En tales escenarios, se deberá analizar, además de las reglas especiales de protección de los derechos, si los beneficios constitucionales de, por ejemplo, suministrar o entregar datos personales son mayores a los que se desprenden del cumplimiento estricto de los principios de circulación restringida y confidencialidad.

En últimas, el ejercicio de ponderación de derechos o de intereses permite establecer si la interferencia en el derecho al habeas data, que supone la entrega, comunicación o circulación de información personal sin el consentimiento del titular, es legítima.

En este mismo sentido, por ejemplo, en la **Sentencia T-058 de 2013**, la Corte Constitucional le ordenó a una IES expedirle a una exalumna suya un certificado de estudios sin incluir información relacionada con sus antecedentes disciplinarios. La Corte consideró que la negativa de la IES a expedir el certificado excluyendo dichos antecedentes era desproporcionada. Recordó (en obiter) que toda medida que suponga una interferencia en los derechos fundamentales, y en concreto en los derechos fundamentales al habeas data y a la educación, debe superar un examen de los siguientes requisitos[2]:

i. la legitimidad de los fines perseguidos por la medida que interviene en el derecho fundamental;

ii. la legitimidad de la medida en sí misma;

iii. su idoneidad para obtener el fin perseguido;

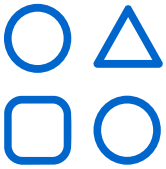
iv. la necesidad de la misma y, finalmente;

v. la proporcionalidad.

2. Corte Constitucional. Sentencia T-058 de 2013. Consideración 3.7. M.P. Alexei Julio Estrada.

Las IES deben acudir a este tipo de procedimientos cuando se enfrenten a situaciones en las que parezca legítima, necesaria y proporcional la comunicación o circulación de información personal sin el consentimiento de los titulares. Como ha indicado la Superintendencia de Industria y Comercio[3]:

> *la ponderación de derechos exige un análisis concreto de las circunstancias del caso particular, en el que se evalúe los derechos en tensión o conflicto, la naturaleza de los datos personales en juego, el contexto fáctico, los intereses legítimos de terceros, así como las finalidades que se persiguen con el tratamiento de los datos personales y de los otros derechos que estén en juego. Solo a partir de dichos elementos específicos sería posible determinar, con criterios de razonabilidad y proporcionalidad, si resulta jurídicamente admisible limitar el derecho al hábeas data en favor de otro derecho o interés relevante en una situación concreta.*



3.2. Clasificar la información académica y administrativa según categorías, tipo de protección y finalidades del tratamiento

Al distinguir entre datos públicos, semiprivados, privados y sensibles, y articular esa clasificación con finalidades específicas, controles de acceso y plazos de conservación, se reduce el riesgo de filtraciones, se facilita la gobernanza sobre la información y se fortalece la confianza de la comunidad académica.

Las IES podrían identificar los tipos de información personal propios del régimen de protección de datos personales en sus procesos de gobernanza de datos y de caracterización de sus activos de información. A modo de ejemplo, cada IES podría contar con una matriz en la que identifique la categoría legal, los tipos de datos en concreto sobre los que realiza tratamiento, el nivel de protección que merecen dichos conjuntos de datos, las dependencias o personas que pueden acceder a ellos y las finalidades para las cuales se realiza el tratamiento de dichos datos.

3. Superintendencia de Industria y Comercio, Oficina Asesora Jurídica. Concepto de junio de 2025. Radicado 25-212411.

CATEGORÍA	EJEMPLOS EN EL CONTEXTO UNIVERSITARIO	NIVEL DE PROTECCIÓN	CONTROL DE ACCESO	FINALIDADES
Público	Calidad de estudiante, docente, o egresado, título otorgado.	Bajo	Todos	[Incluir las finalidades de cada IES]
Semiprivado	Notas, promedios, situación socioeconómica, historial y estatus académico, cartera y saldos financieros.	Intermedio	Admisiones y decanatura	[Incluir las finalidades de cada IES]
Privado	Datos de residencia, correspondencia privada, calidad de acudiente o financiador, expedientes disciplinarios.	Elevado	Admisiones o dependencias específicas	[Incluir las finalidades de cada IES]
Sensible	Datos de salud (física y mental), datos biométricos, pertenencia a grupos étnicos, identidad racial y de género, convicciones religiosas o filosóficas, orientación política y los relativos a la vida sexual.	Reforzado	Decanatura o dependencias específicas	[Incluir las finalidades de cada IES]

