COLEGIO DE BOYACÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2026

CO-PL-04

V.01 / 30-01-2026

COLEGIO DE BOYACÁ

"Iniciador de la Educación Pública en Colombia"

Dr. LUIS SANTIAGO GARCÍA CIFUENTES
Director General

Dr. Diana Carolina Moreno Suesca
Subdirectora Administrativa y Financiera

Merisol Rincón Granados
Subdirectora Académica

Tunja, enero 31 de 2026

TABLA DE CONTENIDO

INTRODUCCIÓN 4
1. **JUSTIFICACIÓN** 5
2. **OBJETIVOS** 6
2.1 OBJETIVO GENERAL 6
2.2 OBJETIVOS ESPECÍFICOS 6
3. **MARCO NORMATIVO** 7
4. **ALCANCE** 9
5. **TÉRMINOS Y DEFINICIONES** 10
6. **METODOLOGÍA** 11
6.1 IDENTIFICACIÓN DEL RIESGO 12
6.1.1 Identificación y valoración de activos 13
6.1.2 Identificación de amenazas 14
6.2. ESTIMACIÓN DEL RIESGO 14
6.3. EVALUACIÓN DEL RIESGO 14
6.4. TRATAMIENTO DEL RIESGO 15
6.5. ACEPTACIÓN DEL RIESGO 15
7. **CRONOGRAMA DE ACTIVIDADES PARA LA EJECUCIÓN DEL PLAN** 16
8. **EVALUACIÓN Y SEGUIMIENTO** 17
9. **PLAN DE COMUNICACIONES** 18
REFERENCIAS 19

INTRODUCCIÓN

La información se ha consolidado como uno de los activos más importantes para las organizaciones, ya que su correcto manejo permite garantizar la continuidad de los procesos institucionales y la confianza de los grupos de interés. El Colegio de Boyacá reconoce que la seguridad y privacidad de la información son esenciales para el cumplimiento de su misión, por lo que se hace necesario contar con lineamientos claros que orienten la identificación, valoración y tratamiento de los riesgos que puedan comprometerla.

El Plan de Tratamiento de Riesgos de Seguridad de la Información busca proteger la confidencialidad, integridad y disponibilidad de los activos de información de la entidad. Para ello, establece mecanismos que permiten anticipar, controlar y mitigar los riesgos que puedan derivarse de amenazas internas o externas, reduciendo así la posibilidad de pérdida, fuga o alteración de datos, así como afectaciones a la continuidad institucional.

Este plan se convierte en una herramienta estratégica para la gestión institucional, en la medida en que promueve una cultura de autocuidado y responsabilidad frente al uso de la información. De esta forma, se asegura que todos los procesos académicos, administrativos y de apoyo cuenten con medidas adecuadas que fortalezcan la protección de la información y garanticen la prestación continua y segura de los servicios ofrecidos por el Colegio de Boyacá.

1. JUSTIFICACIÓN

El Colegio de Boyacá administra información académica, administrativa y financiera que resulta fundamental para el desarrollo de sus funciones esenciales y para la confianza de la comunidad educativa y de las partes interesadas. Esta información, al ser considerada un activo estratégico, debe ser protegida frente a riesgos que puedan comprometer su confidencialidad, integridad y disponibilidad.

La creciente exposición a amenazas internas y externas, como el acceso no autorizado, la alteración de documentos, la fuga de datos o la interrupción de servicios, representa un reto para la institución. La materialización de estos riesgos podría afectar la continuidad de los procesos, la calidad del servicio educativo, así como la imagen y reputación del establecimiento.

En este contexto, se hace indispensable contar con un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que oriente la identificación, análisis y gestión de los riesgos, con el fin de implementar controles y medidas que permitan prevenir, mitigar o responder de manera efectiva a posibles incidentes.
Este plan se justifica en la necesidad de fortalecer la cultura de seguridad institucional, garantizar la adecuada protección de los activos de información y asegurar la prestación continua y confiable de los servicios educativos y administrativos que ofrece el Colegio de Boyacá.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Colegio de Boyacá, definiendo las responsabilidades y actividades que permitan proteger, preservar y garantizar la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información, fortaleciendo así la continuidad de los procesos académicos, administrativos y de apoyo de la institución.

