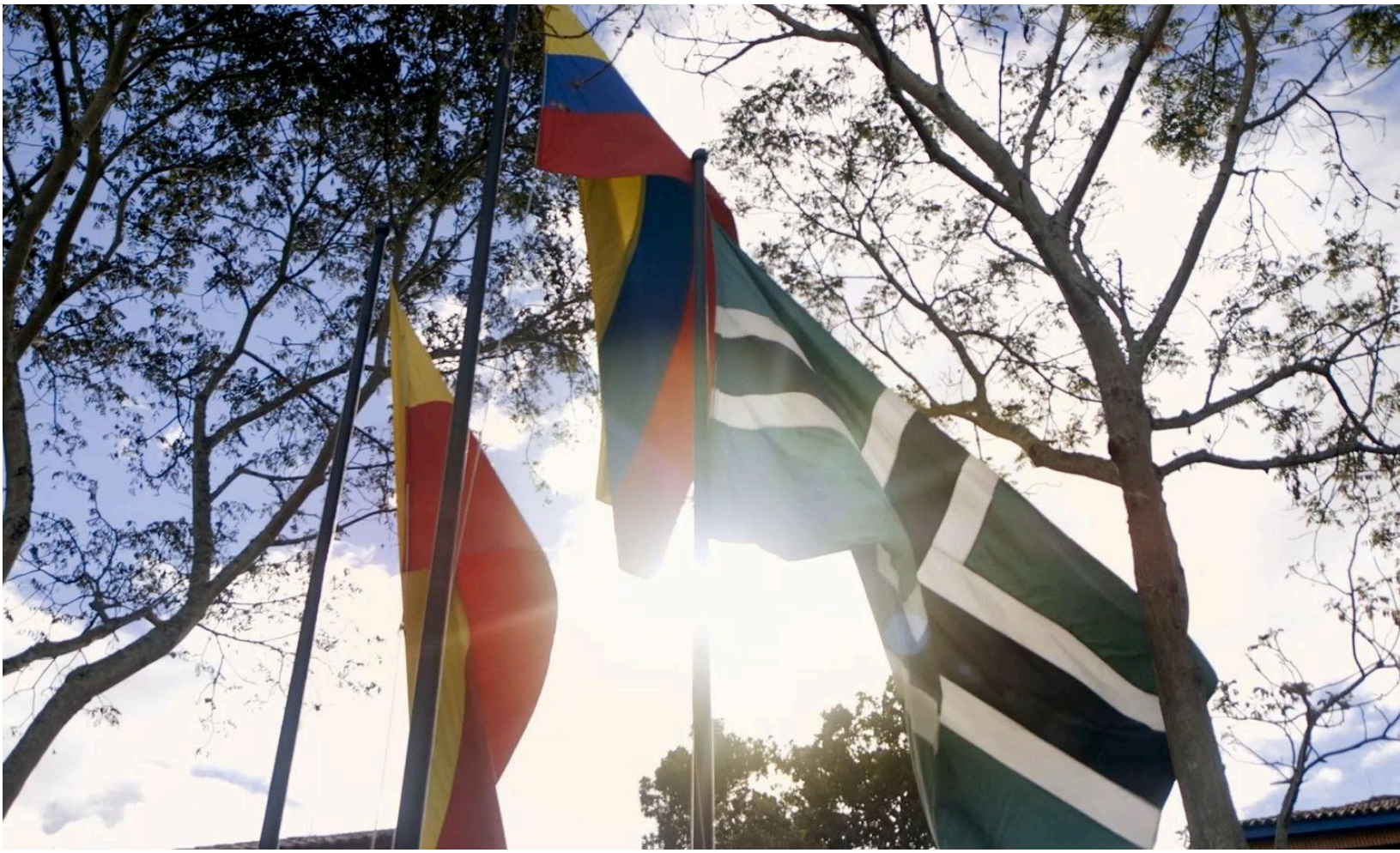

Manual interno de políticas y procedimientos de protección de datos

COLEGIO LOS NOGALES

Corporación Educativa Los Nogales

MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Versión 1.0

INDICE

1. INTRODUCCIÓN 3
2. MARCO NORMATIVO 3
3. DEFINICIONES 5
4. PRINCIPIOS 7
5. DEBERES COMO RESPONSABLE O ENCARGADO DEL TRATAMIENTO 8
6. RESPONSABILIDAD DEMOSTRADA Y ESTRUCTURA ADMINISTRATIVA 11
7. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES 12
8. PROGRAMA DE ENTRENAMIENTO 13
9. TRATAMIENTO DE DATOS PERSONALES Y REQUISITO DE AUTORIZACIÓN (Formatos e Información General) 13
10. FLUJOS DE INFORMACIÓN PERSONAL CON TERCEROS 14
11. EJERCICIO DE DERECHOS DE LOS TITULARES Y GESTIÓN DE PETICIONES, QUEJAS, RECLAMOS Y DENUNCIAS – ADOPCIÓN DE PROCESOS 15
11.1. Requisitos de evaluación de las Consultas y Reclamos 16
11.2. Procedimiento de atención de Consultas 16
11.3. Procedimiento de atención de Reclamos 17
12. PARÁMETROS DE COMPORTAMIENTO DE EMPLEADOS Y CONTRATISTAS –-PERSONAL- EN RELACIÓN CON LOS DATOS PERSONALES 17
13. SEGURIDAD DE LA INFORMACIÓN 19
14. PROCEDIMIENTO PARA INFORMAR A LA AUTORIDAD VIOLACIONES EN LOS CÓDIGOS DE SEGURIDAD 19
14.1. Acciones por tomar en el evento de incidentes de seguridad: 19
14.2. Plantilla para realizar reportes de incidentes de seguridad: 20
15. PROCEDIMIENTO DE ACTUALIZACIÓN DE LA INFORMACIÓN INGRESADA AL REGISTRO NACIONAL DE BASES DE DATOS 22
15.1. Procedimiento para la actualización de la información ingresada al RNBD 22
16. PROCEDIMIENTO PARA ATENDER REQUERIMIENTOS Y VISITAS DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO 24

1. INTRODUCCIÓN

El presente Manual Interno para el Tratamiento de Datos Personales (el "Manual") aplica para la Corporación Educativa Los Nogales (en adelante el "Colegio") incluyendo a su personal directivo, administrativo, logístico, de soporte al negocio (el "Personal"), sea mediante contrato laboral o vínculo de cualquier otra naturaleza, con el objetivo de generar conciencia en el ámbito profesional, académico y desarrollo normal del negocio, en cuanto a la necesidad de usar correctamente Datos Personales en cumplimiento a la norma vigente en la materia, Ley 1581 de 2012, normas complementarias y otras que pudiesen ser aplicables al Colegio.