Las IES podrían adoptar un esquema de clasificación homogéneo, aplicable a todos sus procesos, sistemas y unidades. Se pueden reconocer como datos semiprivados el conjunto de información académica del estudiante (notas, promedios, historiales y algunas situaciones disciplinarias) y su información financiera (cartera, pagos, descuentos, etc.).

En todo caso, la clasificación de la información debe ser dinámica y reconocer que, en ciertos contextos, por ejemplo, la circulación o comunicación de datos públicos, en tanto datos sensibles, implica riesgos que no deberían desestimarse.

3.3. Regular a través de cláusulas contractuales el acceso de terceros: acudientes, responsables económicos, patrocinadores y aseguradoras

Una situación retadora relacionada con el debido tratamiento de datos personales en IES se refiere a la expectativa de madres, padres, acudientes y pagadores de conocer el desempeño académico y otra información de estudiantes mayores de edad. Las IES suelen recibir solicitudes de acudientes o terceros que financian la educación para consultar el historial académico o disciplinario de los y las estudiantes. Sin embargo, el pago de la matrícula no faculta a los terceros a acceder a notas o reportes disciplinarios sin consentimiento del titular. En algunos casos, por ejemplo en el curso de

procesos disciplinarios, las áreas de bienestar especializadas recomiendan a las IES a que informen a los acudientes o responsables económicos sobre los pormenores del proceso, pero las áreas jurídicas pueden disentir dada la posible vulneración del derecho al habeas data del estudiante en cuestión.

Frente a estos casos, en el marco de su autonomía universitaria, las IES pueden optar por incluir en sus contratos de matrícula, o en otro documento jurídicamente vinculante, una autorización para circular o comunicar a terceros autorizados cierta información personal en casos concretos. En tales casos, se debe establecer con claridad cuál es la o las finalidades legítimas que se busca satisfacer con la circulación o comunicación de dichos datos personales y delimitar de forma precisa tales hipótesis.

En todo caso, para aquello eventos en los que no se cuente con la autorización del titular para la circulación o comunicación a terceros de sus datos personales, es importante recordar las hipótesis habilitantes del artículo 10 de la Ley 1581 de 2012, el cual sirve de guía para las actuaciones de las IES:

> ***Artículo 10.*** *Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:*
>
> a.) *Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;*
>
> b.) *Datos de naturaleza pública;*
>
> c.) *Casos de urgencia médica o sanitaria;*
>
> d.) *Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;*
>
> e.) *Datos relacionados con el Registro Civil de las Personas.*
>
> *Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.*

Uno de los supuestos en los que la ley permite circular o comunicar a terceros datos personales sin autorización del titular es en "casos de urgencia médica o sanitaria". Sobre este asunto, la Corte Constitucional en la Sentencia C-748 de 2011 indicó[4]:

> *Frente a los casos de urgencia médica y sanitaria, en aras de la efectividad del derecho a la libertad en el manejo de datos, la norma debe entenderse que opera sólo en los casos en que dada la situación concreta de urgencia, no sea posible obtener la autorización del titular o resulte particularmente problemático gestionarla, dadas las circunstancias de apremio, riesgo o peligro para otros derechos fundamentales, ya sea del titular o de terceras personas.*

4. Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Considerando las diversas situaciones de riesgo físico y bienestar emocional que enfrentan estudiantes, personal administrativo y personal docente, es posible que solo en situaciones concretas de urgencia, y siempre tras un estudio y valoración caso a caso, se comparta información con terceros sin autorización del titular, cuando gestionar dicha autorización resulte particularmente problemático. Piénsese, por ejemplo, en casos de grave afectación a la salud física o mental de los y las estudiantes.