2.2 OBJETIVOS ESPECÍFICOS

- Elaborar y mantener actualizado el inventario de activos de información del Colegio de Boyacá, identificando ubicación, responsables y nivel de criticidad.
- Clasificar y valorar los activos de información de acuerdo con criterios de confidencialidad, integridad y disponibilidad, garantizando que cada activo cuente con su respectiva valoración documentada.
- Diseñar e implementar controles de seguridad de la información que aseguren la protección de los activos críticos y permitan reducir el nivel de riesgo identificado.
- Proyectar y difundir el mapa de riesgos informáticos del Colegio de Boyacá, documentando el contexto, las amenazas y vulnerabilidades que puedan comprometer la seguridad institucional.
- Establecer un sistema de seguimiento y reporte sobre los incidentes de seguridad de la información, con indicadores que permitan medir el nivel de ocurrencia y el porcentaje de incidentes gestionados de manera efectiva.

3. MARCO NORMATIVO

Tabla 1. Normatividad.

Norma / Lineamiento	Entidad emisora	Definición
ISO/IEC 27001	Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC)	Norma internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
ISO/IEC 27005	ISO / IEC	Norma internacional que proporciona directrices para la gestión de riesgos en seguridad de la información, incluyendo identificación, análisis, evaluación y tratamiento.
ISO/IEC 27002	ISO / IEC	Código de buenas prácticas que establece un conjunto de controles de seguridad de la información.
ISO/IEC 27701	ISO / IEC	Extensión de la ISO 27001 que establece directrices para la gestión de la privacidad y la protección de datos personales.
Constitución Política de Colombia (Art. 15)	Asamblea Nacional Constituyente	Reconoce el derecho fundamental a la intimidad, al buen nombre y a la protección de datos personales.
Ley 87 de 1993	Congreso de la República	Establece normas para el ejercicio del control interno en las entidades del Estado.
Ley 1266 de 2008	Congreso de la República	Crea el régimen general de habeas data para el manejo de información financiera, crediticia, comercial y de servicios.
Ley 1273 de 2009	Congreso de la República	Crea nuevos tipos penales relacionados con la protección de la información y de los datos, tipificando delitos informáticos.

Norma / Lineamiento	Entidad emisora	Definición
Ley 1581 de 2012	Congreso de la República	Establece disposiciones generales para la protección de datos personales en Colombia.
Ley 1712 de 2014	Congreso de la República	Regula la transparencia y el derecho de acceso a la información pública nacional.
Decreto 1377 de 2013	Presidencia de la República	Reglamenta parcialmente la Ley 1581 de 2012 en relación con la autorización para el tratamiento de datos personales.
Decreto 612 de 2018	Presidencia de la República / DAFP	Define lineamientos para integrar la planeación y la gestión en las entidades públicas mediante el Modelo Integrado de Planeación y Gestión (MIPG).
CONPES 3854 de 2016	Departamento Nacional de Planeación (DNP)	Formula la Política Nacional de Seguridad Digital, orientada a proteger la infraestructura y los activos de información en el país.
Guía de Administración del Riesgo	Departamento Administrativo de la Función Pública (DAFP)	Documento metodológico que establece lineamientos para la identificación, análisis, valoración y tratamiento de riesgos en entidades públicas.
Guía de Gestión de Riesgos de Seguridad de la Información	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)	Documento técnico que brinda lineamientos específicos para gestionar los riesgos de seguridad de la información en entidades del Estado.
Política de Gobierno Digital	MinTIC	Estrategia nacional que impulsa la transformación digital del Estado y establece lineamientos de seguridad y confianza digital.

