

SCAPE 

3M
SOFTWARE

RESUMEN EJECUTIVO	3
1. INTRODUCCIÓN Y ALCANCE DE LA POLÍTICA.....	4
2.1. Normativa Nacional.....	7
2.2. Normativa Internacional de Referencia	8
2.3. Jurisprudencia y Doctrina Relevante.....	8
3. DEFINICIONES Y GLOSARIO.....	9
4. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES	11
5. TRATAMIENTO DE DATOS PERSONALES: FINALIDADES Y BASES DE LEGITIMACIÓN.....	13
6. AUTORIZACIÓN DEL TITULAR	18
7. DERECHOS DE LOS TITULARES DE LOS DATOS (DERECHOS ARCO).....	20
8. DESTINATARIOS Y TRANSFERENCIA DE DATOS PERSONALES	23
9. MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES	25
10. PLAZO DE CONSERVACIÓN DE LOS DATOS	27
11. USO DE COOKIES.....	28
12. ROLES Y RESPONSABILIDADES	31
13. CAPACITACIÓN Y CONCIENTIZACIÓN.....	33
14. AUDITORÍA Y MONITOREO	34
15. MODIFICACIONES A LA POLÍTICA DE PRIVACIDAD.....	35
16. FECHA DE ENTRADA EN VIGENCIA	35
17. CANAL DE ATENCIÓN.....	35
18. AVISO DE PRIVACIDAD (VERSIÓN RESUMIDA)	36
19. ANEXOS.....	37
20. REFERENCIAS BIBLIOGRÁFICAS	39

RESUMEN EJECUTIVO

El presente documento establece la Política de Tratamiento de Datos Personales y la Política de Cookies del software SCAPE — Sistema de Control de Acceso de Personal y Equipos, desarrollado por 3M Software y utilizado por [Nombre de la Institución Educativa] para la gestión del control de acceso a sus instalaciones y la trazabilidad de equipos de cómputo.

La Política ha sido elaborada en estricto cumplimiento de la Constitución Política de Colombia (Artículo 15), la Ley 1581 de 2012, el Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), la Ley 1098 de 2006 (Código de la Infancia y la Adolescencia), las Circulares de la Superintendencia de Industria y Comercio (SIC) y demás normativa concordante.

El documento aborda, entre otros aspectos: el marco legal aplicable, los principios rectores del tratamiento, las finalidades y bases de legitimación por cada categoría de titulares (estudiantes, acudientes, personal docente y administrativo, visitantes), el tratamiento especial de datos de menores de edad, los derechos ARCO y su procedimiento de ejercicio, las medidas de seguridad técnicas, organizativas y administrativas, el plan de respuesta a incidentes, los plazos de conservación, el uso de cookies, los roles y responsabilidades al interior de la Institución, el plan de capacitación, la auditoría y el monitoreo permanente.

La Institución ratifica su compromiso con la protección de los datos personales de toda su comunidad educativa y con la implementación de medidas proporcionales, razonables y verificables para garantizar los derechos fundamentales de los titulares, en especial de los niños, niñas y adolescentes.

Palabras clave: protección de datos personales, Habeas Data, Ley 1581 de 2012, SCAPE, control de acceso, menores de edad, cookies, seguridad de la información, 3M Software.

1. INTRODUCCIÓN Y ALCANCE DE LA POLÍTICA

1.1. Objetivo de esta Política

El objetivo de la presente Política de Tratamiento de Datos Personales (en adelante, la "Política") es informar a los estudiantes, acudientes, docentes, personal administrativo, visitantes y demás titulares de datos, sobre las prácticas adoptadas por [Nombre de la Institución Educativa] (en adelante, "la Institución") en relación con la recolección, uso, almacenamiento, circulación, tratamiento y protección de sus datos personales capturados a través del software SCAPE — Sistema de Control de Acceso de Personal y Equipos, desarrollado por 3M Software.

Esta Política se expide en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 (compilado en el Decreto 1074 de 2015), y las circulares e instrucciones de la Superintendencia de Industria y Comercio (SIC) en materia de protección de datos personales, así como de las normas concordantes aplicables en la República de Colombia.

La Institución adopta los estándares del Reglamento General de Protección de Datos (RGPD) de la Unión Europea como referente de buenas prácticas internacionales, sin perjuicio del cumplimiento estricto de la normativa colombiana aplicable.

1.2. Alcance de la Política

Esta Política aplica a:

- Todos los datos personales recolectados, almacenados, usados, circulados o suprimidos a través del software SCAPE y herramientas afines.
- Todas las bases de datos y archivos físicos o electrónicos que contengan datos personales gestionados por la Institución.
- Todo el personal de la Institución que tenga acceso a datos personales en el ejercicio de sus funciones.
- 3M Software, en su calidad de Encargado del Tratamiento, y sus empleados, contratistas y subencargados autorizados.
- Los estudiantes, acudientes, docentes, personal administrativo, visitantes y cualquier tercero cuyos datos sean tratados a través de SCAPE.