En todo caso, como se indicó en la primera recomendación sobre "Ponderar el derecho a la protección de datos personales con otros derechos fundamentales e intereses constitucionales legítimos", el derecho fundamental a la protección de datos personales no es un derecho absoluto y no puede interpretarse como un mandato de secretismo total. Cuando no cuenten con autorización para la circulación o comunicación de información personal a terceros, las IES deben realizar un juicio de ponderación con el fin de evaluar si, en el caso concreto, los beneficios de entregar la información, teniendo en cuenta todos los elementos del contexto, superan los beneficios de mantener la confidencialidad.

3.4. Incorporar autorizaciones diferenciadas y revocables en el contrato de matrícula y en instrumentos conexos

En tanto las IES decidan realizar tratamiento de datos personales de distinto tipo y con distintas finalidades, deben contar con mecanismos de autorización y seguimiento diferenciados. Es importante contar con sistemas que permitan visualizar autorizaciones revocables y específicas para tratamientos que no son necesarios para el cumplimiento del contrato de matrícula, para el cumplimiento de deberes constitucionales y legales o para la prestación del servicio público de educación.

En los casos en que se solicite autorización para el tratamiento de datos personales con finalidades adicionales a aquellas estrictamente necesarias para la ejecución del contrato o la prestación del servicio público de educación, la autorización debe presentarse y obtenerse de manera diferenciada.

Las IES deben solicitar la autorización presentando de forma diferenciada las finalidades en al menos dos grupos: las finalidades necesarias y las finalidades accesorias. Son finalidades accesorias, por ejemplo, el envío de publicidad o la oferta de otros servicios universitarios (clubes de lectura, actividades culturales, foros académicos, suscripción a boletines, etc.).

Como parte de su derecho fundamental al habeas data, el titular puede autorizar o no el tratamiento de sus datos personales para finalidades accesorias sin que su aceptación o negativa afecte la prestación del servicio público de educación. Asimismo, el titular tiene el derecho a oponerse, en cualquier momento, al tratamiento de sus datos personales que haya sido autorizado para la realización de finalidades accesorias a la ejecución del contrato de matrícula o a la prestación del servicio público de educación, sin que su negativa afecte la continuidad del (o el acceso al) servicio principal.

3.5. Reconocer la autonomía progresiva de los menores de edad

La Convención sobre los Derechos del Niño aprobada por la Asamblea de las Naciones Unidas en 1989, e incorporada al derecho interno mediante la Ley 12 de 1991, reconoce la autonomía progresiva de los menores de edad e insta a los Estados parte a brindar mecanismos para tener en cuenta las opiniones de niños y niñas. En concreto, el artículo 12 establece:

> ***Artículo 12***
>
> 1. *Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño.*
>
> 2. *Con tal fin, se dará en particular al niño oportunidad de ser escuchado, en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional.*

En Colombia, el ordenamiento jurídico reconoce la autonomía progresiva de niños y niñas a través de distintos instrumentos. Por un lado, **el artículo 26 del Código de la Infancia y la Adolescencia (Ley 1089 de 2006)** establece que "En toda actuación administrativa, judicial o de cualquier otra naturaleza en que estén involucrados, los niños, las niñas y los adolescentes, tendrán derecho a ser escuchados y sus opiniones deberán ser tenidas en cuenta".

La jurisprudencia constitucional también ha reconocido la importancia de valorar las opiniones de los menores de edad. Por ejemplo, en el caso de la Sentencia T-302 de 2025, en el que se analizó la razonabilidad de una medida de protección adoptada por el ICBF, la Corte Constitucional reconoció que "la determinación del interés superior del NNA debe basarse en sus condiciones particulares –como su edad, grado de madurez, situación familiar, entorno social y nivel de autonomía progresiva-"[5].

No obstante lo anterior, el artículo 2.2.2.25.2.9. del Decreto 1074 de 2015 señala los requisitos especiales para el tratamiento de datos personales de menores de 18 años, e insiste en que la autorización para el tratamiento de datos personales debe otorgarse por el representante legal:

5. Corte Constitucional. Sentencia T-302 de 2025. Consideraciones 158 y 255, y resolutivo tercero. M.P. Vladimir Fernández Andrade.