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Colegio de Boyacá aplica a todos los procesos académicos, administrativos, financieros y de apoyo que se desarrollan en la institución, así como a los activos de información que se generan, administran o resguardan en el marco de sus funciones esenciales.

El plan cubre la identificación, análisis, valoración y tratamiento de riesgos asociados a la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información, garantizando que los datos de estudiantes, docentes, administrativos y terceros sean gestionados de manera segura y confiable.

Su implementación se enmarca en los lineamientos internacionales, nacionales y sectoriales establecidos en el marco normativo, destacando los estándares ISO/IEC 27001, ISO/IEC 27005, la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 sobre acceso a la información pública y la Política de Gobierno Digital del MinTIC, entre otros.

El plan es de obligatorio cumplimiento para todas las áreas de la institución, el personal vinculado, contratistas y terceros que tengan acceso o administren información del Colegio de Boyacá, asegurando una gestión integral de los riesgos y la continuidad de los servicios educativos y administrativos que presta la entidad.

5. TÉRMINOS Y DEFINICIONES

Seguridad informática: Se ocupa de la implementación técnica y de la operación para la protección de la información.

Seguridad de la información: Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.

Amenazas: Cualquier evento, persona, situación o fenómeno que pueda causar daño.

Vulnerabilidades: Falla o debilidad en un sistema que puede ser explotada por quien la conozca.

Riesgo: Probabilidad de ocurrencia de una amenaza.

Controles: Conjunto de mecanismos que regulan el funcionamiento de un sistema.

ISO: Organización Internacional de Normalización es una organización para la creación de estándares internacionales.

Activo: Bienes, recursos o derechos que tenga valor para una organización.

Activo de Información: Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.

Análisis de brechas: es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.

Análisis de Riesgo: Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.

Gestión del Riesgo Informáticos: Actividades empleadas para mitigar los riesgos informáticos.

Incidente de seguridad informática: daño que puede comprometer las operaciones del Colegio de Boyacá.

Evento: Acción que puedo haber causado daño, pero fue controlado**.**

Información: Conjunto de datos que tienen un significado.

Probabilidad: Posibilidad de que una amenaza se materialice

Impacto: Daño que provoca la materialización de una amenaza.

SGSI: Sistema de Gestión de seguridad de la Información

MSPI: Modelo de seguridad y privacidad de la información

PHVA: Planear, hacer, verificar, actuar.

6. METODOLOGÍA

Las instituciones educativas, al igual que cualquier otra organización, deben implementar planes que les permitan gestionar los riesgos que afectan sus sistemas de información, las tecnologías utilizadas y los activos de información que administran. En la actualidad, uno de los principales riesgos proviene de amenazas y ataques dirigidos a plataformas académicas, sistemas administrativos y servicios de comunicación digital, los cuales pueden comprometer la disponibilidad, integridad y confidencialidad de la información institucional.

Por esta razón, y siguiendo los lineamientos de la Norma NTC ISO/IEC 27005, que proporciona directrices para la gestión del riesgo en seguridad de la información, así como las orientaciones emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y la estrategia de Gobierno Digital, el Colegio de Boyacá adelantará la gestión de los riesgos asociados a la institución mediante un proceso estructurado que incluye el **diagnóstico, identificación, análisis y evaluación de riesgos**. Este proceso permitirá establecer controles y medidas de tratamiento que aseguren la protección de los activos de información académicos, administrativos y financieros, fortaleciendo la continuidad de los procesos institucionales y la confianza de la comunidad educativa.

En la siguiente ilustración se muestra el procedimiento de la guía 7 que propone el departamento administrativo de la función pública (DAFP) junto con el ministerio de la tecnología de información y comunicación (MinTIC) para la gestión de riesgos informáticos.