1.3. Identidad y datos de contacto del responsable del Tratamiento

El responsable del Tratamiento de los datos personales capturados a través de SCAPE es:

Responsable: [Nombre de la Institución Educativa]

NIT: []

Domicilio: Ibagué, Tolima, Colombia

Correo electrónico: [correo del área encargada]

Teléfono: []

Encargado del Tratamiento (Desarrollador tecnológico): 3M Software — desarrollador del software SCAPE, quien trata los datos personales por cuenta y bajo las instrucciones de la Institución, conforme al contrato de prestación de servicios suscrito y al Acuerdo de Procesamiento de Datos (DPA) vigente.

1.4. Definición de roles: Institución como responsable y 3M Software como Encargado

Para efectos de la presente Política:

- La Institución actúa como responsable del Tratamiento: determina los fines y los medios del tratamiento de los datos personales que recolecta directamente de estudiantes, acudientes, docentes, administrativos y visitantes, para las finalidades de control de acceso, seguridad institucional y trazabilidad de equipos.
- 3M Software actúa como Encargado del Tratamiento: trata los datos personales únicamente siguiendo las instrucciones de la Institución, conforme a los Términos del Servicio y al Acuerdo de Procesamiento de Datos (DPA). 3M Software no utiliza dicha información para fines propios y garantiza su confidencialidad, seguridad e integridad durante la prestación del servicio.

Adicionalmente, cuando los usuarios de SCAPE (docentes, administrativos) ingresen datos personales de terceros al sistema (por ejemplo, datos de acudientes o de estudiantes), dichos usuarios actúan como responsables de esos datos y la Institución como Encargada, conforme al DPA vigente.

1.5. Vigencia y Ámbito Territorial

La presente Política rige a partir de su publicación y se mantendrá vigente mientras la Institución utilice el software SCAPE. Su ámbito territorial de aplicación es la República de Colombia, sin perjuicio de las normas internacionales que resulten aplicables en caso de transferencias internacionales de datos.

La Institución se reserva el derecho de actualizar esta Política conforme a cambios normativos, jurisprudenciales, técnicos u operativos. Las modificaciones sustanciales serán comunicadas a los titulares o sus acudientes antes de su entrada en vigor.

2. MARCO LEGAL APLICABLE

2.1. Normativa Nacional

La presente Política se rige por:

- Constitución Política de Colombia, Artículo 15 (Habeas Data): consagra el derecho fundamental de todas las personas 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.
- Ley 1581 de 2012 — Régimen General de Protección de Datos Personales: desarrolla el derecho constitucional de Habeas Data y establece las disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo: reglamenta la Ley 1581 de 2012.
- Ley 1266 de 2008 — Habeas Data financiero: aplicable cuando se trate de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- Ley 1098 de 2006 — Código de la Infancia y la Adolescencia: establece el interés superior del menor y sus derechos fundamentales.
- Ley 527 de 1999 — Comercio Electrónico: regula los mecanismos electrónicos para la manifestación del consentimiento.
- Ley 1712 de 2014 — Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 886 de 2014: reglamenta el Registro Nacional de Bases de Datos (RNBD).
- Circular Externa 002 de 2015 de la SIC: guía sobre el tratamiento de datos personales.
- Circular Externa 005 de 2017 de la SIC: sobre el tratamiento de datos de niños, niñas y adolescentes.
- Guía sobre Protección de Datos Personales para el sector educativo de la SIC.

2.2. Normativa Internacional de Referencia

Aunque no es de obligatorio cumplimiento en Colombia, la Institución adopta como estándar de buenas prácticas internacionales:

- Reglamento (UE) 2016/679 — Reglamento General de Protección de Datos (RGPD).
- Convenio 108 del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.

2.3. Jurisprudencia y Doctrina Relevante

La Corte Constitucional de Colombia, mediante diversas sentencias (T-414 de 1992, C-748 de 2011, entre otras), ha señalado que el derecho al Habeas Data comprende las facultades de conocer, actualizar, rectificar y suprimir la información personal, así como la garantía de que su tratamiento se realice conforme a los principios de legalidad, finalidad y libertad.

La Superintendencia de Industria y Comercio (SIC), como autoridad nacional de protección de datos personales, ha emitido conceptos y guías que orientan el tratamiento de datos, especialmente en el sector educativo, destacando la protección reforzada de los menores de edad y la necesidad de obtener autorización de los acudientes.

3. DEFINICIONES Y GLOSARIO

Para efectos de la presente Política, se adoptan las siguientes definiciones, basadas en la Ley 1581 de 2012 y el Decreto 1377 de 2013:

- Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y aquellos que no sean semiprivados o privados.
- Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas.
- Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- Dato sensible: aquel que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (origen racial o étnico, orientación política, convicciones religiosas, datos de salud, biometría, entre otros).
- Titular: persona natural cuyos datos personales sean objeto de tratamiento.
- 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.
- 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.
- Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- Aviso de privacidad: comunicación verbal o escrita generada por el responsable, dirigida al titular, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información.