> ***Artículo 2.2.2.25.2.9.*** *Requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes. El Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:*
>
> 1. *Que responda y respete el interés superior de los niños, niñas y adolescentes.*
>
> 2. *Que se asegure el respeto de sus derechos fundamentales.*
>
> ***Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.***
>
> *Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y el presente decreto.*
>
> *La familia y la sociedad deben velar porque los responsables y encargados del tratamiento de los datos personales de los menores de edad cumplan las obligaciones establecidas en la Ley 1581 de 2012 y el presente decreto.*

Ahora bien, la Superintendencia de Industria y Comercio ha determinado que cuando se realiza tratamiento de datos personales como un medio para el goce o la garantía del derecho fundamental a la educación, los adolescentes mayores de 14 años pueden autorizar válidamente el tratamiento de sus datos personales en ciertas situaciones. Cuando se recolectan datos personales para finalidades directamente relacionadas con la prestación del servicio público de educación superior es razonable que se obtenga la autorización para el tratamiento directamente de los adolescentes[6].

En el ámbito de la protección de datos personales debe reconocerse la autonomía progresiva de los menores de 18 años. Así lo reconoció la Corte Constitucional en la sentencia C-748 de 2011[7]:

> *Sumado a la efectividad del interés superior de esta población, también es importante que se les asegure su derecho a ser escuchados en todos los asuntos que los afecten; y el tratamiento de sus datos, sin duda alguna, es un asunto que les concierne directamente.*
>
> *En definitiva, siguiendo las recomendaciones que emitió el Comité [de los Derechos del Niño de las Naciones Unidas a través de la Observación General No. 12] acerca*

6. Superintendencia de Industria y Comercio, Dirección de Investigación de Protección de Datos Personales. Resolución 51290 de 2018.

7. Corte Constitucional. Sentencia C-748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

> *de esta importante garantía, la Corte considera relevante que la opinión del menor de 18 años sea siempre tenida en cuenta, pues la madurez con que expresen sus juicios acerca de los hechos que los afectan debe analizarse caso por caso. La madurez y la autonomía no se encuentran asociadas a la edad, más bien están relacionadas con el entorno familiar, social, cultural en el cual han crecido. En este contexto, la opinión del niño, niña, y adolescente siempre debe tenerse en cuenta, y el elemento subjetivo de la norma "madurez" deberá analizarse en concreto, es decir, la capacidad que ellos tengan de entender lo que está sucediendo (el asunto que les concierne) y derivar sus posibles consecuencias.*

Como indicó esta Superintendencia[8]:

> *De acuerdo con lo anterior, y teniendo como criterio de interpretación el consignado en el citado artículo 8 del Código de la Infancia y la Adolescencia, se debe buscar siempre el interés superior de los adolescentes.*
>
> *Por lo cual, y a fin de evitar que la aplicación de un derecho derive en la inaplicación de otros, se debe considerar que, en el caso específico analizado, es decir, cuando se trate del tratamiento de datos de adolescentes por parte de entidades educativas a fin de brindarles el acceso a la educación, el conocimiento, la ciencia, la tecnología, la investigación y la cultura, es posible que la autorización previa sea otorgada directamente por el estudiante.*
>
> *Dicha interpretación está en consonancia con las normas previstas en nuestro ordenamiento jurídico que reconocen el grado de madurez de los menores adultos y que les otorgan capacidad para llevar a cabo por sí mismos ciertos actos.*

En ese sentido, las IES deben respetar el derecho a ser escuchados y la autonomía progresiva de los adolescentes. Esto supone dar validez a la autorización otorgada por los adolescentes para el tratamiento de sus datos personales para finalidades relacionadas con el ejercicio de su derecho fundamental a la educación y la prestación del servicio público de educación. No reconocer la validez de estas autorizaciones y, por ende, requerir la autorización de los representantes legales para el tratamiento de sus datos personales, desconoce el derecho a ser escuchados y la autonomía progresiva que tienen los menores de edad. En conclusión, es posible que la autorización previa y expresa sea otorgada directamente por el adolescente exclusivamente para las finalidades asociadas a la prestación del servicio público de educación.