Las directrices planteadas en el presente manual propenden por que el personal se familiarice con la existencia, observación y respeto a las normas de protección de datos personales, generando una conciencia colectiva de la utilización positiva y ordenada de este tipo de información, además de constituir parámetros de estricto cumplimiento.

2. MARCO NORMATIVO

El marco normativo y doctrinal a la fecha de entrada en vigencia del presente Manual es el siguiente:

2.1. Ley Estatutaria 1581 de 2012: Establece los principios generales aplicables a cualquier tipo de tratamiento de datos personales, incluyendo datos sensibles y datos de menores de edad, los deberes y obligaciones del responsable y encargado del tratamiento de la información, las consideraciones relativas a la solicitud de autorización o consentimiento de los titulares de la información y establece las reglas relacionadas con la transferencia de datos personales. Así mismo, incluye los derechos de los titulares y los mecanismos para hacerlos efectivos, así como el régimen sancionatorio aplicable, entre otros.

En virtud de la Ley 1581 de 2012, la Superintendencia de Industria y Comercio (en adelante la "SIC") tiene la facultad de iniciar investigaciones administrativas en contra de responsables o encargados del tratamiento de datos personales que presuntamente se encuentren en incumplimiento de las regulaciones en la materia. La verificación de un incumplimiento puede acarrear sanciones que comprenden:

i. Multas de hasta 2.000 salarios mínimos legales vigentes;
ii. Orden de suspensión, hasta por seis (6) meses, de todas las actividades relacionadas con el tratamiento de los datos personales y la indicación de los correctivos a ser implementados;

iii. El cierre temporal de las operaciones relacionadas con el tratamiento de datos personales si el Colegio no cumple con las medidas correctivas ordenadas; y

iv. El cierre permanente e inmediato de las operaciones de tratamiento de datos personales.

2.2. Decreto 1377 de 2013[1]: Decreto reglamentario de la Ley 1581 de 2012, que agrega nuevas reglas relacionadas con la transmisión de datos personales de un responsable a un encargado del tratamiento de la información, regula las autorizaciones para el tratamiento de datos sensibles, los requisitos de forma del aviso de privacidad y la política de tratamiento de datos personales, así como el principio de responsabilidad demostrada.

2.3. Decreto 886 de 2014: Decreto reglamentario de la Ley 1581 de 2012 que agrega disposiciones sobre el Registro Nacional de Bases de Datos (en adelante el "RNBD") como obligación del responsable de las mismas y de la información contenida en ellas. El 3 de noviembre de 2015, la SIC emitió instrucciones para poner en funcionamiento el RNBD. Compilado en el capítulo 26 del Decreto 1074 de 2015.

La creación del RNBD implica que los responsables del tratamiento de los datos personales, que cumplan las características definidas por la normatividad aplicable (actualmente en el Decreto 090 de 2019) tendrán que remitir a través de una plataforma web la información relacionada con el procesamiento de sus bases de datos personales. Adicionalmente mediante la Circular Externa No. 003 de agosto de 2018 la SIC expidió instrucciones específicas sobre el RNBD y la plataforma que lo soporta.

2.4. Circular Externa No. 3 de agosto de 2018: En virtud de la cual se modifican los numerales 2.1 al 2.4 y se eliminan los numerales 2.5 al 2.7 del Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio relacionado con el RNBD, teniendo en cuenta lo señalado en el Decreto 090 de 2018 que modificó los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015. En esta Circular se establece el nuevo universo de las entidades obligadas a inscribir sus bases de datos, cuyo tratamiento manual o automatizado sea realizado por los responsables del tratamiento que reúnan las siguientes características: i) sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario; ii) personas jurídicas de naturaleza pública.

[1] (Compilado en el capítulo 25 del Decreto Único 1074 de 2015)

2.5. Decreto 090 de 2018: Por medio del cual se modifica el ámbito de aplicación y el plazo señalado en los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015, con el fin de reducir el universo de vigilados que deben cumplir con la obligación de registrar sus bases de datos en el RNBD.

2.6. Guía de implementación del principio de responsabilidad demostrada emitida por la SIC: Instructivo publicado por la autoridad competente en materia de protección de datos con miras a brindar orientación en la construcción de un Programa Integral de gestión de datos personales y que tiene como destinatarios a las personas sometidas al cumplimiento del régimen general de protección de datos personales y, por ende, vigilados por la SIC.

Para el cumplimiento del Colegio como organización de los mandatos legales en materia de protección de datos, lo invitamos a conocer el contenido de este Manual, el cual es de obligatorio cumplimiento por parte del personal del responsable. En el caso de ejercicio de queja, rectificación, actualización, consulta, o solicitud de acceso o de sustracción de datos, usted deberá remitirla al correo electrónico: protección_datos@nogales.edu.co

3. DEFINICIONES

Para la comprensión e interpretación del presente manual se tomarán como definiciones las siguientes:

3.1. Base de Datos: conjunto organizado de datos personales objeto de tratamiento.

3.2. Cliente: Toda persona que adquiere un producto o servicio con el Colegio o con quien se sostiene una relación contractual/obligacional diferente al personal, como los estudiantes, padres de familia, estudiantes aspirantes, padres de familia aspirantes y exalumnos.

3.3. Dato Personal**:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, que las identifique o las haga identificables.

3.4. Datos Sensibles**:** Aquellos datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

3.5. La Corporación Educativa Los Nogales: El Colegio como organización y todo su personal, quienes para los efectos del presente manual serán los responsables de cumplir con las directrices aquí planteadas y con la norma aplicable a la protección de datos personales.

