POLÍTICA DE PROTECCIÓN DE DATOS

1. APROBACIÓN OFICIAL DE LA POLÍTICA DE PROTECCIÓN DE DATOS

La DIRECCIÓN de PROMOTORA IDEALES S.A.S. (en adelante EL COLEGIO) aprueba, con fecha 07 de septiembre de 2020, la presente Política de Protección de Datos y lo asume como propio de EL COLEGIO.

La DIRECCIÓN de EL COLEGIO ha adoptado las medidas necesarias para que todos los profesionales de su organización estén familiarizados con la **Ley 1581 de 2012 y normativa complementaria**, las cuales establecen las obligaciones y procedimientos tendientes a garantizar y proteger los derechos de los titulares de datos personales.

Todos los profesionales de EL COLEGIO con acceso a datos personales deberán cumplir las prescripciones contenidas la presente Política de Protección de Datos, así como las medidas de seguridad en ella contempladas.

Así mismo la DIRECCIÓN de EL COLEGIO ha establecido las funciones y responsabilidades necesarias para cumplir y hacer cumplir en todo momento las normas previamente citadas, haciendo especial énfasis en los procedimientos y medidas de seguridad a adoptar por aquellos profesionales que tienen acceso a datos de carácter personal.

Esta política se mantendrá actualizada y será revisada siempre que se produzcan cambios relevantes en la información u organización de la misma. El contenido se adecuará en todo momento a las disposiciones legislativas y reglamentarias vigentes en materia de seguridad de los datos de carácter personal, protegiendo a EL COLEGIO adecuadamente la información conforme a la legislación mencionada.

En Montería, a 07 de septiembre de 2020.

LA DIRECCIÓN

2. INTRODUCCIÓN

Las Tecnologías de la Información fomentan la utilización de la informática tanto en las grandes como en las pequeñas y medianas empresas, facilitando y agilizando el tratamiento de datos.

Si bien lo anterior supone grandes avances desde el punto de vista de la gestión y eficiencia desde el punto de vista del negocio, también aumenta el riesgo de vulneración de los derechos fundamentales de las personas titulares de datos personales.

La confidencialidad de los datos personales y el derecho a la intimidad de las personas físicas pueden verse amenazados dados los avances tecnológicos que permiten la transmisión y fuga de datos personales con un mínimo esfuerzo, si no se realiza un adecuado uso de las tecnologías de la información y se incorporan los controles necesarios.

Ante esta nueva realidad tecnológica, el legislador promulga una serie de normas que tienen por objeto garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, en lo que concierne al tratamiento de los datos personales.

La Constitución Colombiana, en su artículo 15, establece que:

> *"Todas las personas […] tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. […]".*

En desarrollo de este precepto constitucional se ha elaborado una normativa específica sobre Protección de Datos de Carácter Personal, tanto a nivel de ley como de decretos, siendo las normas más relevantes en Colombia:

- **Ley Estatutaria 1266 de 2008**, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley Estatutaria 1581 de 2012**, Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto Único 1074 de 2015**, Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, en los Capítulos 25, 26, 27 y 28.

A partir de dicha normativa se han establecido distintas medidas las cuales se pueden agrupar de la siguiente manera:

- Jurídicas
- Organizativas
- Técnicas

Las medidas **jurídicas, técnicas y organizativas** se recogen en el articulado de las normas en cuestión, las cuales son de aplicación directa a todos los tratamientos de datos personales realizados en Colombia.

La Protección de los Datos de Carácter Personal es una obligación impuesta a toda entidad que realice tratamientos a datos personales. Cualquier empresa que disponga de nombres y apellidos en un fichero de su ordenador o en soporte papel debe de adaptarse a estas normas, debiendo implantar una correcta Política de Protección de Datos dentro de la organización.

3. OBJETIVO DE LA POLÍTICA DE PROTECCIÓN DE DATOS

La presente Política de Protección de Datos responde a la obligación establecida en artículo 2.2.2.25.3.1 del Decreto Único Reglamentario 1074 de 2015, Capítulo 25, Sección 3, la cual tiene como objetivo desarrollar las políticas internas de EL COLEGIO correspondientes al tratamiento de los datos personales, así como describir las medidas de seguridad de índole organizativa y técnica que garantizan la confidencialidad, integridad y disponibilidad de la información contenida en los ficheros con datos de carácter personal.

La finalidad de la Política de Protección de Datos es **dar transparencia al sistema de tratamiento de los datos personales**, plasmando en el mismo medidas frente a los siguientes aspectos:

- Personas autorizadas para acceder a los datos.
- Herramientas utilizadas y sistemas que procesan y tratan los datos.
- Soportes que contienen y almacenan los datos.
- Cualquier otro aspecto relativo al tratamiento de los datos.

Es responsabilidad de EL COLEGIO adoptar las medidas de índole técnico y organizativo que garanticen el nivel de seguridad adecuado para el tratamiento de los datos de carácter personal, evitando su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta la naturaleza de los mismos y los riesgos a los que están expuestos.

Además, la normatividad vigente impone el **deber de confidencialidad** tanto al Responsable del Tratamiento, al Encargado y al Oficial de Protección de Datos, como a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, aún después de finalizar sus obligaciones con el Responsable del Tratamiento.

Por otro lado, en la presente Política de Protección de Datos se determinan los procedimientos y normas de seguridad adoptados con la finalidad de preservar la integridad, confidencialidad y disponibilidad de los datos personales, así como el procedimiento de su publicación para que sea conocido por todos los profesionales que intervienen en su tratamiento.

Por todo ello, se elabora esta Política de Protección de Datos, en la que, en virtud de los principios antes señalados, así como el principio de responsabilidad proactiva o “Accountability”, como eje vertebral de la normativa en Protección de Datos, se desarrolla lo atinente a las Medidas de Seguridad de **Nivel básico, medio y alto**, siendo considerados así de acuerdo a los siguientes criterios:

- **Nivel Básico:** Aplicable a todas las bases de datos y tratamientos realizados.
- **Nivel Medio:** Aplicable a datos financieros, relacionados con la seguridad social (salvo los de salud), así como aquellos que permitan definir características, la

personalidad o comportamientos de la persona y realizar, consecuencialmente, un análisis de perfiles.

- **Nivel Alto:** Aplicable a todos los datos sensibles, así como aquellos referidos a fines policiales o de infracciones o sanciones administrativas o judiciales.

Además, se nombra a un Responsable de Tratamiento de EL COLEGIO, como encargado de coordinar y controlar las medidas definidas en este documento y de verificar el cumplimiento de los controles periódicos a realizar para cada fichero.

Cualquier modificación debidamente informada y documentada de las circunstancias organizativas, normativas o técnicas en relación con un inventario de tratamientos de datos de carácter personal, conllevará la revisión y actualización por parte del Responsable de Tratamiento de la presente política.

A continuación, se relacionan todos aquellos tratamientos no ocasionales con su correspondiente nivel de seguridad:

NOMBRE DEL FICHERO	NIVEL
ESTUDIANTES Y PADRES DE FAMILIA	**ALTO**
PROVEEDORES	**BÁSICO**
EMPLEADOS	**BÁSICO**
VIDEOVIGILANCIA	**BÁSICO**

Las medidas de seguridad que se adopten en esta política serán de aplicación tanto en el local de EL COLEGIO, como en cualquier otro lugar en el que EL COLEGIO autorice el tratamiento de los datos, tanto a trabajadores de la propia empresa como a terceras personas, mediante una relación contractual.

Es decir, los ficheros, automatizados o no, cuyo tratamiento o explotación sean realizados por una empresa o terceras personas externas, a través de un contrato de prestación de servicios y fuera de las instalaciones de EL COLEGIO, están sometidos a la misma Política de Protección de Datos que aquéllos cuyo tratamiento se realiza en las instalaciones de EL COLEGIO.