8. Superintendencia de Industria y Comercio, Oficina Asesora Jurídica. Concepto del 15 de septiembre de 2022. Radicado 22-307607.

3.6. Incorporar medidas de protección de datos desde el diseño y por defecto y de evaluación de riesgos

El despliegue de tecnologías digitales para acceder a recursos educativos o gestionar procesos administrativos es ahora común en la mayoría de las IES: correo institucional, repositorios de documentos, plataformas de videoconferencia, evaluaciones en línea y acceso a programas en la nube, entre otros. La mayoría de las veces, las IES adquieren o licencian tecnología para realizar estos procesos o contratan con proveedores externos para que sus estudiantes accedan a las plataformas.

En tales casos, es fundamental que se informe a los titulares sobre el tratamiento al que serán sometidos sus datos personales, las finalidades asociadas y el tiempo de conservación de la información. Cuando las IES recolecten datos personales por medio de plataformas digitales de forma directa o a través de terceros, se "debe incluir una autorización específica para el tratamiento de datos personales, de tal forma que las personas puedan conocer y autorizar el tratamiento específico que se va a hacer de esos datos"[9].

Ocasionalmente, las IES diseñan sus propios sistemas de información, los cuales permiten realizar tratamiento de datos personales. Cuando resulte aplicable, se deben considerar las instrucciones contenidas en la Circular Externa No. 002 de 2025 de esta Superintendencia, según la cual:

> *En el contexto de los procesos de transferencia de tecnología objeto de esta circular, la incorporación de medidas de protección de datos personales desde el diseño y por defecto es un mecanismo idóneo para concretar el principio de responsabilidad demostrada. Cuando se implementen dichas medidas, se debe considerar que:*
>
> 3.1. *La arquitectura tecnológica integre elementos o medidas orientadas al cumplimiento de los principios del tratamiento de datos personales; en especial, los principios de libertad, necesidad, seguridad, circulación restringida y confidencialidad, conforme al artículo 4 de la Ley 1581 de 2012.*
>
> 3.2. *Se adopten las medidas de seguridad pertinentes según el tipo de tecnología, los costos de implementación, la naturaleza, ámbito, contexto y fines del tratamiento, las personas aliadas o colaboradoras, así como los riesgos que entrañe dicho tratamiento para el derecho a la protección de datos personales.*

9. Corte Constitucional. Sentencia T-049 de 2023, consideración 114. M.P. Natalia Ángel Cabo.

3.3. *Se limite la recolección de datos personales a lo estrictamente necesario y se promueva la minimización del tratamiento, y la anonimización o seudonimización de los datos personales cuando ello sea posible.*

Asimismo, cuando se realice tratamiento de datos personales a través de sistemas de inteligencia artificial, las IES deben realizar un estudio de impacto de privacidad que debe contener, al menos[10]:

a.) Una descripción detallada de las operaciones de tratamiento de datos personales.

b.) Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales. En la evaluación de riesgos se espera, por lo menos, la identificación y clasificación estos.

c.) Las medidas previstas para evitar la materialización de los riesgos, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas que puedan eventualmente resultar afectadas.

La realización de estudios de impacto de privacidad es necesaria en el despliegue de sistemas de inteligencia artificial y también resulta recomendable para otros tratamientos de alto riesgo que involucren datos sensibles, perfilamiento, biometría, analítica predictiva o monitoreo masivo.

Es fundamental evaluar el nivel de riesgo y la necesidad y proporcionalidad de las soluciones tecnológicas que impliquen recolección y tratamiento de datos personales desplegadas en contextos educativos.

Por ejemplo, al estudiar la implementación de sistemas de videovigilancia en entornos universitarios, la Corte Constitucional en la Sentencia T-170 de 2025 consideró que la instalación de cámaras en las aulas era violatoria de las libertades de expresión y de cátedra de estudiantes y docentes, y en el caso concreto también lo consideró violatorio del derecho fundamental al habeas data en tanto la entidad responsable y su encargado (empresa de vigilancia) incumplieron los siguientes deberes[11]:

> *(i) solicitar y conservar prueba de la autorización de los titulares para el tratamiento de los datos, (ii) implementar sistemas de vigilancia solo cuando sea necesario para el cumplimiento de la finalidad propuesta, (iii) limitar la recolección de datos a la estrictamente necesaria para cumplir el fin específico, (iv) informar a los titulares acerca de la recolección y demás formas de tratamiento de datos, y (v) conservar imágenes por el tiempo necesario.*

10. Superintendencia de Industria y Comercio. Circular Externa No. 002 de 2024, “Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial”.