3.6. Encargado del Tratamiento o Encargado**:** 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 Colegio como responsable del tratamiento de los datos personales.

3.7. Ley aplicable**:** Se refiere a todos los cuerpos normativos que le son aplicables al Colegio en materia de protección de datos o privacidad.

3.8. Manual: Es el presente documento, en el cual se presentan las políticas internas del Colegio para el manejo de datos personales.

3.9. Política de Privacidad o de Tratamiento de Datos Personales "PTDP"**:** Se refiere al documento que recoge los parámetros y conductas del Colegio en relación con el tratamiento de datos personales de conformidad con los lineamientos de la legislación vigente en la materia.

3.10. Proveedor: Toda persona natural o jurídica que preste algún servicio al Colegio en virtud de una relación contractual/obligacional.

3.11. Responsable del Tratamiento o Responsable**:** 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 personales, para efectos de esta política, ejercerá como responsable, en principio, el Colegio.

3.12. Titular**:** Persona natural cuyos datos personales sean objeto de tratamiento, ya sea cliente, usuario, proveedor, empleado, o cualquier tercero que, en razón o con ocasión de una relación comercial o jurídica suministre datos personales al Colegio.

3.13. Transferencia**:** Se refiere al envío por parte del Colegio como responsable, a un tercer agente o persona natural/jurídica (receptor) también en calidad de responsable, dentro o fuera del territorio nacional para el tratamiento efectivo de datos personales. Así mismo, incluye los eventos en que el Colegio actúe como un responsable receptor de datos personales, enviados por otro responsable, domiciliado o no en el territorio colombiano.

3.14. Transmisión**:** Se refiere a la comunicación de datos personales por parte del responsable al encargado, ubicado dentro o fuera del territorio nacional, para que el Encargado, por cuenta del responsable, proceda con el tratamiento de datos personales.

3.15. Tratamiento**:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como, pero sin limitarse, a la recolección, almacenamiento, uso, circulación o supresión.

Para el entendimiento de los términos que no se encuentran incluidos dentro del listado anterior, se aplicará la legislación vigente, en especial la Ley 1581 de 2012 y sus decretos reglamentarios, otras normas complementarias, así como cualquier otra normativa aplicable al Colegio con relación a la protección de datos personales, dando el sentido utilizado en éstas a los términos de cuya definición exista duda alguna.

4. PRINCIPIOS

A fin de dar correcto cumplimiento a la norma que reglamenta la materia, el Colegio observará los siguientes principios, siempre que proceda con el tratamiento de datos personales y de bases de datos constituidas por los mismos:

4.1. Principio de legalidad**:** El tratamiento de datos personales es una actividad que debe sujetarse a lo establecido en las normas que reglamentan la materia.

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 por los medios previstos normativamente.

4.3. Principio de libertad**:** El tratamiento sólo 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 sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. El Colegio debe abstenerse de proceder con el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

4.5. Principio de temporalidad de la información: La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad de la base de datos.

4.6. Principio de transparencia**:** En el tratamiento debe garantizarse el derecho del titular a obtener del responsable o del encargado, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan de conformidad con las normas que reglamentan este acceso.

4.7. Principio de acceso y circulación restringida**:** El tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley aplicable, para lo cual el Colegio debe adelantar las acciones necesarias para obtener la correspondiente autorización del titular en cuanto sea necesario.

4.8. Principio de seguridad**:** La información sujeta a tratamiento por el Colegio en calidad de responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los datos evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

4.9. Principio de confidencialidad**:** Todo el personal del Colegio y otros que intervengan en el tratamiento de datos personales en nombre y representación del Colegio, están obligados a garantizar la reserva de la información.

4.10. Principio de responsabilidad demostrada: Al recolectar y realizar el tratamiento de datos personales, el Colegio implementará medidas apropiadas y efectivas para cumplir con las obligaciones establecidas por la Ley aplicable.

5. DEBERES COMO RESPONSABLE O ENCARGADO DEL TRATAMIENTO

Siempre que se haga referencia a obligaciones, deberes o acciones a llevar a cabo por parte del Colegio, deberá comprenderse que su recurso humano debe adelantar las conductas y comportamientos necesarios para cumplir con las mismas. Es necesario destacar que la inobservancia de la norma aplicable o del contenido de este Manual puede implicar investigaciones administrativas en contra del Colegio y en casos excepcionales, de sus funcionarios.

En consecuencia, un esfuerzo conjunto en la detección de conductas contrarias y en la socialización de dichos comportamientos adquiere real importancia al interior del Colegio. De ese modo, lo invitamos a informar al Oficial de Protección de Datos Personales ("OPDP"), sobre cualquier evento o situación que pueda ser contrario a lo aquí dispuesto o que le genere preguntas. Lo anterior con el propósito de que el Colegio pueda tomar las medidas pertinentes y de esa forma mejorar y cumplir, como organización, con la legislación aplicable a la protección de Datos Personales.

De conformidad con la Ley Estatutaria 1581 de 2012, sus Decretos Reglamentarios, la guía para la implementación del principio de responsabilidad demostrada y demás normas reglamentarias, el Colegio podrá fungir como responsable o encargado, según corresponda, de acuerdo con las definiciones indicadas en este Manual. Para esos efectos, en sus procedimientos deberá observar el cumplimiento de las siguientes obligaciones de acuerdo con el rol aplicable a el Colegio para cada situación en particular:

5.1. Responsable del Tratamiento**:** El Colegio actuará como responsable del tratamiento de las bases de datos personales sobre bases de datos (cuando estas comprendan datos de personas naturales) tales como, pero sin limitarse a: bases de datos del personal, proveedores, clientes, entre otros. De acuerdo con la Ley 1581 de 2012, los deberes del Colegio en calidad de responsable frente a esas bases de datos son:

i. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
ii. Solicitar y conservar, en las condiciones previstas en las normas aplicables, copia de la respectiva autorización otorgada por el Titular.

iii. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

iv. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

v. Garantizar que la información que se suministre al encargado (en caso de existir) sea veraz, completa, exacta, actualizada, comprobable y comprensible.

vi. Actualizar la información, comunicando de forma oportuna al encargado, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

vii. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

viii. Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado.

ix. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

x. Tramitar las consultas y reclamos formulados por los titulares.

xi. Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

xii. Informar a solicitud del titular sobre el uso dado a sus datos personales.

xiii. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

xiv. Reservarse el derecho de proceder con auditorías frente al tratamiento dado por terceros encargados, así como asegurarse que los mismos cumplen con los principios que tutelan el tratamiento de datos personales y su acogimiento a la normatividad colombiana.

xv. Contar con mecanismos y procedimientos para la respuesta a incidentes que afecten o amenacen la seguridad e integridad de datos personales y bases de datos por constituidas con los mismos.