- Base de datos: conjunto organizado de datos personales que sea objeto de tratamiento.
- Tratamiento: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recolección, almacenamiento, uso, circulación o supresión de datos personales.
- Transferencia: la transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
- Transmisión: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el Encargado por cuenta del responsable.
- Cookies: pequeños archivos de texto que el sistema SCAPE almacena en el navegador del usuario para reconocer su sesión y mantener sus preferencias.
- Menor de edad: persona que no ha cumplido los 18 años, conforme al Artículo 3 de la Ley 1098 de 2006.
- Acudiente: padre, madre o representante legal del menor de edad.
- Datos biométricos: datos personales que resultan de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural.
- Seudonimización: tratamiento de datos personales de manera que ya no puedan atribuirse a un titular sin utilizar información adicional.
- Anonimización: proceso irreversible mediante el cual los datos dejan de ser asociables a un titular.

4. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

Todo tratamiento de datos personales realizado a través de SCAPE se rige por los principios establecidos en el Artículo 4 de la Ley 1581 de 2012:

4.1. Principio de Legalidad

El tratamiento es una actividad reglada que debe sujetarse a lo establecido en la ley y en las demás disposiciones que la desarrollen. La Institución y 3M Software tratarán los datos personales únicamente conforme a las finalidades autorizadas por el titular o por la ley.

4.2. Principio de Finalidad

El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular. Las finalidades están expresamente detalladas en la Sección 5 de esta Política.

4.3. Principio de Libertad

El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

4.4. Principio de Veracidad o Calidad

La información debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

4.5. Principio de Transparencia

En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

4.6. Principio de Acceso y Circulación Restringida

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. Los datos personales, salvo información pública, no podrán estar disponibles en Internet u otros medios de divulgación masiva, salvo que el acceso sea técnicamente controlable.

4.7. Principio de Seguridad

La información debe manejarse con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

4.8. Principio de Confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

4.9. Principio de Responsabilidad Demostrada (Accountability)

La Institución y 3M Software deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, el cumplimiento de los principios y obligaciones establecidos en la Ley 1581 de 2012. Para ello, mantendrán políticas, procedimientos, registros y evidencias del tratamiento.

5. TRATAMIENTO DE DATOS PERSONALES: FINALIDADES Y BASES DE LEGITIMACIÓN

En esta sección se detallan las categorías de datos, las finalidades específicas y las bases de legitimación bajo la Ley 1581 de 2012 y el Decreto 1377 de 2013.

5.1. Estudiantes

Finalidad del Tratamiento	Datos Tratados	Base de Legitimación
Control de acceso a las instalaciones	Nombres, apellidos, tipo y número de documento, rol, grado/grupo, fotografía (opcional), fecha y hora de ingreso/salida	Consentimiento del acudiente (Art. 7 Ley 1581 / Art. 12 Decreto 1377)
Verificación de identidad en portería	Documento de identidad, código estudiantil, fotografía	Consentimiento del acudiente
Registro histórico de accesos por seguridad	Fecha, hora, punto de ingreso/salida	Interés superior del menor y seguridad institucional
Notificación a acudientes sobre eventos	Nombre del estudiante, evento, hora	Consentimiento del acudiente
Asignación y trazabilidad de equipos institucionales	Identificación del equipo asociado al estudiante	Consentimiento del acudiente / necesidad operativa
Gestión de novedades y reportes institucionales	Datos de acceso, inasistencias	Consentimiento del acudiente

5.2. Acudientes y Padres de Familia

Finalidad	Datos	Base de Legitimación
Autorización para el retiro de estudiantes	Nombre, documento, parentesco, fotografía (opcional)	Consentimiento
Notificaciones sobre ingreso/salida del estudiante	Teléfono, correo electrónico	Consentimiento
Comunicaciones institucionales	Correo, teléfono	Consentimiento / interés legítimo
Registro histórico de autorizaciones	Datos de identificación, fechas	Obligación legal / consentimiento

5.3. Personal Administrativo, Docente y de Servicios

Finalidad	Datos	Base de Legitimación
Control de acceso laboral	Nombre, documento, rol, fecha y hora	Ejecución del contrato laboral
Trazabilidad de equipos asignados	Identificación del equipo, responsable	Ejecución del contrato laboral
Seguridad institucional y auditoría	Registros de acceso, IP, logs	Interés legítimo / obligación legal
Gestión de nómina y seguridad social	Datos bancarios, identificación, información laboral	Obligación legal / ejecución del contrato
Capacitación y	Historial de formación,	Ejecución del contrato

evaluación de desempeño	de	evaluaciones	laboral
--------------------------------	-----------	--------------	---------

5.4. Visitantes y Terceros

Finalidad	Datos	Base de Legitimación
Registro de ingreso/salida	Nombre, documento, motivo de visita, hora	Consentimiento
Seguridad institucional	Registro histórico de accesos	Interés legítimo
Control de proveedores y contratistas	Datos de identificación, empresa, motivo	Interés legítimo / ejecución contractual

5.5. Datos de Equipos de Cómputo

SCAPE permite el registro y trazabilidad de equipos de cómputo asociados a personas (estudiantes, docentes o administrativos). Los datos tratados incluyen:

- Identificación del equipo: serial, placa, código interno, marca, modelo.
- Tipo de equipo: portátil, tablet, celular, otro.
- Persona asociada: nombre, documento, rol.
- Fecha y hora de ingreso/salida.
- Estado del equipo: ingreso, salida, mantenimiento.
- Observaciones y novedades registradas por portería.

