COLEGIO DE BOYACÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

CO-PL-03

V.01 / 30-01-2026

COLEGIO DE BOYACÁ

"Iniciador de la Educación Pública en Colombia"

Dr. LUIS SANTIAGO GARCÍA CIFUENTES
Director General

Dra. Diana Carolina Moreno Suesca
Subdirectora Administrativa y Financiera

Merisol Rincón Granados
Subdirectora Académica

Tunja, enero 31 de 2026

19

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento describe el Plan de Seguridad y Privacidad de la Información del Establecimiento Público Colegio de Boyacá, el cual se encuentra alineado con los objetivos, metas y procedimientos institucionales, y en concordancia con el Modelo Integrado de Planeación y Gestión – MIPG, atendiendo a lo establecido en la norma NTC-ISO/IEC 27001, que proporciona lineamientos sobre cómo gestionar la seguridad y privacidad de la información en las organizaciones. El propósito de este plan es que el Establecimiento cuente con una visión integral de los riesgos que puedan afectar la seguridad y privacidad de los activos de información, y que establezca controles y medidas efectivas, viables y transversales para salvaguardar la confidencialidad, integridad y disponibilidad de los datos generados en el desarrollo de los procesos académicos, administrativos y financieros.

De acuerdo con lo señalado en el Decreto 612 de 2018, “por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, y en cumplimiento del artículo 2.2.22.3.14 sobre la integración de planes institucionales y estratégicos, se actualiza el presente Plan de Seguridad y Privacidad de la Información del Establecimiento Público Colegio de Boyacá, garantizando su articulación con los instrumentos de planeación y gestión institucional.

1. JUSTIFICACIÓN

El Establecimiento Público Colegio de Boyacá administra información académica, administrativa y financiera que constituye un activo estratégico para el cumplimiento de sus funciones. La creciente exposición a riesgos tecnológicos, amenazas internas y externas, así como incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos, hacen indispensable contar con un plan que oriente la gestión de la seguridad y privacidad de la información.

Este plan se justifica en la necesidad de garantizar la protección de los datos de estudiantes, docentes, personal administrativo y partes interesadas, asegurando la continuidad institucional, el cumplimiento de la normatividad vigente en materia de seguridad digital y la generación de confianza en la comunidad educativa. Asimismo, su formulación permite articular las acciones de seguridad de la información con el Modelo Integrado de Planeación y Gestión – MIPG**,** fortaleciendo los procesos internos y alineando al Colegio con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y el Departamento Administrativo de la Función Pública – DAFP**.**

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer e implementar un plan de tratamiento de riesgos de seguridad y privacidad de la información en el Establecimiento Público Colegio de Boyacá, que permita identificar, evaluar y mitigar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información, garantizando la continuidad de los procesos académicos, administrativos y financieros de la entidad.

2.2 OBJETIVOS ESPECÍFICOS

1. Identificar y clasificar los activos de información del Colegio de Boyacá, determinando su nivel de criticidad y los procesos asociados.

2. Analizar y evaluar los riesgos de seguridad de la información a partir de amenazas, vulnerabilidades y consecuencias que puedan afectar los procesos institucionales.

3. Definir e implementar medidas y controles de seguridad que permitan mitigar o prevenir los riesgos identificados, en concordancia con la norma NTC-ISO/IEC 27001 y la metodología del MinTIC.

4. Establecer mecanismos de gestión de incidentes, que garanticen la detección, atención y seguimiento de eventos que comprometan la seguridad de la información.

5. Promover la cultura de seguridad digital, capacitando y sensibilizando a funcionarios, docentes y contratistas sobre el manejo seguro de la información.

6. Realizar seguimiento y evaluación periódica al plan mediante indicadores de cumplimiento, asegurando su mejora continua y su articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

3. MARCO NORMATIVO

La seguridad y privacidad de la información en el sector público se encuentra respaldada por un conjunto de normas internacionales, nacionales y lineamientos institucionales que establecen directrices claras para garantizar la confidencialidad, integridad y disponibilidad de los datos. Estas disposiciones normativas orientan la gestión de riesgos, la protección de los activos de información y la adopción de buenas prácticas en el uso responsable de los recursos tecnológicos y digitales.