11. Corte Constitucional. Sentencia T-170 de 2025, consideración 43. M.P. Juan Carlos Cortés González.

Las IES deben implementar mecanismos de evaluación de riesgos y verificar el cumplimiento de los requisitos legales y constitucionales propios del debido tratamiento de datos personales. Asimismo, cuando se advierta una posible tensión entre finalidades legítimas (como la seguridad o la protección de derechos de terceros) con el derecho al habeas data y otros derechos o intereses constitucionales, las IES deben realizar un cuidadoso análisis de proporcionalidad y deben hacerlo antes de iniciar las actividades de tratamiento y el despliegue efectivo de sistemas de recolección masiva de datos personales a través de medios tecnológicos.

3.7. Designar un oficial de protección de datos personales

Las IES pueden designar un oficial de protección de datos personales para velar por la implementación efectiva de las políticas y procedimientos necesarios para cumplir con el régimen general de protección de datos personales. La “Guía Oficial de Protección de Datos Personales” expedida por esta Superintendencia ofrece orientaciones útiles sobre las funciones, responsabilidades, características y naturaleza del oficial de protección de datos personales.

3.8. Adoptar medidas de seguridad reforzada y responsabilidad demostrada

Las IES deben conservar la información personal que obre en sus sistemas de información, archivos o bases de datos bajo condiciones de seguridad proporcionales al riesgo y a la naturaleza de los datos. La información sensible debe encontrarse resguardada por medidas técnicas y humanas para impedir su acceso, divulgación o adulteración no autorizadas. Asimismo, es necesario contar con controles diferenciados de acceso que garanticen efectivamente que en las IES solo ciertas personas tengan acceso a la información.

El análisis de las medidas de seguridad y controles de acceso se debe realizar en cada caso concreto, en atención al nivel de riesgo, al medio en el que se encuentre la información, a la capacidad de las IES y al sistema interno de gobernanza de la información que se determine. En todo caso, las IES deben garantizar que, al realizar operaciones de transmisión de la información, se mantendrán al menos los mismos controles y medidas de seguridad. Las transmisiones de datos personales deben

encontrarse respaldadas por instrumentos jurídicos que regulen las obligaciones del encargado, las medidas de seguridad aplicables, las instrucciones del responsable y las condiciones para la devolución o eliminación de la información una vez finalice el tratamiento.

3.9. Adoptar medidas en relación con el tratamiento de datos personales realizado por estudiantes en ejercicio de actividades académicas y de investigación

En los casos de actividades de tratamiento de datos personales realizadas por estudiantes en el contexto de actividades académicas o de investigación, las IES conservan su calidad de responsables del tratamiento. Las IES ostentan tal calidad en virtud de los mandatos constitucionales y legales que rigen su actividad y porque, por lo general, en ejercicio de su autonomía universitaria, deciden y precisan las finalidades del tratamiento, y habilitan y disponen los medios para ello.

Por tanto, en aquellos casos en que estudiantes adelanten tratamiento de datos personales en ejercicio de actividades académicas o de investigación, cuando dicho tratamiento se desarrolle bajo lineamientos o instrucciones de la IES, o usando recursos, sistemas o bases de datos institucionales o en el marco de proyectos formalmente aprobados por la IES, la IES tiene el deber de establecer mecanismos de supervisión y de velar por el cumplimiento del régimen de protección de datos personales. Entre otros, la IES debe asegurar que se cuente con las autorizaciones correspondientes, se adopten las medidas de seguridad pertinentes y se disponga de otras medidas razonables para la debida protección de los derechos de los titulares.

Superintendencia de
Industria y Comercio