5.2. Encargado del Tratamiento**:** El Colegio únicamente actuará como encargado cuando sea receptor de datos personales y realice el tratamiento por cuenta y riesgo de un tercero responsable.

También es posible que, como parte de su rol como responsable, el Colegio transmita los datos personales a terceros que también tendrán la calidad de encargados. En

este evento, dichos terceros también deberán cumplir, respecto del Colegio como responsable, con los deberes que más adelante se precisan.

Para mayor claridad de las responsabilidades que este rol puede comprender, es importante tener en cuenta los deberes del encargado, los cuales se precisan a continuación:

i. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.
ii. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
iii. Realizar oportunamente la actualización, rectificación o supresión de los datos personales.
iv. Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
v. Tramitar las consultas y los reclamos formulados por los titulares.
vi. Registrar en la base de datos la leyenda "reclamo en trámite" cuando esto sea aplicable.
vii. Insertar en la base de datos la leyenda "información en discusión judicial" una vez sea notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
viii. Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
ix. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
x. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
xi. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Bajo las anteriores obligaciones, especialmente cuando el Colegio actúe como responsable, es importante que el personal tenga en cuenta el siguiente punto clave y requisito para el tratamiento de los datos personales: deben obtener, en principio, la autorización previa, expresa e informada del titular. Por regla general, cualquier forma de tratamiento de datos personales requiere la autorización previa, expresa e informada del titular salvo ciertas excepciones.

Así las cosas, siempre que el personal proceda con iniciativas o acciones tendientes a recolectar datos personales será necesario que acuda al Oficial de Protección de Datos del Colegio para decidir los pasos a seguir. El rol y funciones del OPDP de la Protección de Datos Personales se explica de manera más detallada en el numeral 7 de este documento.

6. RESPONSABILIDAD DEMOSTRADA Y ESTRUCTURA ADMINISTRATIVA

En su calidad de responsable del tratamiento de datos personales, el Colegio comprende la importancia de dar cumplimiento al principio de responsabilidad demostrada desarrollado por el Decreto 1377 de 2013 y por la Guía para la Implementación del principio de responsabilidad demostrada.

En razón a lo anterior, han implementado medidas y/o políticas internas apropiadas y efectivas para dar cumplimiento a la Ley 1581 de 2012, en cuanto a la protección integral de datos personales. Como parámetro para el planteamiento de estas medidas se ha seguido lo establecido del artículo 27 del Decreto 1377 de 2013 al exigir que las medidas deben garantizar:

6.1. La existencia de una estructura administrativa proporcional a la estructura y tamaño del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y el Decreto 1377 de 2013.

6.2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

6.3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.

Así las cosas, el Colegio en consideración a su estructura administrativa ha procedido con la implementación de medidas efectivas a fin de poder demostrar a la autoridad competente, y poner en conocimiento de su personal, la protección proactiva -más no reactiva- de datos personales sobre los cuales el Colegio ostenta la calidad responsable del tratamiento.

El Colegio ha adoptado un grupo de trabajo de protección de datos personales al interior de la organización, quien se encarga de sesionar sobre las oportunidades de mejora del programa integral de gestión de datos personales del Colegio y adicionalmente realizar actividades de identificación de posibles brechas en materia de seguridad en conjunto con las áreas internas de del Colegio. El personal del Colegio, podrá, en cualquier momento, llevar al grupo de trabajo de

protección de datos personales sus inquietudes o comentarios relacionados con el cumplimiento de la normativa de privacidad.

7. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

El Decreto 1377 de 2013 (compilado en el Capítulo 25 del Decreto Único 1074 de 2015) establece la obligación a cargo de todos los responsables y encargados del tratamiento de designar a un área o persona para que asuma la función de velar por la protección de datos personales. De conformidad con lo anterior y la Guía de Responsabilidad Demostrada, el Colegio ha designado a la Secretaría Académica como Oficial de Protección de Datos Personales (o el "OPDP" o el "Oficial") como parte de su operación en Colombia. El área de OPDP del Colegio es adecuada y proporcional para su estructura administrativa y su tamaño institucional. Los principales deberes del Oficial son los siguientes:

7.1. Coordinar la atención y respuesta a las peticiones, consultas y reclamos mediante los cuales el titular de la información ejerza los derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

7.2. Impulsar una cultura de protección de datos dentro del Colegio.

7.3. Socializar la Política de Tratamiento de Datos Personales ("PTDP") del Colegio y ponerla a disposición de terceros cuando así sea requerido.

7.4. Prestar colaboración para la integración de las PTDP dentro de las actividades de las demás áreas del Colegio.

7.5. Servir de enlace y coordinador con las demás áreas del Colegio para el cumplimiento de la normativa de protección de datos personales.

7.6. Prestar apoyo en cuanto a la estructuración de contratos de transmisión de datos personales que deban suscribirse.

7.7. Desarrollar un programa de capacitación en protección de datos personales para personal nuevo, o de actualización y ajustes en la materia.

7.8. Llevar registros de la participación en los entrenamientos de protección de datos para posterior conocimiento de la alta dirección del Colegio.

7.9. Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realicen las autoridades competentes en materia de protección de datos personales, tales como la SIC.

7.10. Llevar un control y registro de los entrenamientos y/o capacitaciones que se lleven a cabo por parte del Colegio a fin de actualizar a sus integrantes en cuanto a la protección de datos personales a través del programa integral de gestión de datos personales del Colegio.