Es, por tanto, responsabilidad de estos terceros adecuar las medidas de seguridad necesarias en los equipos informáticos, aplicaciones e instalaciones en las que se encuentren los ficheros.

4. DEFINICIONES LEGALES

- **Datos de carácter personal**: Cualquier información concerniente a personas físicas identificadas o identificables.

- **Fichero o Bases de Datos**: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- **Inventario de Tratamiento**: Registro automatizado en donde se contemplan las distintas categorías de datos, los datos del oficial de protección de datos, el responsable y el encargado, la finalidad del tratamiento y demás información relevante para efectuar las actividades de tratamiento.

- **Tratamiento de datos**: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- **Tratamiento Automatizado**: Cualquier operación o procedimiento técnico que permita la recogida, grabación, conservación, elaboración, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, cotejo o interconexión, así como su bloqueo o cancelación.

- **Responsable del Tratamiento**: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

- **Afectado o interesado**: Persona física titular de los datos que sean objeto del tratamiento.

- **Usuario**: sujeto o proceso autorizado para acceder a datos o recursos.

- **Encargado del tratamiento**: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

- **Oficial de Protección de Datos:** Persona física, especialista en materia de Protección de Datos, quien informará y asesorará al responsable o al encargado del tratamiento y a los empleados que tengan acceso a datos, en virtud de la normativa aplicable. Además, tiene como funciones, informar y asesorar al responsable del tratamiento de las obligaciones contractuales por parte de encargado, formación del personal de EL COLEGIO, supervisar el cumplimiento del orden jurídico en cuestión, velar por la conservación de la documentación, evitar riesgos de violación a las medidas de seguridad, supervisar la respuesta a las autoridades de control y cooperar con dichas entidades, ejercer de punto de contacto entre la autoridad de control y EL COLEGIO, entre otras.

- **Consentimiento del interesado**: Toda manifestación de voluntad de forma expresa, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- **Comunicación de datos**: Toda revelación de datos realizada a una persona distinta del interesado.

- **Sistema de información**: Conjunto de ficheros automatizados, programas soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

- **Recurso**: Cualquier parte o componente de un sistema de información.

- **Accesos autorizados**: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

- **Identificación**: Procedimiento de reconocimiento de la identidad de un usuario.

- **Autenticación**: Procedimiento de comprobación de la identidad de un usuario.

- **Contraseña**: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

- **Control de acceso**: Mecanismo que en función de la identificación ya autenticada permite acceder a los datos y recursos.

- **Incidencia**: Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

- **Soporte**: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

- **Copia de respaldo**: Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

5. IDENTIFICACIÓN DE LOS RESPONSABLES Y RECURSOS PROTEGIDOS

5.1 IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

Responsable del Tratamiento	**Promotora Ideales S.A.S.**
NIT:	**890.480.145-7**
Dirección:	**Carrera 3 # 69 – 11. Montería, Córdoba**
Correo electrónico:	**gimelre@yahoo.com.mx**
Teléfono:	**7850962 - 3174273346**
Representante Legal:	**Susana del Carmen Burgos De la Espriella**

6. DESCRIPCIÓN DE LOS TRATAMIENTOS

6.1 INVENTARIO: ESTUDIANTES Y PADRES DE FAMILIA

Sistema	MIXTO
Nivel de Seguridad	ALTO
Procedencia	DEL PROPIO INTERESADO Y/O REPRESENTANTE
Procedimiento de Recogida	CONTRATOS Y DOCUMENTACIÓN LEGAL
Soporte de Obtención	PAPEL Y/O PROCESADOR DE TEXTO

6.1.1 DESCRIPCIÓN

Datos relativos a la gestión de la prestación del servicio de educación a los estudiantes de EL COLEGIO.

6.1.2 FINALIDAD

Los datos recabados tienen la finalidad de gestión de: I) La correcta prestación del servicio de educación a los estudiantes; II) Alimentar los procesos del sistema de gestión de calidad; III) Contratación del seguro estudiantil; IV) Rendir informe a los padres de familia y/o acudientes sobre la formación de los estudiantes; V) El cumplimiento de protocolos técnicos para la prestación de servicios de educación preescolar y básica primaria; VI) Enviar información sobre programas y actividades realizados por EL COLEGIO, así como, novedades, noticias y publicaciones propias; VII) El cumplimiento de la normatividad vigente y del manual de convivencia.

6.1.3 ESTRUCTURA

Los datos de carácter personal que hagan parte de este inventario de tratamiento serán tratados hasta la terminación del contrato de matrícula, con posterioridad a ello, serán eliminados. Los datos académicos no serán eliminados, toda vez que, deberán ser conservados para la expedición de certificados. Los datos personales recabados en este inventario son:

DATOS DE CARÁCTER IDENTIFICATIVO
DOCUMENTO DE IDENTIDAD
NOMBRE Y APELLIDOS

DIRECCIÓN
DATOS DE CARACTERÍSTICAS PERSONALES
FECHA DE NACIMIENTO
LUGAR DE NACIMIENTO
EDAD
SEXO
DATOS DE FAMILIARES O ACUDIENTES
DOCUMENTO DE IDENTIDAD
NOMBRE Y APELLIDOS
TELÉFONO FIJO Y CELULAR
FECHA DE NACIMIENTO
LUGAR DE NACIMIENTO
DIRECCIÓN
CORREO ELECTRÓNICO
LUGAR DE TRABAJO
PROFESIÓN Y/O OCUPACIÓN
NÚMERO DE HERMANOS INSCRITOS EN EL COLEGIO
DATOS ACADÉMICOS
HISTORIAL ACADÉMICO
DATOS SENSIBLES
DATOS DE SALUD

6.1.4 COMUNICACIÓN DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la comunicación esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

EL COLEGIO transfiere datos del inventario de ESTUDIANTES Y PADRES DE FAMILIA a las autoridades públicas competentes para conocerlos, a Positiva de Seguros S.A. y a quienes por mandato legal o judicial se encuentre obligado a compartirlos.

6.1.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de EL COLEGIO han de contemplarse los siguientes aspectos:

- El tratamiento debe tener siempre un carácter temporal.

- Ha de firmarse un contrato de encargado de tratamiento entre las partes, en el cual debe de contemplarse:
  - Responsabilidades, obligaciones y limitaciones.
  - Inventarios de tratamiento de datos de carácter personal que se tratan.
  - Medidas de seguridad que aplica el tercero en función de los datos que se tratan.
  - Cláusula de confidencialidad.

Es necesario que los datos que vayan a ser tratados por terceros ya sean empresas o personas físicas estén sujetos a una relación contractual que regule los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

6.2 INVENTARIO: PROVEEDORES

Sistema	MIXTO
Nivel de Seguridad	BÁSICO
Procedencia	DEL PROPIO INTERESADO O REPRESENTANTE
Procedimiento de Recogida	CONTRATOS Y DOCUMENTACIÓN APORTADA
Soporte de obtención	PAPEL Y/O PROCESADOR DE TEXTO

6.2.1 DESCRIPCIÓN

Datos relativos a la gestión de proveedores, contable, fiscal y administrativa.

6.2.2 FINALIDAD

Los datos recabados tienen la finalidad de: I) Gestionar las relaciones comerciales de EL COLEGIO con sus proveedores; II) Operatividad del sistema integrado de gestión de la empresa; III) Validar el cumplimiento de la normatividad, requisitos legales aplicables, competencias e idoneidad de los proveedores y su personal.