Finalidad: gestionar la asignación, control, trazabilidad y seguridad de los equipos institucionales y personales que ingresan a la Institución, así como prevenir hurtos, pérdidas o usos indebidos.

Base de legitimación: consentimiento del titular o del acudiente (en caso de menores) y necesidad operativa/contractual.

5.6. Tratamiento de Datos de Menores de Edad

De conformidad con el Artículo 7 de la Ley 1581 de 2012, el Artículo 12 del Decreto 1377 de 2013, el Artículo 44 de la Constitución Política y la Ley 1098 de 2006, el tratamiento de datos de estudiantes menores de edad:

- Respetar el interés superior del menor y sus derechos fundamentales.
- Requiere la autorización previa, expresa e informada del padre, madre o acudiente legal, la cual se obtiene al momento de la matrícula y se registra en el módulo Estudiante-Acudiente de SCAPE.
- Se limita estrictamente a la finalidad de control de acceso, seguridad institucional y trazabilidad de equipos.
- El menor tiene derecho a ser escuchado en función de su edad y madurez, conforme al Artículo 26 de la Ley 1098 de 2006.
- No se recolectan datos sensibles (salud, biometría, origen étnico) salvo que exista una finalidad adicional expresa y se solicite autorización específica.
- Se prohíbe el tratamiento de datos de menores con fines publicitarios, comerciales o de perfilamiento.

La Institución garantiza que cualquier tratamiento de datos de menores se realiza con medidas reforzadas de seguridad y con el acompañamiento del acudiente en todo momento.

5.7. Tratamiento de Categorías Especiales de Datos (Datos Sensibles)

La Institución no recolecta ni trata datos sensibles a través de SCAPE, salvo en los siguientes casos excepcionales:

- Obligación legal: cuando una norma exija el tratamiento de datos de salud para el cumplimiento de obligaciones en materia de seguridad y salud en el trabajo (SST) para personal docente y administrativo.
- Consentimiento explícito: en circunstancias excepcionales y para una finalidad específica que no pueda ampararse en otra base legal.

Cualquier tratamiento de datos sensibles se realiza con medidas reforzadas de seguridad, acceso restringido y máxima confidencialidad, conforme al Artículo 6 de la Ley 1581 de 2012.

5.8. Tratamiento de Datos de Salud

SCAPE no está diseñado para almacenar datos de salud. En caso de que, por requerimiento legal (por ejemplo, en el marco del Sistema de Gestión de Seguridad y Salud en el Trabajo — SG-SST), se requiera tratar datos de salud de empleados, la Institución aplicará las siguientes garantías:

- Consentimiento explícito y por escrito del titular.
- Acceso restringido únicamente al personal autorizado (área de talento humano y SST).
- Almacenamiento separado de otras bases de datos.
- Cifrado de la información.
- Eliminación segura una vez cumplida la finalidad.

3M
SOFTWARE

6. AUTORIZACIÓN DEL TITULAR

6.1. Mecanismos de Autorización

Cuando se registre a un usuario en SCAPE (directamente o a través de su acudiente, en el caso de menores), se solicitará la aceptación expresa de esta Política mediante un mecanismo verificable que incluye:

- Casilla de verificación (checkbox) de aceptación.
- Registro de fecha y hora de aceptación.
- Identificación del medio por el cual se otorgó la autorización.
- Dirección IP desde la cual se otorgó la autorización (cuando aplique).

El solo hecho de navegar por el sitio NO se interpretará como aceptación. Se requiere una acción afirmativa y explícita del titular.

6.2. Autorización para el Tratamiento de Datos de Menores

En el caso de menores de edad, la autorización será otorgada por el padre, madre o acudiente legal al momento de la matrícula, mediante:

- Formato físico firmado por el acudiente.
- Formato electrónico con firma digital o aceptación mediante checkbox.
- Registro en el módulo Estudiante-Acudiente de SCAPE.

El acudiente podrá revocar la autorización en cualquier momento sin efectos retroactivos, salvo obligación legal de conservación.

6.3. Revocatoria de la Autorización

El titular o su representante legal podrá revocar la autorización en cualquier momento mediante solicitud escrita dirigida al correo [correo del área encargada]. La revocatoria no procederá cuando exista un deber legal o contractual de conservar los datos.

La Institución atenderá la solicitud en los términos y plazos establecidos en el Artículo 15 de la Ley 1581 de 2012.