7.11. Mantener un inventario de las bases de datos personales en poder de la organización en línea con el RNBD.

7.12. Registrar las bases de datos de la organización en el RNBD y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC

8. PROGRAMA DE ENTRENAMIENTO

El Colegio ha desarrollado un programa de entrenamiento en el cual se actualiza al Personal, Proveedores entre otros, en cuanto a los deberes y derechos derivados de la norma de protección de Datos Personales.

Este programa se ejecuta de la siguiente manera:

8.1. Procedimiento de inducción a nuevos empleados y/o contratistas**:** El personal contratado tiene un proceso de inducción del cual hará parte una capacitación y/o entrenamiento en datos personales para informar a los nuevos empleados sobre las obligaciones legales a cargo del Colegio en materia de datos personales, así como para socializar el contenido del presente Manual y sus PTDP.

8.2. Actualización y/o capacitación anual**:** Como parte del ejercicio de las funciones del personal, es obligatoria la asistencia de los empleados a una capacitación y/o actualización anual en materia de protección de datos personales. En la misma se informan cambios normativos y se socializan los cambios que pudiese haber ocurrido del presente Manual.

De todas las anteriores gestiones/entrenamientos se llevará a cabo el diligenciamiento de una lista de asistencia en soporte al acta que relacione el contenido de cada entrenamiento, tarea a cargo del OPDP.

9. TRATAMIENTO DE DATOS PERSONALES Y REQUISITO DE AUTORIZACIÓN (Formatos e Información General)

De acuerdo con la normatividad colombiana vigente se requiere, por regla general y salvo ciertas excepciones, la autorización previa, expresa e informada del titular para la recolección y posterior tratamiento de sus datos personales. Esto aplica a cualquier dato personal que deba tratarse en cualquiera de las áreas del Colegio, pero sin limitarse a, proveedores, clientes, potenciales clientes y personal.

Aun cuando en muchas ocasiones exista una norma legal que requiere la recolección de la información, y por transparencia con el titular, el Colegio en aras de promover la cultura

de privacidad y protección de datos personales ha decidido como procedimiento interno solicitar, en algunos casos, la autorización o generar avisos de privacidad, informando así al titular la existencia de la Política de Tratamiento de Datos Personales aplicable y las finalidades para el uso de sus datos personales.

El propósito de este mecanismo interno es proveer de herramientas de fácil acceso a las diferentes áreas del Colegio cuando requieran gestionar datos personales en cualquiera de sus procesos. En caso de requerirse formatos adicionales, el OPDP se encargará de hacerlos parte integral del presente Manual mediante seguimiento a las actualizaciones del mismo.

Todas las áreas del Colegio deberán observar las siguientes reglas al momento de recolectar, conservar o realizar cualquier operación de tratamiento que involucre datos personales:

9.1. La autorización debe ser obtenida de manera previa al inicio del tratamiento de datos personales por parte del Colegio.

9.2. La autorización debe ser obtenida por un medio que permita consulta posterior sobre su contenido y alcance. Por ejemplo, en formato físico, formato digital, medio electrónico, e incluso a través de un acto inequívoco que permita interpretar el consentimiento -sin lugar a dudas o interpretaciones- por parte del titular.

9.3. La autorización debe ser almacenada durante el tiempo que los datos personales reposen en las bases de datos del Colegio, es decir, por el término de vida útil del dato personal y el tiempo durante el cual se continúe realizando el tratamiento de esos datos.

9.4. En caso de existir dudas relacionadas con la recolección de datos personales se debe realizar la consulta al OPDP, quien dará instrucciones y respuesta a la misma.

9.5. Si los datos personales que se desea recolectar son relacionados con la salud, intereses políticos, hábitos, orientación sexual o política, imágenes faciales o datos biométricos, entre otros, debe consultarse previamente con el OPDP, quien deberá evaluar la conveniencia de esa recolección, considerando que se trata de datos sensibles y merecen protección especial. En caso de ser procedente, el OPDP prestará colaboración para la elaboración del texto de autorización para el tratamiento de datos sensibles, precisando el carácter facultativo de esta autorización, lo cual se realizará caso a caso.

9.6. En caso de tener preguntas o ser requerido por un titular para dar información relacionada con el tratamiento de datos personales, es necesario dirigir de forma inmediata la consulta al OPDP quien es el canal institucional para esos fines.

10. FLUJOS DE INFORMACIÓN PERSONAL CON TERCEROS

El Colegio podrá realizar la transmisión de datos a otros encargados del tratamiento dentro o fuera del país cuando así esté autorizado por el titular de la información, por un contrato o cláusula de transmisión o por la ley o por un mandato administrativo o judicial.

A su turno, el Colegio podrá realizar la transferencia de datos a otros responsables del tratamiento dentro o fuera del país cuando así esté autorizado por el titular de la información o ante la configuración alguna de las causales de excepción establecidas por la Ley aplicable.

10.1. Para la Transferencia de datos se deberán observar las siguientes condiciones (aplica para eventos de recepción y comunicación de información personal):

- No se podrá realizar una transferencia de datos personales (o recibir los mismos a título de transferencia por parte de un tercero) sin antes verificar con el OPDP la existencia de la autorización previa e informada del titular o la configuración de las excepciones que establece la ley aplicable, a saber:

  - ✓ Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública;
  - ✓ Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
  - ✓ Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
  - ✓ Transferencias necesarias para la ejecución de un contrato entre el titular y el Colegio, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular;
  - ✓ Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

10.2. Para la Transmisión de datos se deberán observar las siguientes condiciones (aplica para eventos de recepción y comunicación de información personal):

- Las transmisiones de datos deben ser informadas y autorizadas por el titular. Para tal efecto, se debe incluir la finalidad dentro de la autorización para el tratamiento.
- Se debe verificar que exista un contrato o cláusula de transmisión de datos personales con el encargado del tratamiento.
  En el caso en el que el Colegio actúe como encargado del tratamiento, se deberá solicitar al responsable del tratamiento la suscripción de un contrato de transmisión o la inclusión de dicha cláusula en el contrato principal, para efectos de limitar la responsabilidad del Colegio de cara al eventual tratamiento de datos personales.