6.2.3 ESTRUCTURA

Los datos de carácter personal sujetos a tratamiento en este inventario serán tratados hasta diez (10) años contados desde la terminación del contrato de prestación de servicios con el proveedor, término en el cual prescribe la acción ordinaria, dando fin a cualquier obligación de orden legal o judicial que pueda tener EL COLEGIO. Los datos personales recabados en este inventario son:

DATOS DE CARÁCTER IDENTIFICATIVO
DOCUMENTO DE IDENTIDAD
NOMBRE Y APELLIDOS
DIRECCIÓN DE LA EMPRESA/TRABAJO
TELÉFONO (FIJO, CELULAR)
DATOS ACADÉMICOS Y PROFESIONALES
FORMACIÓN, TITULACIONES
EXPERIENCIA PROFESIONAL
REFERENCIAS
DATOS DE DETALLES DE EMPLEO
PROFESIÓN
PUESTO DE TRABAJO
DATOS FINANCIEROS
NÚMERO DE CUENTA BANCARIA

6.2.4 COMUNICACIÓN DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la comunicación esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

EL COLEGIO no transfiere datos de carácter personal del inventario de PROVEEDORES a terceros, salvo orden legal o judicial emitida por la autoridad competente.

6.2.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de EL COLEGIO han de contemplarse los siguientes aspectos:

- El tratamiento debe tener siempre un carácter temporal.

- Ha de firmarse un contrato de acceso a datos entre las partes, en el cual debe de contemplarse:
  - Responsabilidades, obligaciones y limitaciones.
  - Inventarios de tratamiento de datos de carácter personal que se tratan.
  - Medidas de seguridad que aplica el tercero en función de los datos que se tratan.
  - Cláusula de confidencialidad.

Es necesario que los datos que vayan a ser tratados por terceros ya sean empresas o personas físicas estén sujetos a una relación contractual que regule los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

6.3 INVENTARIO: EMPLEADOS

Sistema	MIXTO
Nivel de Seguridad	BÁSICO
Procedencia	DEL PROPIO INTERESADO
Procedimiento de Recogid	ENTREVISTAS, HOJAS DE VIDA Y CONTRATOS
Soporte de Obtención	PAPEL Y/O PROCESADOR DE TEXTO

6.3.1 DESCRIPCIÓN

Datos relativos a la gestión de todos los datos relacionados con los trabajadores de EL COLEGIO.

6.3.2 FINALIDAD

Los datos recabados por EL COLEGIO tienen como finalidad la gestión de nóminas, recursos humanos, prevención de riesgos laborales y seguridad social.

6.3.3 ESTRUCTURA

Los datos de carácter personal sujetos a tratamiento en este inventario no serán tratados por un tiempo mayor a la duración de la relación laboral más el término máximo legal de tres (3) años, contados desde la terminación de la misma, tiempo en el cual

prescribe las acciones laborales que pudiesen emprenderse y prosperar en contra de EL COLEGIO. Como salvedad a esta regla general, se encuentran los datos relacionados con la pensión de los trabajadores y certificaciones laborales, información que será custodiada hasta el momento en que el trabajador se pensione o cumpla 67 años, es decir, haya sobrepasado por dos (2) años la edad de retiro forzoso, tiempo en el cual se presumirá, de buena fe, que el trabajador ha obtenido su pensión, lo que ocurra primero. Los datos personales recabados en este inventario son:

DATOS DE CARÁCTER IDENTIFICATIVO
DOCUMENTO DE IDENTIDAD
NOMBRE Y APELLIDOS
DIRECCIÓN (POSTAL, ELECTRÓNICA)
TELÉFONO (FIJO, CELULAR)
IMAGEN
DATOS DE CARACTERÍSTICAS PERSONALES
FECHA DE NACIMIENTO
LUGAR DE NACIMIENTO
DATOS ACADÉMICOS Y PROFESIONALES
FORMACIÓN, TITULACIONES
EXPERIENCIA PROFESIONAL
REFERENCIAS
DATOS DE DETALLES DE EMPLEO
PROFESIÓN
PUESTO DE TRABAJO
DATOS FINANCIEROS
NÚMERO DE CUENTA BANCARIA

6.3.4 COMUNICACIÓN DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la comunicación esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

EL COLEGIO transfiere datos a organismos de la seguridad social, así como a las entidades públicas con competencia para conocer dichos datos, por mandato legal o judicial.

6.3.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de EL COLEGIO han de contemplarse los siguientes aspectos:

- El tratamiento tendrá vigor hasta que la prestación de servicios finalice.
- Ha de firmarse un contrato de acceso a datos entre las partes, en el cual debe de contemplarse:
  - Responsabilidades, obligaciones y limitaciones.
  - Inventarios de tratamiento de datos de carácter personal que se tratan.
  - Medidas de seguridad que aplica el tercero en función de los datos que se tratan.
  - Cláusula de confidencialidad.

Es necesario que los datos que vayan a ser tratados por terceros ya sean empresas o personas físicas estén sujetos a una relación contractual que regule los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

6.4 INVENTARIO: VIDEOVIGILANCIA

Sistema	AUTOMATIZADO
Nivel de Seguridad	BÁSICO
Procedencia	DEL PROPIO INTERESADO
Procedimiento de Recogida	GRABACIÓN DE CÁMARAS DE SEGURIDAD
Soporte de Obtención	CÁMARAS DE SEGURIDAD

6.4.1 DESCRIPCIÓN

Datos relativos a la videovigilancia de las instalaciones de EL COLEGIO.

6.4.2 FINALIDAD

Los datos recabados por EL COLEGIO tienen como finalidad la integridad y la seguridad de las instalaciones y las personas dentro de ellas.

6.4.3 ESTRUCTURA

Los datos de carácter personal sujetos a tratamiento en este inventario no serán tratados por un tiempo mayor a un (1) mes. Los datos personales recabados en este inventario son:

DATOS DE CARÁCTER IDENTIFICATIVO
IMAGEN/VOZ

6.4.4 COMUNICACIÓN DE DATOS

A menudo las empresas comunican datos de carácter personal de sus ficheros para el cumplimiento de fines directamente relacionados con la actividad empresarial con el previo consentimiento del interesado, salvo que, la comunicación esté autorizada por una ley o cuando ésta responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión con ficheros de terceros, siempre y cuando se limite a la finalidad que lo justifique.

EL COLEGIO podrá comunicar los datos a la fuerzas públicas y militares del estado por imperativo legal y a los jueces y tribunales cuando sea por un motivo justificado.

6.4.5 ENCARGADOS DE TRATAMIENTO

Es posible el tratamiento de datos por terceros como parte de los procedimientos administrativos y comerciales convencionales.

Siempre que un tercero tenga que tratar de datos de EL COLEGIO han de contemplarse los siguientes aspectos:

- El tratamiento tendrá vigor hasta que la prestación de servicios finalice.
- Ha de firmarse un contrato de acceso a datos entre las partes, en el cual debe de contemplarse:
  - Responsabilidades, obligaciones y limitaciones.
  - Inventarios de tratamiento de datos de carácter personal que se tratan.
  - Medidas de seguridad que aplica el tercero en función de los datos que se tratan.
  - Cláusula de confidencialidad.

Es necesario que los datos que vayan a ser tratados por terceros ya sean empresas o personas físicas estén sujetos a una relación contractual que regule

los distintos aspectos necesarios para garantizar la confidencialidad, integridad y disponibilidad de dichos datos.

7. MANUAL DE FUNCIONES Y OBLIGACIONES DEL PERSONAL

7.1 FUNCIONES DEL PERSONAL

Las distintas funciones que deben existir dentro de la organización de EL COLEGIO, con responsabilidades en el tratamiento de datos de carácter personal, son las siguientes:

7.1.1 RESPONSABLE DEL TRATAMIENTO

La dirección de EL COLEGIO será quien decida sobre la finalidad, contenido y uso de los datos contenidos en un fichero y será el encargado de implantar lo establecido en la presente política, adoptando las medidas necesarias para que los profesionales con acceso a los datos personales conozcan las normas que afecten al desarrollo de sus funciones.