Tabla 1. Marco Normativo.

Norma / Lineamiento	Entidad emisora	Alcance
ISO/IEC 27001:2013	Organización Internacional de Normalización (ISO) / IEC	Define los requisitos para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27002:2013	ISO / IEC	Proporciona buenas prácticas para la gestión de controles de seguridad de la información.
ISO/IEC 27005:2011	ISO / IEC	Establece directrices para la gestión de riesgos en seguridad de la información.
ISO/IEC 27701:2019	ISO / IEC	Amplía la ISO 27001 con lineamientos para la gestión de la privacidad y protección de datos personales.
Constitución Política de Colombia (1991), Art. 15	Asamblea Nacional Constituyente	Reconoce el derecho a la intimidad y a la protección de datos personales.
Ley 87 de 1993	Congreso de la República	Regula el control interno en las entidades estatales.
Ley 1266 de 2008	Congreso de la República	Establece el régimen de habeas data financiero, crediticio, comercial y de servicios.
Ley 1273 de 2009	Congreso de la República	Define los delitos informáticos y establece sanciones para la afectación de datos y sistemas.
Ley 1581 de 2012	Congreso de la República	Crea el régimen general de protección de datos personales.
Ley 1712 de 2014	Congreso de la República	Regula la transparencia y el acceso a la información pública.
Decreto 1377 de 2013	Presidencia de la República	Reglamenta la Ley 1581 sobre autorizaciones para el tratamiento de datos.

Norma / Lineamiento	Entidad emisora	Alcance
Decreto 612 de 2018	Presidencia de la República / DAFP	Define lineamientos para integrar planes institucionales y estratégicos al Plan de Acción (MIPG).
CONPES 3854 de 2016	Departamento Nacional de Planeación (DNP)	Formula la Política Nacional de Seguridad Digital.
Guía de Administración del Riesgo	DAFP	Orienta metodológicamente la gestión de riesgos en entidades públicas.
Guía de Gestión de Riesgos de Seguridad de la Información	MinTIC	Establece procedimientos específicos para riesgos informáticos en el sector público.
Política de Gobierno Digital	MinTIC	Define la estrategia nacional para la transformación digital y la confianza en el uso de la información.
Modelo Integrado de Planeación y Gestión – MIPG	DAFP / Presidencia de la República	Instrumento para integrar la planeación y la gestión institucional, incluyendo la seguridad de la información.

4. TÉRMINOS Y DEFINICIONES

Activo de información: Todo recurso, físico o digital, que posee valor para la entidad y que soporta sus procesos académicos, administrativos o financieros (bases de datos, aplicaciones, documentos, equipos, redes).

Amenaza: Evento, acción o situación que puede explotar una vulnerabilidad y causar daño a los activos de información.

Autenticidad: Propiedad que garantiza que la información y las comunicaciones provienen de una fuente legítima y confiable.

Confidencialidad: Principio que asegura que la información solo esté disponible para las personas autorizadas.

Disponibilidad: Cualidad que garantiza que la información y los sistemas puedan ser accedidos y utilizados en el momento requerido.

Gestión de incidentes de seguridad de la información: Conjunto de actividades orientadas a detectar, analizar, registrar y dar respuesta a eventos que comprometen la seguridad de la información.

Integridad: Principio que asegura que la información se mantenga completa, precisa y no sea alterada de manera no autorizada.

Política de seguridad de la información: Declaración formal de la entidad que establece el marco de referencia y las directrices para la protección de la información.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y cause impacto en los activos de información de la entidad.

Tratamiento del riesgo: Proceso mediante el cual se adoptan medidas para mitigar, transferir, aceptar o evitar los riesgos identificados.