Nota: Ante cualquier evento de comunicación y/o recepción de datos personales, el personal deberá comunicarse de manera previa con el OPDP.

11. EJERCICIO DE DERECHOS DE LOS TITULARES Y GESTIÓN DE PETICIONES, QUEJAS, RECLAMOS Y DENUNCIAS – ADOPCIÓN DE PROCESOS

De acuerdo con la ley aplicable, el Colegio tiene la obligación de atender las solicitudes, consultas y reclamos que presenten los titulares en ejercicio de sus derechos a conocer, acceder de forma gratuita, actualizar, rectificar, suprimir sus datos personales, solicitar prueba y revocatoria de la autorización otorgada, ser informado respecto al tratamiento que se le ha dado a los datos y denunciar el incumplimiento de las normas que rigen la materia.

En ese sentido, el Colegio está comprometido a dar respuesta a los titulares de los datos personales como se expondrá a continuación y en todo caso respetará los límites temporales establecidos por la Ley 1581 de 2012. Igualmente, es responsabilidad del personal del Colegio remitir cualquier solicitud que reciba con relación al tratamiento de datos personales de los titulares al OPDP al siguiente canal electrónico: protección_datos@nogales.edu.co

11.1. Requisitos de evaluación de las Consultas y Reclamos

Antes de atender cualquier consulta y reclamo, el OPDP del Colegio debe confirmar el vínculo que guarda la persona que envía la consulta o el reclamo con los datos personales, ello con el fin de corroborar que quien pretende ejercer el derecho es uno de los sujetos facultados por la ley para ejercer los derechos de los titulares, a saber:

- El titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Los causahabientes del titular, quienes deberán acreditar tal calidad.
- El representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Los padres o acudientes en el caso de los menores de edad, quienes deberán acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

Igualmente, se deberá identificar los hechos que dieron lugar al reclamo o consulta, la petición formal elevada por el interesado, el contenido los documentos que se quieren hacer valer, y los datos de contacto donde se espera la respuesta: email o dirección física.

11.2. Procedimiento de atención de Consultas

Cuando los titulares realicen consultas, es decir, que envíen solicitudes a el Colegio manifestando su intención de querer conocer/acceder los datos que sobre ellos reposan en las bases de datos del Colegio, el tratamiento que se le ha dado a sus datos, así como si desean obtener la prueba de la autorización para el tratamiento de sus datos personales, el Colegio como responsable del tratamiento, suministrará a dichas personas toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

La consulta se recibirá a través de los canales habilitados por el Colegio y será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la solicitud.

Cuando no fuere posible atender la consulta dentro de dicho término, el OPDP del Colegio le informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, que en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

11.3. Procedimiento de atención de Reclamos

Cuando los titulares realicen reclamos, es decir que envíen solicitudes a el Colegio manifestando su intención de corregir, actualizar, suprimir, revocar su autorización del tratamiento de los datos o cuando indiquen el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley aplicable, dichas peticiones serán tramitadas bajo los siguientes parámetros:

(i) Se confirmará que el reclamo esté completo acorde a los requisitos contenidos en el numeral 11.1.
(ii) Si el reclamo resulta incompleto, se informará al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas.
(iii) Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
(iv) En caso de que quien reciba el reclamo no sea competente para resolverlo, enviará la solicitud al OPDP al correo electrónico protección_datos@nogales.edu.co en un término máximo de dos (2) días hábiles e informará la situación al interesado.
(v) Una vez recibido el reclamo completo, en un término no mayor a dos (2) días hábiles se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y las causas que lo motivaron. Dicha leyenda deberá mantenerse hasta que el reclamo sea resuelto de fondo.
(vi) El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.
(vii) Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

El Colegio llevará un registro semestral del número de reclamos que haya recibido, incluyendo la petición de fondo de cada uno de ellos, con el objetivo proceder a llevar a cabo correctamente los reportes semestrales de reclamos ante la SIC en la plataforma del RNBD.

12. PARÁMETROS DE COMPORTAMIENTO DE EMPLEADOS Y CONTRATISTAS – PERSONAL – EN RELACIÓN CON LOS DATOS PERSONALES

Como parte del compromiso de la alta dirección del Colegio se han adoptado ciertas reglas en cuanto al uso de datos personales y bases de datos de propiedad del Colegio por parte del personal. Así las cosas, y con el interés principal de transmitir un mensaje claro e integral bajo el

cual se compromete el Colegio dando lugar a una cultura de privacidad consolidada, se han diseñado y puesto en marcha los siguientes parámetros que deben observarse respecto del tratamiento de datos personales, los cuales deben ser observados por todos los empleados y contratistas del Colegio sin importar su rango o la labor que desempeñen al interior de la misma.

El incumplimiento de cualquiera de las reglas aquí planteadas puede dar lugar a la terminación del vínculo laboral/contractual o de cualquier otra índole con el Colegio con justa causa, razón por la cual invitamos a los empleados del Colegio a leer detenidamente la siguiente información:

12.1. Los datos personales y bases de datos constituidas por los mismos sean de clientes, empleados, proveedores, contratistas, entre otros, son propiedad exclusiva del Colegio.

12.2. El personal sólo está autorizado al acceso y uso de los mismos en la medida en que sea necesario para el cumplimiento de la labor para la cual fue contratado.

12.3. El personal tiene expresamente prohibido utilizar los canales de contacto del titular de la información en virtud o relación con el desempeño de sus funciones en el Colegio para la creación de bases personales con fines o propósitos propios o de terceros diferentes a los del Colegio, fuera del ámbito relacionado con sus funciones como parte del personal del Colegio.

12.4. La Información de clientes (dirección electrónica, física, teléfono, nombre, intereses que hagan identificable al cliente) o cualquier otra información que haga identificable a esa persona natural es propiedad del Colegio, por lo cual el empleado sólo está autorizado para usarla bajo las instrucciones que previamente le imparta el Colegio.