En el caso de EL COLEGIO, aunque la responsabilidad legal ante la SIC es de la propia sociedad, la ejecución de las tareas y las obligaciones asignadas al Responsable del Tratamiento serán llevadas a cabo por la dirección de la misma.

7.1.2 USUARIOS

Se entenderá por usuarios, el personal que habitualmente utiliza el sistema informático de acceso a los ficheros en EL COLEGIO, muchos de los cuales pueden tener acceso al tratamiento de datos de carácter personal.

7.2 OBLIGACIONES DEL PERSONAL

7.2.1 OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

1. Implantar las medidas establecidas en la presente política de protección de datos, así como obligar a su cumplimiento.
2. Implantar las medidas de seguridad correspondientes a cada tratamiento de acuerdo con la Evaluación de Impacto, cuando fuere necesaria.
3. Adoptar las medidas necesarias para que el personal conozca las normas de seguridad, así como las consecuencias de su incumplimiento.
4. Designar a la persona competente para decidir el nivel de acceso al sistema de tratamiento de cada usuario.
5. En relación con el entorno del sistema operativo y de comunicaciones deberá aprobar o designar al Administrador del Sistema, quien será el encargado del mantenimiento informático.
6. En relación con el sistema informático o aplicaciones de acceso a los ficheros, a través del encargado del mantenimiento informático, se encargará de que exista una relación actualizada de personas que tengan acceso autorizado al sistema de

información y de establecer procedimientos de identificación y autenticación para dicho acceso (mediante contraseñas).

7. Autorizar, en caso de que sea necesario, el tratamiento de los datos personales en lugar distinto de donde están ubicados los ficheros.
8. El tratamiento de datos personales fuera de EL COLEGIO deberá ser autorizado por el Responsable del Tratamiento. (Debe habilitarse un listado en el que se especifique los equipos móviles, PDA's, portátiles, smartphones, etc., que salen de EL COLEGIO, y la persona a la que se le ha asignado cada uno de ellos).
9. Encargarse de la autorización, alteración y anulación de los accesos permitidos, estableciendo los mecanismos necesarios para evitar que un usuario pueda acceder a los datos o recursos con derechos distintos de los autorizados.
10. Deberá conservar una copia de respaldo (física y virtual) de los datos y de los procedimientos de recuperación de datos, en un lugar con acceso restringido al personal autorizado.

7.2.2 OBLIGACIONES DE LOS USUARIOS

1. Garantizar que la información no pueda ser visible por personas no autorizadas.
2. Las pantallas, impresoras y cualquier tipo de dispositivos conectados al puesto de trabajo, deberán estar ubicados en lugares que garanticen la confidencialidad.
3. Impedir la visualización de los datos a terceros, protegiendo a través de protectores de pantalla y/u otros mecanismos la visualización de datos personales por terceros.
4. El usuario deberá comprobar que no hay documentos que contengan datos protegidos en la bandeja de salida de la impresora. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
5. La conexión a redes o sistemas desde los que se realiza el acceso a datos de carácter personal estará sujeta a las medidas establecidas en la política de protección de datos.
6. En el caso de que se produjese cualquier incidencia relacionada con la entrada y salida de datos por red, deberá notificarse al Responsable del Tratamiento y cumplimentar el correspondiente registro de violaciones de seguridad.
7. Responsabilizarse de la confidencialidad de la contraseña de acceso al sistema y, en el supuesto de que dicha contraseña sea conocida, fortuita o fraudulentamente, por personal no autorizado, proceder al cambio de la misma, así como a notificárselo al Responsable del Tratamiento, que lo hará constar en el registro de violaciones de seguridad.

7.2.3 OBLIGACIONES GENERALES (PARA TODO EL PERSONAL)

Con carácter general todo el personal empleado de EL COLEGIO deberá cumplir con las siguientes obligaciones:

1. Cumplir con todo lo dispuesto por el Responsable del Tratamiento.
2. Actuar según las especificaciones, medidas y procedimientos conforme determina la política de protección de datos de EL COLEGIO.
3. Usar los datos de carácter personal única y exclusivamente para la finalidad para la que fueron recabados y que necesiten para el desarrollo de sus funciones.
4. Guardar secreto sobre los datos que manejen, con un rango de secreto profesional, incluso después de finalizar su relación con EL COLEGIO.
5. Cumplir con el deber de informar a los titulares de los datos según lo dispuesto por la ley y normas complementarias y, en especial de la existencia de un tratamiento de datos de carácter personal y de su finalidad, así como de la posibilidad de ejercer sus derechos.
6. Facilitar los destinatarios de la información, la identidad y dirección del Responsable del Tratamiento y, en su caso, su representante legal, cuando así lo soliciten.
7. En caso de que un afectado ejerza sus derechos (acceso, rectificación, supresión, etc.), tramitar el asunto conforme a lo dispuesto en la legislación vigente.
8. Recabar los datos de carácter personal que sean adecuados, pertinentes y no excesivos en relación a la finalidad para la que se recogen, no extralimitándose en las instrucciones de recogida de datos que imponga el Responsable del Tratamiento. En ningún caso podrán ser tratados con finalidades incompatibles a las que motivaron su recogida.
9. Mantener la exactitud de los datos actualizándolos verazmente a la situación real, rectificando los datos incompletos o inexactos, sustituyéndolos por los correctos, en todas las aplicaciones.
10. Cancelar los datos una vez que dejen de ser pertinentes y necesarios para la finalidad para la que fueron recabados.
11. Garantizar la seguridad de los datos tanto en lo referente a su custodia y tratamiento, como en lo referente a permitir el acceso por el usuario afectado. La obligación se entiende en evitar la pérdida, tratamiento o acceso no autorizado a los datos de carácter personal.
12. No utilizar los datos con fines fraudulentos, desleales o ilícitos.

7.2.4 OBLIGACIONES DEL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

1. Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

2. Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
3. Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
4. Impulsar una cultura de protección de datos dentro de la organización.
5. Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
6. Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
7. Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
8. Revisar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
9. Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.
10. Realizar un entrenamiento general en protección de datos personales para todos los empleados de la compañía.
11. Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.
12. Integrar las políticas de protección de datos dentro de las actividades las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.).
13. Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.
14. Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.
15. Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.
16. Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.
17. Realizar seguimiento al Programa Integral de Gestión de Datos Personales.
18. Elaboración de los contratos de encargado de tratamiento necesarios para regular su tratamiento de datos.

19. Redacción e implementación de cláusulas de información y de confidencialidad a utilizar por EL COLEGIO.

7.2.5 NORMAS DE USO DEL MATERIAL INFORMÁTICO Y ACCESO A INTERNET

Todos los usuarios dados de alta en el sistema deberán atender a las siguientes normas de utilización:

1. Los usuarios serán plenamente responsables del uso adecuado de los terminales, así como sus accesorios desde el momento de su asignación.
2. Todo el material informático deberá ser utilizado conforme a las instrucciones dadas por el Responsable del Tratamiento.
3. Todo el material asignado deberá ser utilizado sólo y exclusivamente para la realización de las tareas empresariales designadas, no pudiendo, por tanto, utilizarse para cuestiones personales.
4. Los usuarios sólo podrán acceder a los recursos que el Responsable del Tratamiento les haya comunicado, en ningún caso intentarán acceder a recursos sin los privilegios necesarios. El Responsable del Tratamiento, en todo momento podrá visualizar el intento de acceso a los mismos.
5. Queda totalmente prohibida la utilización de dispositivos USB o soportes informáticos, salvo autorización expresa del Responsable del Tratamiento.
6. Se mantendrá bajo estricta confidencialidad las claves de acceso a los recursos, quedando totalmente prohibido escribir las mismas, así como pegarlas en las pantallas de los terminales o comunicárselas a terceros. En caso de olvido de contraseñas deberán comunicárselo al Responsable del Tratamiento.
7. El acceso a Internet está sólo autorizado para cuestiones laborales, quedando totalmente prohibida la navegación por ocio, así como la descarga de información, ficheros o programas de internet.
8. La utilización de correo electrónico está autorizada únicamente para cuestiones laborales.
9. Facebook, WhatsApp, Twitter, así como cualquier otra red social o aplicación de mensajería instantánea está totalmente prohibida, salvo autorización expresa del Responsable del Tratamiento, y siempre por motivos justificados de trabajo, en el caso de tener autorización, no podrán descargarse, en ningún caso, ficheros por este medio.

8. NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE VIOLACIONES DE SEGURIDAD

Se considera una violación de seguridad cualquier evento o suceso que pueda suponer un peligro para la seguridad de inventarios, datos, ficheros, sistemas y centros de tratamiento en general o para la confidencialidad, integridad o disponibilidad de los mismos.

El Registro de Violaciones de Seguridad, si bien no se encuentra contemplado por la normativa, es una herramienta muy importante para la prevención de riesgos, así como para realizar un seguimiento de las mismas; y además ayuda a cumplir con la normativa de Protección de Datos, desde el punto de vista del principio de responsabilidad demostrada.

Los aspectos a tener en cuenta son los siguientes:

- Cualquier profesional, sea o no usuario de los sistemas, que tenga conocimiento de una incidencia deberá informar inmediatamente al Responsable del Tratamiento, mediante correo electrónico en primer lugar, y si no es posible mediante llamada telefónica o cualquier otro medio efectivo de comunicación.
- El conocimiento y la no notificación o registro de una violación de seguridad por parte de un profesional puede ser considerado como una falta contra la seguridad de los tratamientos.

8.1 CONCEPTO Y TIPOS DE VIOLACIONES DE SEGURIDAD

Algunos sucesos que se pueden catalogar como violaciones de seguridad son:

- Averías de servidores y otros componentes hardware.
- Extravío de componentes hardware que puedan almacenar datos.
- Indisponibilidad del software del sistema.
- Fallo o indisponibilidad de las líneas de comunicaciones.
- Acceso y uso no autorizado de servicios y sistemas.
- Necesidad de una restauración total del sistema.
- Mal funcionamiento de los procesos de restauración de ficheros y bases de datos.
- Extravío de soportes y copias de seguridad.
- Intrusiones en la red.
- Consecutivas situaciones de bloqueo de identificadores de usuario.
- Intentos reiterados de accesos a recursos no autorizados.
- Modificaciones no autorizadas de los datos.
- Intento de suplantación de usuarios específicos.

- Desprotección de recursos protegidos.
- Intentos reiterados de accesos al sistema por usuarios inexistentes.
- Distintos aspectos relacionados con la seguridad física (alarma de incendios, humedades, accesos no autorizados a zonas restringidas, etc.).

8.2 PROCEDIMIENTO

Cualquier suceso que un usuario considere relevante será notificado al Responsable del Tratamiento el cual tomará la decisión de considerarlo o no como una violación de seguridad, lo será en la medida en que pueda afectar a la integridad y calidad de los datos personales y, por tanto, deberá poner en marcha los procedimientos de actuación correspondientes:

1. Identificación de la posible incidencia por cualquier profesional de EL COLEGIO.
2. Comunicación inmediata al Responsable del Tratamiento por e-mail en primer lugar, si esto no es posible por teléfono o mediante cualquier medio de comunicación efectiva. No obstante, de detectarse una violación de seguridad que constituya un riesgo para los derechos y libertades de los interesados, la comunicación deberá ser, en primer lugar, telefónica, a la par con la comunicación mediante email.

Tras la comunicación de un empleado de una posible incidencia, el Responsable del Tratamiento deberá actuar conforme al siguiente procedimiento:

1. Valorar la gravedad de la violación detectada, de conformidad con los análisis correspondientes que el Responsable del Tratamiento debe realizar junto con el resto de los profesionales que considere necesario.
2. En el caso de que el Responsable del Tratamiento lo valore como una incidencia que pueda constituir un riesgo para los derechos y libertades de los interesados, debe comunicar a las autoridades competentes, en un término no mayor a las 72 horas de haber tenido constancia de la violación de seguridad, señalando lo siguiente:
   - La naturaleza de la violación de seguridad (tipo de incidente) de los datos personales, incluyendo, las categorías (tipos de datos) y el número aproximado de titulares afectados, categorías e inventarios o registros afectados.
   - Comunicar el nombre y los datos de contacto del Responsable del Tratamiento o, si hubiese, del Oficial de Protección de Datos; en su defecto, comunicar los datos de contacto de cualquier persona que pueda brindar más información.

- Describir las consecuencias de la violación de la seguridad de los datos personales de acuerdo a la Evaluación de Impacto.
- Describir las medidas adoptadas o propuestas realizadas por el Responsable del Tratamiento para remediar la violación detectada, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- La fecha en la que acaeció el incidente y la fecha en la cual se tuvo conocimiento del mismo.
- La causa del incidente con el mayor grado de detalle posible.

3. Si no fuese posible facilitar toda la información requerida por la autoridad competente de Protección de Datos, de manera simultánea, esta tiene que ser brindada de forma gradual y sin dilación.
4. Asimismo, cuando sea probable que la violación detectada sea de riesgo para los interesados, además de realizar la comunicación a la autoridad, el Responsable del Tratamiento tiene que comunicar al interesado lo sucedido inmediatamente; señalando como mínimo el nombre del Responsable del Tratamiento, las consecuencias de la violación detectada y las medidas adoptadas por el Responsable. Esto no será necesario, si es que las medidas tomadas por el Responsable han podido evitar los riesgos de la violación, o cuando, por la cantidad de interesados, una comunicación individual suponga un esfuerzo desproporcionado, por lo tanto, se hará de forma colectiva.
5. En el supuesto de que el Responsable del Tratamiento, considere que la violación de seguridad detectada no constituye un riesgo para los derechos y libertades de los interesados, este llevará a cabo un registro de violaciones de seguridad, con el propósito de reforzar los puntos débiles en las medidas de seguridad que permitieron la realización de la violación detectada.

9. MEDIDAS Y NORMAS DE SEGURIDAD DE QUE SE DISPONE

9.1 PROCEDIMIENTOS Y NORMAS TÉCNICAS DE ACCESO

La presente Política de Protección de Datos regula el uso y acceso a los sistemas y comunicaciones de forma que se impida el acceso no autorizado a los datos de los ficheros e inventarios de tratamiento.

Ninguna herramienta o programa de utilidad que permita el acceso a los ficheros e inventarios de tratamiento deberá ser accesible a ningún usuario o administrador no autorizado.

Si la aplicación o sistema de acceso al fichero o inventario de tratamiento utiliza normalmente ficheros temporales, o cualquier otro medio en el que pudiesen ser grabados copias de los datos protegidos, los administradores del sistema deben verificar que los datos no son accesibles posteriormente por personal no autorizado.

Si el ordenador y/o servidor en el que están ubicados los ficheros e inventarios está integrado en una red de comunicaciones, de forma que, desde otros ordenadores conectados a la misma sea posible el acceso a los datos, los administradores del sistema deberán asegurarse de que este acceso no se permite a personas no autorizadas.