6.4. Prueba de la Autorización

La Institución conservará las pruebas de las autorizaciones otorgadas, incluyendo registros electrónicos, formatos físicos o digitales, y podrá suministrarlas al titular cuando este las solicite.

3M
SOFTWARE

7. DERECHOS DE LOS TITULARES DE LOS DATOS (DERECHOS ARCO)

De acuerdo con el Artículo 8 de la Ley 1581 de 2012 y el Capítulo III del Decreto 1377 de 2013, el titular (o su representante legal en el caso de menores) tiene derecho a:

7.1. Derecho de Acceso

Conocer, actualizar y rectificar sus datos personales. Solicitar prueba de la autorización otorgada. Ser informado sobre el uso dado a sus datos. Acceder gratuitamente a sus datos personales que hayan sido objeto de tratamiento.

7.2. Derecho de Rectificación

Solicitar la corrección de datos inexactos, incompletos o desactualizados. La solicitud debe indicar las correcciones y aportar la documentación soporte.

7.3. Derecho de Supresión

Solicitar la eliminación de sus datos cuando no sean necesarios para la finalidad, salvo deber legal de conservarlos. La supresión implica la eliminación total o parcial de la información personal.

7.4. Derecho a la Revocatoria de la Autorización

Revocar la autorización y/o solicitar la supresión de sus datos, salvo que exista un deber legal o contractual de conservarlos.

7.5. Derecho a Presentar Quejas ante la SIC

Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la Ley 1581 de 2012, una vez agotado el trámite de consulta o reclamo ante la Institución.

7.6. Derecho a la Información

Ser informado, previa solicitud, respecto del uso que se le ha dado a sus datos personales.

7.7. Procedimiento para el Ejercicio de los Derechos

Las solicitudes podrán radicarse en:

Correo electrónico: [correo del área encargada]

Área encargada: [Secretaría / Rectoría / Área de Sistemas]

Dirección física: [Dirección de la Institución]

La solicitud debe incluir:

- Nombre y datos de contacto del titular.
- Descripción clara del derecho que desea ejercer.
- Documento que permita verificar la identidad del titular (o del acudiente en caso de menores).
- Dirección de notificación.
- Documentos que soporten la solicitud (cuando aplique).

7.8. Plazos de Respuesta

Conforme a los Artículos 14 y 15 de la Ley 1581 de 2012:

- Consultas: máximo 10 días hábiles, prorrogables 5 días hábiles más.
- Reclamos: máximo 15 días hábiles, prorrogables 8 días hábiles más.

Si la solicitud está incompleta, se requerirá al solicitante para que subsane las fallas, dentro de los 5 días siguientes a la recepción.

7.9. Modelo de Solicitud

A continuación se presenta un modelo de solicitud de ejercicio de derechos ARCO:

Yo, _____, identificado(a) con documento N.º
 _____, en calidad de titular / acudiente del menor
 _____, solicito a [Nombre de la Institución Educativa]
 el ejercicio del derecho de: () Acceso () Rectificación () Supresión () Revocatoria.
 Fundamentos: _____. Anexos:
 _____. Notificaciones al correo:

_____. Firma: _____. Fecha:
_____.

3M
SOFTWARE

8. DESTINATARIOS Y TRANSFERENCIA DE DATOS PERSONALES

La Institución no vende ni alquila datos personales a terceros. Solo comparte datos cuando es necesario para las finalidades descritas en esta Política, bajo obligaciones de confidencialidad y seguridad.

8.1. Comunicación de datos a terceros

Se podrán comunicar datos a:

- 3M Software: como Encargado del Tratamiento, para el funcionamiento, soporte y mantenimiento de SCAPE.
- Proveedores de infraestructura tecnológica: hosting, almacenamiento, bases de datos (bajo DPA).
- Autoridades públicas competentes: cuando exista obligación legal.
- Personal autorizado de la Institución: bajo control de acceso basado en roles (RBAC).
- Auditores y asesores externos: bajo estrictos acuerdos de confidencialidad.

8.2. Transferencias Internacionales de Datos Personales

En caso de que los datos sean almacenados en servidores ubicados fuera de Colombia, la Institución garantizará que se cumplan los requisitos del Artículo 26 de la Ley 1581 de 2012 y del Artículo 25 del Decreto 1377 de 2013, asegurando un nivel adecuado de protección o suscribiendo contratos de transmisión de datos con los proveedores.

Actualmente, la Institución y 3M Software almacenan los datos de SCAPE en servidores ubicados en [país/región]. Cualquier cambio será informado oportunamente a los titulares.

8.3. Transmisiones a Encargados

Las transmisiones de datos a Encargados del Tratamiento (como 3M Software) se realizan conforme al Artículo 25 del Decreto 1377 de 2013, sin requerir autorización

previa de la Superintendencia de Industria y Comercio, siempre que exista un contrato de transmisión de datos vigente.