12.5. El personal no está autorizado para usar datos personales de clientes para el ofrecimiento de servicios o productos que sean ajenos al giro ordinario de las actividades del Colegio o a los asuntos inherentes a la misma. Por ejemplo: Una vez recolectados las fotografías de los estudiantes provenientes de actividades académicas o extracurriculares, los empleados deberán enviarlas al área interna encargada de su recopilación para posteriormente proceder con la eliminación de dichos datos personales de sus dispositivos.

12.6. Los datos personales y bases de datos del Colegio deben ser protegidos por el personal del Colegio bajo medidas de seguridad y confidencialidad adecuadas, por lo cual deben abstenerse de compartirlos con terceros ajenos a las labores del Colegio o ajenos a gestiones para los cuales el titular haya autorizado su tratamiento.

Si usted como parte del personal del Colegio tiene preguntas o no está seguro de cual tratamiento debe darle a ciertos datos personales o bases de datos que puedan contener información personal, por favor enviar su consulta al OPDP quien deberá dar instrucciones al respecto.

13. SEGURIDAD DE LA INFORMACIÓN

En el Colegio debemos mantener los datos personales seguros y protegerlos de cualquier acceso no autorizado, pérdida, daño o destrucción accidental, por ello, el Colegio cuenta con políticas y procedimientos de seguridad, los cuales están diseñados para proteger nuestros sistemas de TIC, nuestras instalaciones y los datos en su interior (tanto la información confidencial como los datos personales). En ese sentido, es deber del personal conocer y aplicar las políticas y procedimientos desarrollados por respecto de la seguridad de la información, así como realizar las capacitaciones en la materia y seguir las instrucciones para el uso de sistemas y equipos del Colegio.

14. PROCEDIMIENTO PARA INFORMAR A LA AUTORIDAD VIOLACIONES EN LOS CÓDIGOS DE SEGURIDAD

Las potenciales violaciones a los códigos de seguridad de las organizaciones generan un riesgo para los titulares de la información y son causantes en muchos casos de impactos significativos a la reputación corporativa y, en el peor de los casos, pueden afectar directamente a los titulares de información personal.

En principio, deben reportarse todos los incidentes de seguridad que comprometan datos personales, independiente de su impacto. Por esta razón, el Colegio cuenta con un procedimiento para manejar los incidentes o vulneraciones a los sistemas de información descrito a continuación:

14.1. Acciones por tomar en el evento de incidentes de seguridad:

Acción		Descripción
1.	**Identificación del incidente**	En caso de que cualquier miembro del Colegio considere que se presentó un manejo irregular de datos personales contenidos en bases de datos administradas por el Colegio debe considerar si se ha materializado un incidente que afecte los datos personales almacenados o custodiados por el Colegio En caso afirmativo frente a la ocurrencia de un incidente, o en caso de surgir duda sobre la ocurrencia del mismo, quien se

Acción		Descripción
		percate del incidente debe informarlo al OPDP y se deben realizar los pasos siguientes. **Nota**: conforme al Título V de la Circular Única de la SIC, un incidente de seguridad "se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado".
2.	**Generación del Informe del Incidente Ocurrido**	Se deberá generar un informe detallado del incidente ocurrido de acuerdo con la información registrada en el formato de incidentes de datos personales. La información que debe, como mínimo, incluir: **i.** Descripción de la identificación del incidente de seguridad. **ii.** Tipo de incidente. **iii.** Fecha de ocurrencia incidente. **iv.** Fecha en la que se obtuvo conocimiento del mismo. **v.** Causa probable de la materialización del incidente. **vi.** Tipo y cantidad de Datos Personales comprometidos en los cuales se debe identificar si se trata de datos generales, de identificación, ubicación, sensibles, contenido socioeconómico, u otros.
3.	**Informe para la Alta Dirección**	Se deberá generar un informe tipo ejecutivo para ser presentado a la alta dirección del Colegio respecto del incidente de seguridad para adoptar las medidas desde la dirección del Colegio que resulten aplicables.
4.	**Informe de incidente a la SIC**	Conforme a las obligaciones establecidas en el Título V de la Circular Única de la SIC, se debe reportar a la Superintendencia de Industria Comercio la ocurrencia de incidentes presentados dentro de los (15) días hábiles siguientes al momento en que se detecten.

14.2. Plantilla para realizar reportes de incidentes de seguridad:

Sin perjuicio de que el OPDP determine un formato específico para cada caso, se recomienda el uso del formato general presentado para generar el reporte interno de evento o incidente de seguridad ocurrido, el cual también podrá servir como soporte de gestión por parte de las áreas al interior de la organización. En caso de utilizar un formato diferente, debe incluirse, como mínimo la información incluida en el punto 2 de las acciones por tomar en el evento de incidentes de seguridad:

EVENTO O INCIDENTE DE DATOS PERSONALES			
No. De Caso			
1. FECHA Y HORA			
2. DETALLE DE LA PERSONA QUE REPORTA:			
2.1 Nombre completo			
2.2. Correo electrónico			
2.3. Ciudad			
3. DESCRIPCIÓN DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN			
¿Qué ocurrió?			
¿Cómo ocurrió?			
¿Por qué Ocurrió?			
Consideraciones iniciales sobre componentes afectados (Activos de información)			
Impactos adversos al negocio			
Vulnerabilidad identificada			
4. DETALLE DEL EVENTO O INCIDENTE DE SEGURIDAD DE LA INFORMACION:			
4.1 Fecha y hora en la que ocurrió el evento			
4.2 Fecha y hora en la que se descubrió el evento			
4.3 ¿El evento ya ha finalizado?		SI	NO
4.4 En caso afirmativo, especifique cuánto duró el evento (días/horas/minutos):			

Es necesario destacar que el incumplimiento de la norma aplicable o del contenido de este Manual puede conllevar investigaciones administrativas en contra del Colegio y de sus colaboradores.

En consecuencia, un esfuerzo conjunto en la detección de conductas contrarias y en la socialización de dichos comportamientos adquiere real importancia al interior del Colegio.

Lo invitamos a informar a la Rectoría del Colegio, a su superior, o al OPDP cualquier evento que pueda ser contrario a lo aquí dispuesto o que le genere preguntas; todo con la intención de que el Colegio pueda mejorar y cumplir, como organización, con la legislación aplicable a la protección de Datos Personales.