9.2 CONTROL DE ACCESO LÓGICO

9.2.1 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

El Responsable del Tratamiento, es el responsable de la relación actualizada de usuarios con acceso a los datos, ficheros e inventarios protegidos, y de establecer los procedimientos de identificación y autenticación para dicho acceso mediante código de usuario y contraseña. Ambos son las llaves de acceso a los sistemas y constituyen un componente básico de la seguridad de los datos y deben de estar especialmente protegidos:

- La identificación de usuario (User ID) es personal e intransferible y es asignado una sola vez. La nomenclatura del usuario está definida con la primera letra del nombre seguida por el apellido.
- Las contraseñas son estrictamente confidenciales y secretas, y cualquier incidencia que comprometa su confidencialidad debe ser inmediatamente comunicada al Responsable del Tratamiento y subsanada en el menor tiempo posible.
- Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida, fortuita o fraudulentamente, por personas no autorizadas, debe registrarse como una incidencia y procederse por parte del Usuario a su cambio inmediato.
- Las contraseñas no son almacenadas, se asigna una única contraseña de acceso al sistema, y es el usuario el encargado de cambiarla en el primer acceso. En caso de ser necesario el administrador del sistema invalida dicha contraseña.

- El procedimiento de asignación, distribución, almacenamiento y gestión de las contraseñas debe seguirse en todos los casos.

9.2.2 GESTIÓN DE CONTRASEÑAS

Las contraseñas de acceso al sistema son un pilar fundamental de la Protección de Datos, pues otorgan y garantizan confidencialidad en la información.

- Longitud de la contraseña: Al menos 8 caracteres
- Complejidad de la contraseña: alfanumérica
- Vigencia de la contraseña: 3 meses
- Bloqueo de los sistemas tras intentos fallidos de acceso: 3 intentos

9.2.3 BLOQUEO DE USUARIOS Y CONTRASEÑAS

Tras un tercer intento fallido de acceso, el sistema bloqueará automáticamente el usuario.

El procedimiento para que el usuario afectado pueda ser rehabilitado es el siguiente:

El usuario afectado deberá dirigirse mediante llamada telefónica o bien personalmente, al Responsable del Tratamiento para que, una vez verificada la situación y comprobado que el usuario no está intentando acceder de manera fraudulenta, se lo comunique al administrador del Sistema para que reactive al usuario asignándole una nueva contraseña que obligará a cambiarla al primer acceso.

9.2.4 ASIGNACIÓN, DISTRIBUCIÓN Y ALMACENAMIENTO DE USUARIOS Y CONTRASEÑAS

PROCEDIMIENTO DE ALTA DE USUARIOS

- La Dirección comunica al Administrador del Sistema correspondiente el alta de un profesional en EL COLEGIO, indicando el puesto de trabajo y los privilegios necesarios para el desempeño de sus funciones.
- El Administrador del Sistema procederá a dar de alta en el mismo al nuevo usuario, procediendo el Responsable del Tratamiento a actualizar los registros necesarios incluyéndolo en la Política de Protección de Datos.
- El Responsable del Tratamiento comunica al nuevo profesional los siguientes aspectos:
    - Nombre de usuario.
    - Contraseña asignada.
    - Aplicaciones a las que tiene acceso.

- El sistema obliga al nuevo usuario a cambiar la contraseña la primera vez que accede.

PROCEDIMIENTO DE BAJA DE USUARIOS

- La Dirección, tan pronto como tenga noticia de la baja de un profesional en EL COLEGIO, lo comunicará de manera inmediata al Administrador del Sistema correspondiente.
- En el plazo de 3 días, el Administrador del Sistema correspondiente, procederá al bloqueo del usuario y contraseña del profesional que causó baja.

PROCEDIMIENTO DE MODIFICACIÓN DE USUARIOS

- La Dirección comunicará al Administrador del Sistema correspondiente la necesidad de un cambio en el perfil del profesional indicando el nuevo puesto asignado y los nuevos privilegios a asignar.
- El Administrador del Sistema correspondiente previa autorización del Responsable del Tratamiento, procederá a realizar las modificaciones pertinentes, debiendo tener especial atención a dar de baja al profesional en los recursos a los que ya no deba acceder.
- El Administrador del Sistema comunica al nuevo profesional los siguientes aspectos, en el caso de que sea necesario:
    - Nombre de usuario.
    - Contraseña asignada
    - Aplicaciones a las que tiene acceso.

9.2.5 DIRECTIVAS DE AUDITORÍA

- **Auditoría de inicio de sesión de cuenta**: Se puede auditar cuando un usuario inicia sesión y, si en ese inicio ha habido incidencias, tales como introducir mal las contraseñas o intento de inicio de sesión con otra cuenta, etc. Todos estos sucesos, se graban en el registro de seguridad del sistema.
- **Auditoría del seguimiento de procesos**: Controlar la actividad de un usuario en el sistema, verificando los pasos que sigue, los accesos, rutinas y pautas de comportamiento.

9.3 GESTIÓN DE SOPORTES

Los soportes informáticos son todos aquellos objetos físicos susceptibles de ser tratados en un sistema de información, medios de grabación y recuperación de datos

que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestiona los ficheros.

Los soportes mayormente utilizados son fácilmente transportables, por lo que es evidente la peligrosidad para la seguridad de los datos y, por lo tanto, la importancia de gestionar un control sobre estos medios.

Dado que la mayor parte de los soportes que actualmente se utilizan (discos duros externos, pendrives, etc.) son fácilmente transportables, reproducibles y/o copiables, es necesario adoptar las medidas de seguridad necesarias para evitar los riesgos contra la confidencialidad, integridad o disponibilidad de los datos.

9.3.1 PROCEDIMIENTO DE USO DE LOS SOPORTES

En relación con los soportes deben seguirse las siguientes normas:

- Identificación inequívoca mediante etiqueta externa que permita a EL COLEGIO conocer los siguientes aspectos:
  - Fecha de creación.
  - Información que contienen.
- Deben guardarse en un lugar protegido, con acceso restringido a personas no autorizadas. Dicho almacenamiento se realiza en cajones bajo llave, bajo el control del Responsable del Tratamiento.
- La salida de estos soportes, fuera de los locales donde están ubicados dichos ficheros protegidos, deberá ser expresamente autorizada por el Responsable del Tratamiento, y este lo hará constar en el registro de salida de soportes establecido al efecto.
- Cuando los soportes con información de carácter personal tengan que salir del lugar de ubicación del fichero para operaciones de mantenimiento o reparación, se establecerán unas medidas de seguridad tendientes a evitar la recuperación de información por terceros no autorizados, por lo que, en el caso de que sea posible se deberá extraer el disco duro del terminal o bien realizar una copia de la información contenida en el mismo y proceder a su formateo a bajo nivel. Cuando esto no sea posible se establecerá un contrato de encargado de tratamiento durante el período de dicho mantenimiento, haciéndolo responsable del uso malintencionado o indebido de los datos en él contenidos.
- Los soportes reutilizables deberán ser formateados o sobrescritos con anterioridad a su reutilización libres de información anterior y de forma que los datos que contenían, no se puedan recuperar.
- Cuando los soportes con información de datos de nivel alto salgan del centro de tratamiento deben estar protegidos mediante contraseña de forma que sea ilegibles para impedir cualquier tercero tenga acceso a la información almacenada en ellos.

- Para la destrucción de los soportes se seguirán las siguientes pautas:
    - Destrucción física de los mismos, para ello, se dará de baja previamente en el inventario y se darán al Responsable del Tratamiento correspondiente que procederá a su destrucción física.
    - En el caso de ficheros no automatizados en soporte papel es necesario el uso generalizado de destructoras de papel con las calidades adecuadas al tipo de documento que se pretenda eliminar o, su tercerización con una empresa destructora de documentos.

9.3.2 INVENTARIO DE SOPORTES

La relación de los soportes con datos de carácter personal, existentes en EL COLEGIO, se lleva a cabo por los Responsables de Tratamiento a través del registro establecido debidamente, así como la información que contienen.

9.3.3 CONTROL DE TERMINALES PORTÁTILES

Todos los terminales portátiles estarán controlados por el Responsable del Tratamiento, que será quien decida sobre la asignación o no de un terminal a un usuario de forma esporádica, así como la información que deberá estar contenida en el mismo.