Vulnerabilidad: Debilidad en procesos, personas, infraestructura o sistemas que puede ser aprovechada por una amenaza para afectar la seguridad de la información.

5. ACTIVIDADES PARA EL DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las actividades definidas en el marco del Plan de Seguridad y Privacidad de la Información del Establecimiento Público Colegio de Boyacá se orientan a garantizar la protección de los activos de información institucionales, fortaleciendo la gestión documental, el control de accesos, la atención de incidentes, la sensibilización de funcionarios y contratistas, así como la implementación de medidas preventivas y correctivas en materia tecnológica. Estas acciones se estructuran en ejes estratégicos que permiten una ejecución organizada y un seguimiento efectivo, asegurando la confidencialidad, integridad y disponibilidad de la información que soporta los procesos académicos, administrativos y financieros del Colegio.

Tabla 2. Actividades del Plan de Seguridad y Privacidad de la Información.

N°	Eje	Actividad	Duración estimada
1	Documentación	Creación e implementación de la Política de Seguridad y Privacidad de la Información, integrada al proyecto de gestión documental del Colegio.	2 meses
2	Documentación	Elaboración y socialización del Manual de Políticas de Seguridad de la Información, alineado a la política institucional.	2 meses
3	Documentación	Actualización de documentos del sistema de gestión de seguridad de la información, conforme a ISO 27001 y lineamientos MinTIC.	2 meses
4	Gestión de incidentes	Creación e implementación del formato para la gestión de riesgos e incidentes de seguridad de la información y acompañamiento en su diligenciamiento.	2 meses

N°	Eje	Actividad	Duración estimada
5	Gestión de incidentes	Atención y gestión de incidentes de seguridad que se presenten, aplicando acciones de mejora y respuesta.	Permanente
6	Sensibilización	Realización de campañas de sensibilización e inducción/reinducción a funcionarios y contratistas sobre seguridad de la información y protección de datos personales.	3 jornadas al año
8	Copias de seguridad	Implementar políticas de copias de seguridad para software institucional.	6 meses
9	Copias de seguridad	Realizar copias periódicas de seguridad en los equipos de cómputo para garantizar la disponibilidad de la información.	Permanente (mensual)
10	Copias de seguridad	Realizar copia de seguridad del servidor institucional para garantizar el acceso a la información.	Permanente (mensual)
11	Control de accesos	Creación de usuarios en los sistemas institucionales para funcionarios y contratistas autorizados.	Según requerimiento
13	Control de accesos	Cambio y actualización periódica de contraseñas de correos institucionales y plataformas digitales.	Trimestral

6. EVALUACIÓN Y SEGUIMIENTO

La evaluación y seguimiento permiten verificar el cumplimiento de las actividades definidas en el Plan de Seguridad y Privacidad de la Información, medir su avance mediante indicadores de gestión y asegurar que las acciones implementadas estén alineadas con los objetivos institucionales. Este proceso facilita la identificación de mejoras y garantiza la adecuada protección de los activos de información del Establecimiento Público Colegio de Boyacá.

Tabla 3. Indicador 01 de gestión

<table>
<tr><th colspan="6">NOMBRE DEL INDICADOR</th></tr>
<tr><td colspan="6">PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EJECUTADO AL 100%</td></tr>
<tr><th colspan="5">OBJETIVO DEL INDICADOR</th><th>PLAZO DE CUMPLIMIENTO</th></tr>
<tr><td colspan="5">MEDIR EL NIVEL DE AVANCE DE LAS ACTIVIDADES PROGRAMADAS EN EL PLAN, GARANTIZANDO SU EJECUCIÓN SEGÚN LO ESTABLECIDO</td><td>12 MESES</td></tr>
<tr><th colspan="6">INFORMACIÓN PARA LA MEDICIÓN DEL INDICADOR</th></tr>
<tr><td>UNIDAD DE MEDIDA</td><td>FRECUENCIA</td><td>META VIGENCIA</td><td>RESPONSABLE MEDICIÓN</td><td>RESPONSABLE ANÁLISIS</td><td>TIPO DE INDICADOR</td></tr>
<tr><td>%</td><td>SEMESTRAL</td><td>100%</td><td>PROFESIONAL SISTEMAS</td><td>PLANEACIÓN-CONTROL INTERNO</td><td>EFICACIA</td></tr>
<tr><th colspan="6">FORMULA DE CALCULO</th></tr>
<tr><td colspan="6">$$\frac{N°\ DE\ INICIATIVAS\ EJECUTADAS}{N°\ DE\ INICIATIVAS\ PLANTEADAS}\ x\ 100$$</td></tr>
</table>