3M
SOFTWARE

9. MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES

La Institución y 3M Software implementan medidas técnicas, organizativas y administrativas para proteger los datos personales, entre ellas:

9.1. Medidas Técnicas

- Contraseñas almacenadas mediante hash (nunca en texto plano).
- Control de acceso basado en roles (RBAC).
- Conexión cifrada (HTTPS) en el entorno de producción.
- Registros de auditoría sobre accesos a información sensible.
- Copias de seguridad periódicas de la base de datos.
- Cifrado de datos sensibles en reposo y en tránsito.
- Autenticación de dos factores (2FA) para accesos administrativos.
- Monitoreo continuo de la plataforma.

9.2. Medidas Organizativas

- Políticas internas de seguridad de la información.
- Capacitación al personal sobre protección de datos.
- Acuerdos de confidencialidad con empleados y contratistas.
- Procedimientos documentados para el tratamiento de datos.
- Designación de un responsable interno de protección de datos.
- Revisión periódica de accesos y permisos.

9.3. Medidas Administrativas

- Registro Nacional de Bases de Datos (RNBD) ante la SIC, cuando aplique.
- Contratos de transmisión de datos con Encargados.
- Evaluaciones de impacto en protección de datos (cuando aplique).
- Auditorías internas y externas.
- Plan de continuidad del negocio y recuperación ante desastres.

9.4. Plan de Respuesta a Incidentes de Seguridad

En caso de un incidente de seguridad que pueda comprometer datos personales, la Institución aplicará el siguiente protocolo:

1. Detección: identificar el incidente a través de monitoreo, alertas o reportes.
2. Contención: aislar los sistemas afectados para evitar la propagación.
3. Evaluación: determinar el alcance, los datos comprometidos y los titulares afectados.
4. Notificación: informar a la SIC y a los titulares afectados cuando exista riesgo para sus derechos.
5. Remediación: implementar medidas correctivas.
6. Documentación: registrar el incidente y las lecciones aprendidas.

9.5. Confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con la Institución. Esta obligación se extiende a empleados, contratistas, proveedores y terceros autorizados.

10. PLAZO DE CONSERVACIÓN DE LOS DATOS

Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir las finalidades descritas:

- Registros de acceso: durante [1 año lectivo / el periodo que defina la Institución], tras lo cual serán eliminados o anonimizados.
- Datos académicos y de matrícula: durante el tiempo de vinculación y los plazos legales aplicables.
- Datos de equipos: durante el tiempo de asignación y trazabilidad.
- Datos con obligación legal de conservación: por el plazo exigido por la ley.
- Datos laborales: durante la relación laboral y los plazos legales posteriores.

Una vez cumplidas las finalidades, los datos serán eliminados, anonimizados o archivados de forma segura, conforme a la Política Interna de Conservación y Eliminación de Datos de la Institución.

10.1. Criterios de Conservación

Para determinar los plazos de conservación, la Institución aplica los siguientes criterios:

- La duración de la relación con el titular (académica, laboral o contractual).
- El tiempo necesario para gestionar solicitudes, consultas, reclamos o auditorías.
- Los plazos legales de conservación (fiscal, contable, laboral, entre otros).
- El interés legítimo de la Institución para conservar información estrictamente necesaria.

10.2. Eliminación Segura

Una vez cumplidos los plazos, los datos serán eliminados mediante métodos seguros que impidan su recuperación, o anonimizados de forma irreversible.

11. USO DE COOKIES

11.1. ¿Qué son las cookies?

Las cookies son pequeños archivos de texto que SCAPE almacena en su navegador al utilizar la plataforma. Permiten reconocer su sesión, mantener sus preferencias y garantizar el funcionamiento seguro del sistema.

En Colombia no existe una ley específica sobre cookies; su uso se regula bajo la Ley 1581 de 2012, ya que una cookie que permite identificar a una persona (por ejemplo, a través de su sesión o su dirección IP) constituye un dato personal sujeto a las mismas garantías de Habeas Data.

11.2. Tipos de cookies que utiliza SCAPE

a) Cookies estrictamente necesarias (no requieren autorización)

Permiten el funcionamiento básico del sistema, como mantener iniciada la sesión de un docente, administrativo o acudiente. Sin ellas, SCAPE no puede operar correctamente.

- Cookie de sesión (ej. identificador de sesión PHP)
- Duración: mientras dure la sesión activa

b) Cookies de preferencias (requieren autorización)

Recuerdan configuraciones del usuario, como idioma o modo de visualización.

- Duración: hasta 30 días o hasta que el usuario las elimine

c) Cookies analíticas (requieren autorización)

Permiten conocer el uso general de la plataforma con fines de mejora interna (por ejemplo, módulos más consultados en el panel administrativo). No se usan para perfilar ni identificar el comportamiento individual de estudiantes.

- Duración: hasta 90 días

d) Cookies de terceros

SCAPE no instala cookies de publicidad ni de rastreo de terceros. En caso de integrarse en el futuro alguna herramienta externa que las use, se informará expresamente y se solicitará autorización previa antes de su instalación.