El Responsable del Tratamiento en su caso, determinará la asignación de terminales portátiles permanentes a los usuarios designados.

Para controlar dichos terminales, el Responsable del Tratamiento de cada centro de trabajo, llevará un registro de asignaciones, incluyendo el usuario designado, la identificación del terminal, la información que contiene y la fecha de entrega y devolución.

Durante el tiempo que el usuario tenga designado el terminal será responsable del buen mantenimiento y manejo del mismo, respondiendo de los deterioros que pudiera llegar a sufrir por negligencia del mismo.

En el caso de pérdida o robo de un terminal mientras el usuario lo tenga asignado deberá comunicárselo inmediatamente a su Responsable del Tratamiento para que tome las debidas medidas necesarias.

9.3.4 DISTRIBUCIÓN DE SOPORTES

Se considera distribución de soportes, el traslado físico de soportes fuera del lugar de ubicación del fichero, independientemente del soporte que contenga la información, debiendo ser cifrados o bien utilizar cualquier otro mecanismo que evite su manipulación durante su traslado.

Cuando dichos traslados afecten a ficheros de Nivel Alto, dicha documentación se entregará en sobre cerrado con cierre “open-trac”, procediendo el usuario a la

estampación de dos sellos de EL COLEGIO en los bordes del cierre del sobre de forma que el destinatario de la información conozca si el contenido ha sido manipulado o no, cuando se trate de datos en soporte papel, y encriptados mediante contraseña cuando se trate de datos contenidos en soportes informáticos.

9.4 SEGURIDAD FÍSICA

El centro de trabajo donde se ubican los inventarios de tratamiento de datos de carácter personal y donde se encuentran los sistemas de información, corresponde a instalaciones propias y privadas de EL COLEGIO. El edificio dispone acceso a las instalaciones equipadas con sistemas de seguridad que limitan la entrada a las mismas, únicamente, al personal así autorizado para ello. De igual manera, cuentan con una sala de archivo con acceso controlado que queda cerrada mediante llave y extintores contra incendios como medidas de seguridad física.

La información en papel que es necesario mantener por obligaciones legales, se almacena durante el periodo legal establecido, en armarios cerrados con llave.

9.5 FICHEROS E INVENTARIOS DE TRATAMIENTO TEMPORALES

Los ficheros temporales, utilizados en general para obtener ficheros finales tras distintos tratamientos de los mismos, contienen datos personales que deben ser objeto de las mismas medidas de seguridad que los datos finales.

NORMAS DE USO DE LOS FICHERO TEMPORALES

- Los usuarios sólo podrán crear ficheros temporales previa autorización del Responsable del Tratamiento y siempre por motivos justificados de trabajo, siempre se almacenarán en las carpetas departamentales compartidas, salvo disposición contraria del responsable.
- El Responsable del Tratamiento realizará comprobaciones periódicas de los ficheros temporales creados por los usuarios, procediendo al borrado de todos aquellos ficheros que no estén previamente justificados o que hayan dejado de ser necesarios para la finalidad para el que se creó.
- Dichos ficheros temporales deberán ser dados de alta en un registro establecido al efecto por el Responsable del Tratamiento.

9.6 COPIAS DE SEGURIDAD Y RESTAURACIÓN

Las copias de seguridad del sistema informático y de los datos son realizadas por EL COLEGIO con una periodicidad semanal de todo el sistema y los datos mediante un procedimiento establecido debidamente por medio de disco duro externo y servidor NAS.

En caso de ser necesario recuperar datos, el Responsable del Tratamiento lo registrará como una incidencia, y será quien autorizará o no dicha recuperación. En caso de ser autorizada se lo comunicará a EL COLEGIO de mantenimiento contratada que realizará la recuperación de datos a través de acceso remoto.

9.7 TRANSMISIONES TELEMÁTICAS

Toda transmisión de datos por redes de telecomunicaciones se realizará cifrando dichos datos o estableciendo un mecanismo que evite su manipulación por terceros no autorizados mediante la transmisión y llegada a su destinatario, mediante contraseña, según el siguiente procedimiento.

9.7.1 PROTOCOLO DE ACTUACIÓN PARA EL CIFRADO DE FICHEROS

FORMA DE PROCEDER:

El usuario cuando envíe un archivo que deba ir cifrado, enviará a su destinatario la contraseña en un archivo diferente, a aquél que se quiere distribuir. Podrá efectuarse dicha comunicación por cualquier medio, bien, por teléfono, carta ordinaria o a través de correo electrónico, pero siempre la contraseña irá en un mensaje diferente al medio donde se inserte del fichero.

Toda otra comunicación por parte de **EL COLEGIO** por redes de telecomunicaciones a terceros que afecten a datos personales se realizará cifrando su contenido mediante contraseña.

Todos los ficheros, con independencia de su formato, deben enviarse convenientemente cifrados.

10. DERECHOS DE LOS INTERESADOS Y PROCEDIMIENTO PARA SU EJERCICIO.

En la normativa de Protección de Datos se podrá encontrar un catálogo de derechos de los interesados a ejercer ante el responsable del tratamiento, dentro de los cuales nos encontramos con el derecho de acceso, rectificación, cancelación y oposición, no obstante la mención, reconocemos expresamente todos los derechos de los titulares consagrados en el régimen de protección de datos personales.

10.1 DERECHO DE ACCESO.

El derecho de acceso consiste en que todos los interesados gozan del derecho a que los responsables del tratamiento le brinden confirmación sobre si se están tratando o no sus datos de carácter personal, así como con respecto a los datos personales que se están tratando y a conocer lo siguiente:

- La finalidad del tratamiento.
- Las categorías de los datos personales que están siendo tratados.
- Los destinatarios o las categorías de ellos a quienes se le comunicarán o se les ha comunicado dichos datos, con especial mención de si se trata de organizaciones internacionales o de destinatarios en terceros países.
- El plazo estipulado para la conservación de los datos o, en su defecto, los criterios necesarios para determinarlo.
- La existencia de los demás derechos que le asisten al interesado con respecto a sus datos de carácter personal.
- La posibilidad de presentar reclamación ante la autoridad de control competente.
- Cuando los datos personales no se hubiesen obtenido del propio interesado, toda la informacion disponible sobre el origen de los datos tratados.
- Si las hubiere, la existencia de decisiones automatizadas y la elaboración de perfiles y la consecuente información relativa a la lógica aplicada, la importancia y las consecuencias previstas para el interesado.

Adicional a lo antes planteado, cuando el responsable del tratamiento realice transferencias internacionales de datos el interesado, tendrá que notificar al interesado sobre las garantías adecuadas prestadas para la validez de la transferencia internacional. Igualmente, el responsable se encuentra obligado a facilitar, gratuitamente, una copia de los datos de carácter personal que se estén tratando.

Cuando la solicitud elevada por el interesado se hubiere realizado por medios electrónicos, como regla general, se está en la obligación de facilitar la información en formato electrónico de uso común, salvo que el interesado en su solicitud dispusiese que se le fuera entregada en alguna otra forma.

10.2 DERECHO DE RECTIFICACIÓN.

El derecho de rectificación se refiere a la facultad que tienen todos los interesados de que sin dilación indebida el responsable del tratamiento rectifique los datos personales inexactos que tenga del interesado, e incluso a que dichos datos sean completados por declaración adicional.

Cuando los datos sean rectificados, el responsable deberá notificar a los destinatarios a quienes les hubiese comunicado los datos, salvo ante la imposibilidad o esfuerzo desmedido de realizar tal aviso, así como al interesado, cuando lo solicitase, sobre la existencia de dichos destinatarios.