Tabla 4. Indicador 02 de gestión

NOMBRE DEL INDICADOR					
GESTIÓN DE INCIDENTES Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN					
OBJETIVO DEL INDICADOR					**PLAZO DE CUMPLIMIENTO**
EVALUAR LA CAPACIDAD INSTITUCIONAL PARA ATENDER, CONTROLAR Y MITIGAR LOS RIESGOS E INCIDENTES QUE AFECTAN LOS ACTIVOS DE INFORMACIÓN					12 MESES
INFORMACIÓN PARA LA MEDICIÓN DEL INDICADOR					
UNIDAD DE MEDIDA	FRECUENCIA	META VIGENCIA	RESPONSABLE MEDICIÓN	RESPONSABLE ANÁLISIS	TIPO DE INDICADOR
%	TRIMESTRAL	100%	PROFESIONAL SISTEMAS	PLANEACIÓN-CONTROL INTERNO	EFICACIA
FORMULA DE CALCULO					
$\frac{N° \, DE \, INICIATIVAS \, EJECUTADAS}{N° \, DE \, INICIATIVAS \, PLANTEADAS} \; x \, 100$					

7. PLAN DE COMUNICACIONES

El Profesional en Sistemas encargado de formulación y seguimiento del Plan Seguridad y privacidad de la Información del Colegio de Boyacá realizara los pasos de socialización, aprobación y publicación.

- Socialización del Plan de seguridad y privacidad de la información ante Comité de Gestión y Desempeño de la entidad.

- Se someterá a su respectiva aprobación ante el Comité de Gestión y Desempeño de la entidad.

- Una vez aprobado se publicará en la página web de Colegio https://www.colboy.edu.co/colboy/

REFERENCIAS

- Constitución Política de Colombia (1991). Artículo 15: Derecho a la intimidad y protección de datos personales.
- Congreso de la República de Colombia. Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.
- Congreso de la República de Colombia. Ley 1266 de 2008. Régimen de Habeas Data financiero, crediticio, comercial y de servicios.
- Congreso de la República de Colombia. Ley 1273 de 2009. Modifica el Código Penal en materia de delitos informáticos y protección de la información y de los datos.
- Congreso de la República de Colombia. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Congreso de la República de Colombia. Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Presidencia de la República de Colombia. Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012.
- Presidencia de la República / Departamento Administrativo de la Función Pública (DAFP). Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción.
- Departamento Nacional de Planeación (DNP). CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- Departamento Administrativo de la Función Pública (DAFP). Guía de Administración del Riesgo.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Guía de Gestión de Riesgos de Seguridad de la Información.
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Política de Gobierno Digital.

- Organización Internacional de Normalización (ISO) / International Electrotechnical Commission (IEC). ISO/IEC 27001:2013. Sistemas de Gestión de Seguridad de la Información.
- Organización Internacional de Normalización (ISO) / IEC. ISO/IEC 27002:2013. Código de buenas prácticas para controles de seguridad de la información.
- Organización Internacional de Normalización (ISO) / IEC. ISO/IEC 27005:2011. Gestión de riesgos de seguridad de la información.
- Organización Internacional de Normalización (ISO) / IEC. ISO/IEC 27701:2019. Extensión de la ISO 27001 para gestión de la privacidad.