11.3. Consentimiento

Al ingresar por primera vez a SCAPE, se mostrará un banner visible con las siguientes opciones, todas con el mismo nivel de facilidad y visibilidad:

[Aceptar todas] [Rechazar no esenciales] [Configurar]

- El solo hecho de navegar por el sitio NO se interpretará como aceptación.
- Se requiere una acción explícita (clic) para instalar cualquier cookie distinta de las estrictamente necesarias.
- La decisión del usuario quedará registrada y podrá modificarse en cualquier momento desde el enlace "Configuración de cookies" visible en el pie de página del sistema.

11.4. Tratamiento de cookies en usuarios menores de edad

Las cookies estrictamente necesarias para el funcionamiento de la sesión de un estudiante (si aplica) se instalan sin requerir autorización adicional, al ser indispensables para el servicio. Cualquier cookie no esencial asociada a un perfil de estudiante requerirá la misma autorización del acudiente exigida para el tratamiento general de sus datos.

11.5. Cómo administrar o eliminar las cookies

El usuario puede eliminar o bloquear las cookies en cualquier momento desde la configuración de su navegador:

- Google Chrome: Configuración > Privacidad y seguridad > Cookies
- Mozilla Firefox: Opciones > Privacidad y seguridad > Cookies y datos del sitio
- Microsoft Edge: Configuración > Cookies y permisos del sitio

Tenga en cuenta que bloquear las cookies estrictamente necesarias puede impedir el correcto funcionamiento de SCAPE (por ejemplo, cerrar sesión automáticamente).

3M

SOFTWARE

12. ROLES Y RESPONSABILIDADES

12.1. De la Institución (Responsable del Tratamiento)

- Definir las finalidades y bases de legitimación del tratamiento.
- Obtener y conservar las autorizaciones de los titulares.
- Atender las consultas y reclamos de los titulares.
- Implementar medidas de seguridad.
- Registrar las bases de datos ante la SIC, cuando aplique.
- Capacitar a su personal en protección de datos.
- Suscribir contratos de transmisión de datos con Encargados.

12.2. De 3M Software (Encargado del Tratamiento)

- Tratar los datos personales únicamente siguiendo las instrucciones de la Institución.
- Implementar medidas de seguridad técnicas y organizativas.
- No utilizar los datos para fines propios.
- Notificar a la Institución sobre cualquier incidente de seguridad.
- Permitir auditorías de la Institución.
- Eliminar o devolver los datos al finalizar la relación contractual.

12.3. Del Comité de Protección de Datos

La Institución conformará un Comité de Protección de Datos, integrado por:

- El Rector o su delegado.
- El responsable del área de sistemas.
- El responsable del área jurídica o de contratación.
- Un representante de los docentes.
- Un representante de los acudientes.

El Comité se reunirá trimestralmente y tendrá las siguientes funciones: revisar la Política, evaluar incidentes, aprobar nuevas finalidades, supervisar el cumplimiento y rendir informes.

12.4. De los Titulares

- Ejercer sus derechos ARCO.
- Proporcionar información veraz y actualizada.
- Informar sobre cambios en sus datos.
- Respetar las políticas institucionales.

3M
SOFTWARE

13. CAPACITACIÓN Y CONCIENTIZACIÓN

La Institución implementará un programa anual de capacitación en protección de datos personales dirigido a:

- Personal administrativo y directivo.
- Docentes y personal de apoyo.
- Personal de portería y vigilancia.
- Personal de 3M Software con acceso a datos.

13.1. Contenidos de la Capacitación

- Fundamentos legales de la protección de datos en Colombia.
- Principios y derechos ARCO.
- Tratamiento de datos de menores de edad.
- Medidas de seguridad y buenas prácticas.
- Procedimiento de respuesta a incidentes.
- Uso responsable de SCAPE.

13.2. Periodicidad

La capacitación se realizará al menos una vez al año y será obligatoria para todo el personal con acceso a datos personales. Se llevará registro de asistencia y evaluación.

14. AUDITORÍA Y MONITOREO

La Institución realizará auditorías internas y externas para verificar el cumplimiento de esta Política y de la normativa aplicable.

14.1. Auditorías Internas

- Revisión anual de la Política.
- Verificación de autorizaciones otorgadas.
- Revisión de accesos y permisos.
- Análisis de incidentes de seguridad.
- Evaluación de contratos con Encargados.

14.2. Auditorías Externas

- Auditorías por parte de la SIC, cuando sean requeridas.
- Auditorías por parte de terceros especializados.
- Evaluaciones de impacto en protección de datos.

14.3. Indicadores de Cumplimiento

- Número de solicitudes ARCO atendidas en plazo.
- Número de incidentes de seguridad reportados.
- Porcentaje de personal capacitado.
- Número de auditorías realizadas.
- Nivel de satisfacción de los titulares.

15. MODIFICACIONES A LA POLÍTICA DE PRIVACIDAD

La Institución se reserva el derecho de modificar la presente Política según lo requiera para su funcionamiento y cumplimiento normativo. Los cambios sustanciales se comunicarán a los titulares o sus acudientes antes de entrar en vigencia, a través de medios físicos o electrónicos.