10.3 DERECHO DE CANCELACIÓN.

El derecho de cancelación de los interesados se erige como aquel del que disponen los interesados para solicitar la eliminación de sus datos de carácter personal, sin dilación indebida, al responsable del tratamiento. Cuando el titular ejerza su derecho de cancelación, EL COLEGIO estará obligada a suprimir los datos ante los siguientes supuestos:

- Cuando los datos personales del interesado no sean necesarios para el cumplimiento de la finalidad del tratamiento.
- Cuando el tratamiento se fundase en el consentimiento del interesado como base legitimadora del tratamiento y éste lo retire.
- Cuando el interesado se opone al tratamiento.
- Cuando los datos de carácter personal se hubiesen tratado ilícitamente.
- Cuando sea obligatoria su supresión debido a una obligación legal aplicable al responsable del tratamiento.
- Cuando los datos de carácter personal se deriven de una oferta de servicios de la sociedad de la información a menores.

Ante la eventualidad en la que el responsable del tratamiento haya hecho públicos datos de carácter personal del interesado y éste se encuentre obligado a suprimir los datos en cuestión, se encontrará obligado a tomar todas las medidas razonables (analizando las tecnologías disponibles y el costo de aplicación) correspondientes para informar a los demás responsables que traten

dichos datos que deben suprimir todos los enlaces, copias o réplicas de los datos en cuestión, es decir, se introduce el derecho al olvido.

No será procedente la obligación de supresión de la totalidad de los datos del responsable por ser el tratamiento necesario para:

- Ejercer el derecho a la libertad de expresión e información.
- El cumplimiento de una obligación legal, de una misión realizada en interés público o en ejercicio de poderes públicos.
- Motivos de interés público en materia de salud pública.
- Fines estadísticos, de investigación científica o histórica o de archivo en interés público.
- Formular, ejercer o defender reclamaciones.

Igualmente, cuando los datos sean suprimidos el responsable deberá notificar a los destinatarios a quienes les hubiese comunicado los datos, salvo ante la imposibilidad o esfuerzo desmedido de realizar tal aviso, así como al interesado, cuando lo solicitase, sobre la existencia de dichos destinatarios.

10.4 DERECHO DE OPOSICIÓN.

Por su parte, el derecho de oposición se conoce como aquel que tienen los interesados a oponerse al tratamiento de sus datos personales en cuanto se relacionan con motivos de su situación particular, el interesado podrá oponerse únicamente cuando la base legitimadora del tratamiento de dichos datos sea el interés legítimo o el interés público, incluida la elaboración de perfiles adelantada con la misma base. Cuando un interesado ejerza su derecho de oposición, no será necesario que él sea quien pruebe motivos suficientes para oponerse al tratamiento, por el contrario, será el responsable del tratamiento quien se encuentra llamado a demostrar que existen motivos legítimos para que el tratamiento prevalezca sobre los intereses, derechos y libertades del interesado o que son necesarios para formular, ejercer o defender reclamaciones.

Ulteriormente, se establecen dos previsiones para tener en cuenta:

- Cuando el interesado se oponga a cualquier tratamiento que tenga como fines el marketing directo deberá cesarse todo tratamiento con dicha finalidad sobre los datos personales del interesado.
- El interesado podrá oponerse al tratamiento de sus datos con fines estadísticos o de investigación científica o histórica, excepto cuando se haga en el cumplimiento de una misión realizada por motivos de interés público.

10.5 PROCEDIMIENTO ANTE EL EJERCICIO DE DERECHOS DEL INTERESADO.

Para dar cumplimiento a la normativa colombiana, las directrices a cumplir serán las siguientes:

1. El Titular de la información contenida en las bases de datos de EL COLEGIO podrá ejercer su derecho de conocer, actualizar, rectificar, suprimir y revocar la información contenida en las mismas, mediante cualquier medio que se encuentre conforme al orden jurídico actual.

2. La solicitud debe ser clara en lo que se pretende, ya sea conocer, actualizar, rectificar, suprimir y/o revocar la información que se encuentra contenida en una base de datos. Además, deberá contener los datos de contacto del peticionario para poder darle una respuesta.

3. Independientemente del mecanismo utilizado para la radicación de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

4. Los reclamos para corrección, actualización o supresión de datos serán contestados dentro de los quince (15) días hábiles siguientes, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo 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.

5. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. De igual forma, si transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

6. La primera instancia de la reclamación será EL COLEGIO, y una vez agotada ésta, sin respuesta satisfactoria, podrá el titular recurrir a la Superintendencia de Industria y Comercio.

También será importante tener en cuenta las siguientes recomendaciones:

- El responsable del tratamiento deberá tomar todas las medidas adecuadas para responder a las solicitudes realizadas por los interesados de manera concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo, especialmente cuando la información estuviese encaminada a la respuesta brindada a un menor.
- La información podrá ser brindada por cualquier medio, incluso, por medios electrónicos, sin embargo, cuando el interesado solicite que la información sea facilitada de manera verbal, será procedente, exclusivamente, una vez se haya comprobado la identidad del interesado por otros medios.
- Cuando la solicitud sea presentada por medios electrónicos, el responsable del tratamiento deberá responderla por el mismo medio siempre que sea posible, salvo que el interesado manifieste que desea recibir la comunicación por otro medio.

11. CONTROLES DE VERIFICACIÓN DE CUMPLIMIENTO

La veracidad de los datos contenidos en la Política de Protección de Datos y sus Anexos, así como el cumplimiento de las normas que contiene, deben ser comprobados, de forma que puedan detectarse y subsanarse las posibles anomalías.

Es muy importante que se realicen tanto revisiones puntuales, como periódicas, de forma que se verifique que los procedimientos, controles y medidas implantados están operativos y que el entorno se adapta tanto a la realidad del tratamiento de los datos como a las normas e instrucciones legales vigentes.

El Responsable del Tratamiento trimestralmente verificará, al menos, los siguientes aspectos:

- Que los usuarios autorizados se corresponden con la lista de los usuarios realmente autorizados.
- El cumplimiento de lo previsto en relación con las entradas y salidas de datos, sean por red, en soporte magnético o analógico (papel).
- La existencia de las copias de respaldo que permitan la recuperación de los ficheros.
- Analizará las incidencias registradas para, independientemente de las medidas concretas adoptadas en su momento, adoptar las acciones necesarias que las limiten en el futuro.
- Revisará los cambios que se haya realizado en el entorno (hardware, software, aplicaciones, etc.) procediendo a la actualización de la Política de Protección de Datos y de los registros correspondientes.
- Otros aspectos que el Responsable del Tratamiento pueda considerar.

El Responsable del Tratamiento mensualmente, verificará la información de control registrada en registro de violaciones de seguridad y elaborará un Informe de Revisión el cual recogerá los incidentes detectados proponiendo, en su caso, las medidas a adoptar.

11.1 POLÍTICA DE PROTECCIÓN DE DATOS

Cualquier variación que afecte a los aspectos contemplados en las disposiciones vigentes deberá recogerse de inmediato en la Política de Protección de Datos, debiendo por tanto ser actualizada constantemente.

Tras las revisiones realizadas debe emitirse un Informe de Revisión, el cual será compartido por el Responsable del Tratamiento a los Encargados y al Oficial de Protección de Datos, si lo hubiera.

En caso de no producirse ningún cambio significativo en el entorno al menos ser efectuará una revisión anual del contenido de la Política de Protección de Datos y sus Anexos.

Las revisiones periódicas darán lugar a la actualización de la Política de Protección de Datos y su correspondiente alta en el registro establecido al efecto.

11.2 REVISIÓN MENSUAL LOG DE ACCESO A FICHEROS DE NIVEL ALTO

El Responsable del Tratamiento deberá revisar, al menos, una vez al mes los logs de acceso a las aplicaciones que tratan datos de nivel alto, y elaborar un Informe en el que se relacionen las incidencias detectadas.