15. PROCEDIMIENTO DE ACTUALIZACIÓN DE LA INFORMACIÓN INGRESADA AL REGISTRO NACIONAL DE BASES DE DATOS

El presente capítulo tiene por objetivo servir como instructivo para la actualización de la información ingresada en el sistema del Registro Nacional de Bases de Datos (o "RNBD")

De acuerdo al Decreto 090 del 18 de enero de 2018 la actualización de la información consignada procede en los siguientes eventos: **i)** Anualmente entre el 2 de enero y el 31 de marzo de cada año; y **ii)** cuando se realicen cambios sustanciales en la información registrada, dentro de los primeros 10 días hábiles de cada mes.

Se consideran cambios sustanciales respecto de la información consignada en el RNBD la relacionada con: **i)** La finalidad de la base de datos; **ii)** Los Encargados del Tratamiento; **iii)** Los canales de atención al titular; **iv)** La clasificación o tipos de datos personales almacenados en cada base de datos; **v)** Las medidas de seguridad de la información implementadas; **vi)** La Política de Tratamiento de Datos Personales; y **vii)** La transferencia y transmisión internacional de datos personales.

Igualmente, debe actualizarse la información de los reclamos presentados por los titulares. Este reporte debe incluir: **i)** La información incluida en la solicitud presentada por los titulares; y **ii)** Los tipos de reclamos prestablecidos en el RNBD.

Este reporte es el resultado de consolidar los reclamos presentados por los titulares ante los responsables del tratamiento. El reporte se debe presentar en los primeros 15 días hábiles de febrero y agosto de cada año calendario.

15.1. Procedimiento para la actualización de la información ingresada al RNBD

15.1.1. Ingresar con el usuario y contraseña del RNBD

15.1.2. Para modificar la información de bases de datos específicas: Debe ingresarse a la pestaña "*Inscribir base de datos*", ubicar la base de datos inscrita por su nombre y seleccionar la opción "*Modificar registro*" se desplegará una ventana con la información general de la base de datos en la que podrán modificarse algunos de los datos de la base de datos, tales como el nombre de la base de datos o las finalidades de la misma o el número de titulares.

Una vez se indique “Guardar” se podrán modificar otros datos de la misma base datos, tales como los encargados, los canales de comunicación y atención a titulares y la Política de Tratamiento de Datos Personales.

Una vez se realicen las modificaciones aplicables, se deben guardar los cambios.

15.1.3. Para realizar el reporte de reclamos presentados por los titulares: Para reportar los reclamos que el Colegio como responsable de datos pudo haber recibido, aun cuando este número sea 0, debe proceder de la siguiente forma:

a. Seleccionar la pestaña “RNBD”;
b. Seleccionar “Inscribir bases de datos”;
c. Seleccionar el enlace “que indica Reporte de Novedades”;
d. Seleccionar el enlace “Reclamos presentados por los titulares”;
e. Seleccionar el enlace “Adicionar Información de Reclamos”; y
f. Diligenciar la información respectiva según sea el caso de las reclamaciones que apliquen, o si no hubo, así indicarlo.

Para efectos de ingresar la información de manera masiva, de ser necesario, se puede utilizar a través de formato mencionado en el numeral 6.1. del Manual del RNBD, el cual puede ser ubicado en el enlace a continuación: https://rnbd.sic.gov.co/sisiAyuda/. A continuación, se transcribe el aparte pertinente, donde se indica el formato a seguir:

“[Es] posible cargar la información de los reclamos de manera masiva mediante un archivo plano tipo txt, por la opción ***Cargar Información de Reclamos.*** *En el numeral 5.5.3.1 se muestra un ejemplo para generar un archivo plano tipo txt.*

El archivo por cargar debe tener separado cada campo por el carácter punto y coma (;) y es necesario tener en cuenta la siguiente estructura:

Nota: Todos los campos son obligatorios, es decir, si alguno aparece en blanco el archivo no se cargará”.

La lista de "TIPO Y DETALLE DE RECLAMO LEY 1581 DE 2012" para construir este archivo se encuentran en el Manual del Registro Nacional de Bases de Datos.

Ante cualquier inquietud relacionada con el contenido de este Manual, por favor contactar a la Secretaría Académica - Oficial de Protección de Datos del Colegio.

16. PROCEDIMIENTO PARA ATENDER REQUERIMIENTOS Y VISITAS DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Cuando el Colegio sean notificado formalmente de cualquier tipo de procedimiento adelantado por la SIC en su contra, con ocasión al tratamiento de un dato personal sobre el cual actúa como responsable, el representante legal del Colegio (o a quien este delegue expresamente como su representante para efectos de los asuntos en que el Colegio actúe como responsable del tratamiento de datos personales) comunicará de tal situación de inmediato al OPDPD al correo protección_datos@nogales.edu.co, para que este último, de trámite a la misma.

El Colegio, junto a los encargados de los tratamientos, deben atender de forma oportuna y colaborativa todos los requerimientos y visitas de la SIC. Para ello, el OPDP coordinará la atención de dichos requerimientos y visitas, para lo cual, según el procedimiento se pondrá en contacto con las áreas o sujetos involucrados (internos y/o externos a el Colegio), y facilitará la labor brindando el soporte que se requiera sobre protección de los datos personales.

En el evento en que funcionarios de la SIC visiten las instalaciones del Colegio, los miembros del personal deberán:

- Informar de inmediato de dicha circunstancia al OPDP.
- En el evento en que dicho órgano no se encuentre disponible, se deberá enviar un correo electrónico dirigido a todos los responsables informándoles de la situación y en especial al correo protección_datos@nogales.edu.co
- Solicitar a los funcionarios de la autoridad una debida acreditación de su pertenencia a la entidad.
- Cooperar con los funcionarios cuando se realice la práctica de testimonios, y entregar, sin dilación alguna, y si es requerido, cualquier equipo, dispositivo o documento solicitado por los funcionarios.
- Verificar la existencia de un acta de la visita con el objetivo de dejar constancia de todos los hechos que transcurrieron, la información que fue entregada, entre otros.

¡Gracias!

*** * ***

Corporación Educativa Los Nogales