Las modificaciones serán publicadas en el sitio web de la Institución y en el sistema SCAPE. Se recomienda a los titulares revisar periódicamente la Política.

16. FECHA DE ENTRADA EN VIGENCIA

La presente Política de Tratamiento de Datos Personales fue creada el día [DD/MM/AAAA] y su última actualización corresponde al [DD/MM/AAAA]. Cualquier cambio se informará a través de los canales oficiales de la Institución y del sistema SCAPE.

17. CANAL DE ATENCIÓN

Las solicitudes relacionadas con el ejercicio de derechos de Habeas Data podrán radicarse en:

Correo electrónico: [correo/área encargada de la institución]

Dirección física: [Dirección de la Institución]

Teléfono: []

Horario de atención: [Lunes a viernes de 8:00 a.m. a 4:00 p.m.]

Tiempo de respuesta: máximo 15 días hábiles (10 días hábiles para consultas, prorrogables 5 días más).

18. AVISO DE PRIVACIDAD (VERSIÓN RESUMIDA)

El siguiente aviso de privacidad es una versión resumida de la presente Política, para informar al titular de manera clara y concisa sobre el tratamiento de sus datos personales:

[Nombre de la Institución Educativa], con NIT [_____] y domicilio en Ibagué (Tolima), es el Responsable del Tratamiento de sus datos personales. Los datos recolectados a través de SCAPE serán utilizados para: control de acceso a las instalaciones, verificación de identidad, registro histórico de accesos, trazabilidad de equipos y notificación a acudientes. Sus derechos ARCO pueden ejercerse escribiendo a [correo del área encargada]. Consulte la Política completa en [enlace].

3M
SOFTWARE

19. ANEXOS

Anexo A. Formato de Autorización para el Tratamiento de Datos de Menores

Yo, _____, identificado(a) con documento N.º _____, en calidad de padre/madre/acudiente del menor _____, autorizo de manera previa, expresa e informada el tratamiento de los datos personales del menor por parte de [Nombre de la Institución Educativa], conforme a la Política de Tratamiento de Datos Personales. Finalidades: control de acceso, seguridad institucional y trazabilidad de equipos. Firma: _____. Fecha: _____.

Anexo B. Formato de Solicitud de Ejercicio de Derechos ARCO

Yo, _____, identificado(a) con documento N.º _____, solicito el ejercicio del derecho de: () Acceso () Rectificación () Supresión () Revocatoria. Fundamentos: _____ . Notificaciones al correo: _____ . Firma: _____ . Fecha: _____.

Anexo C. Matriz de Riesgos

Riesgo	Probabilidad	Impacto	Medida de Mitigación
Acceso no autorizado a datos	Media	Alto	RBAC, 2FA, cifrado
Pérdida de datos	Baja	Alto	Copias de seguridad
Divulgación accidental	Media	Medio	Capacitación, acuerdos de

			confidencialidad
Incidente de seguridad	Baja	Alto	Plan de respuesta a incidentes
Tratamiento indebido de datos de menores	Baja	Alto	Autorización del acudiente, controles reforzados

Anexo D. Glosario de Siglas

- ARCO: Acceso, Rectificación, Cancelación y Oposición.
- DPA: Data Processing Agreement (Acuerdo de Procesamiento de Datos).
- RGPD: Reglamento General de Protección de Datos.
- RNBD: Registro Nacional de Bases de Datos.
- SIC: Superintendencia de Industria y Comercio.
- SST: Seguridad y Salud en el Trabajo.
- RBAC: Role-Based Access Control (Control de Acceso Basado en Roles).
- 2FA: Autenticación de Dos Factores.

SOFTWARE

20. REFERENCIAS BIBLIOGRÁFICAS (NORMAS APA)

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial N.º 48.587.

Congreso de la República de Colombia. (2013). Decreto 1377 de 2013, por el cual se reglamenta la Ley 1581 de 2012. Diario Oficial N.º 48.834.

Congreso de la República de Colombia. (2006). Ley 1098 de 2006, por la cual se expide el Código de la Infancia y la Adolescencia. Diario Oficial N.º 46.446.

Congreso de la República de Colombia. (2008). Ley 1266 de 2008, por la cual se dictan las disposiciones generales del Habeas Data. Diario Oficial N.º 47.219.

Congreso de la República de Colombia. (1999). Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos. Diario Oficial N.º 43.673.

Presidencia de la República de Colombia. (2015). Decreto 1074 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

Superintendencia de Industria y Comercio. (2015). Circular Externa 002 de 2015.

Superintendencia de Industria y Comercio. (2017). Circular Externa 005 de 2017.

Superintendencia de Industria y Comercio. (2019). Guía sobre Protección de Datos Personales para el sector educativo.

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011.

Corte Constitucional de Colombia. (1992). Sentencia T-414 de 1992.

Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 — Reglamento General de Protección de Datos (RGPD).