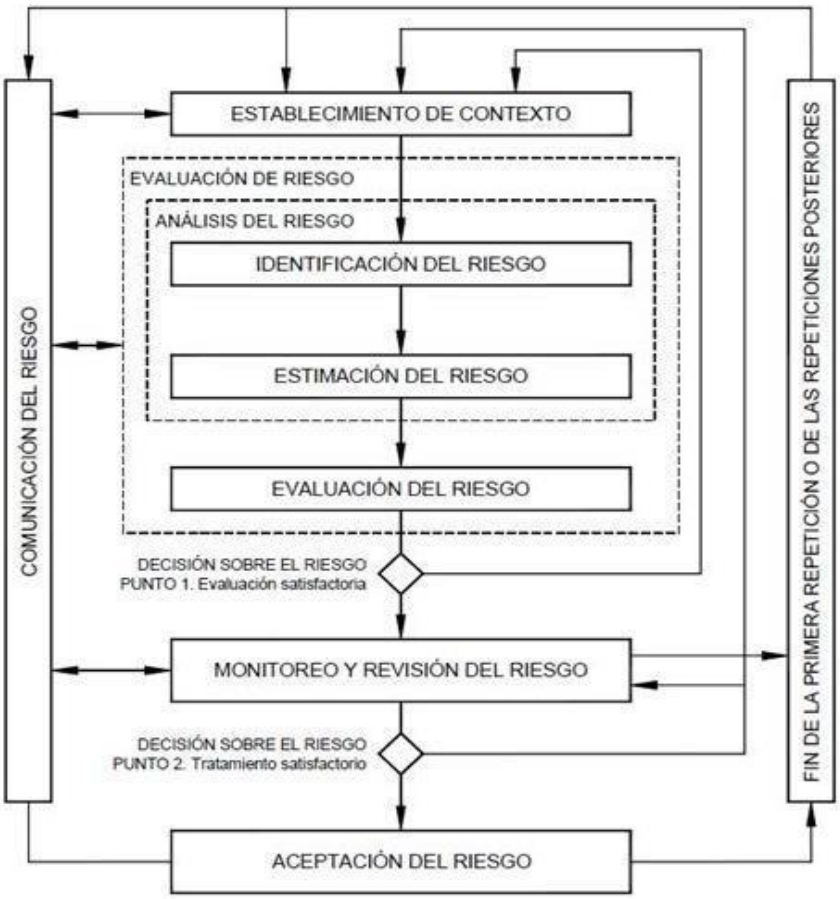

Ilustración 1: Tomada de NTC-ISO/IEC 27005 Gestión de Riesgos

6.1 IDENTIFICACIÓN DEL RIESGO

La seguridad de la información en el Colegio de Boyacá se fundamenta en la triada compuesta por la confidencialidad, integridad y disponibilidad, principios que permiten garantizar un manejo seguro y confiable de los activos de información. La confidencialidad asegura que los datos sean accesibles únicamente por las personas autorizadas; la integridad busca mantener la exactitud y consistencia de la información a lo largo de su ciclo de vida; y la disponibilidad garantiza que los usuarios tengan acceso oportuno a la información cuando la requieran. Estos tres elementos, en conjunto, constituyen la base para la gestión de los riesgos de seguridad de la información en la institución.

Ilustración 2: *Pilares de la seguridad informática*

6.1.1 Identificación y valoración de activos

En el contexto de la seguridad digital, un activo de información es todo elemento que posee un valor para la organización. Estos activos pueden estar representados en bases de datos, servicios web, redes de comunicación, aplicaciones, documentos físicos o digitales, y en general, cualquier recurso que soporte el funcionamiento institucional. Para la elaboración del inventario de activos de información en el Colegio de Boyacá, se deben listar los activos por cada proceso, identificar al responsable o dueño del activo, clasificar tanto los activos como la información que contienen, determinar su nivel de criticidad y establecer si hacen parte de la infraestructura crítica cibernética de la institución. Este ejercicio constituye la base para la gestión de riesgos y la definición de controles que garanticen la protección de la información.

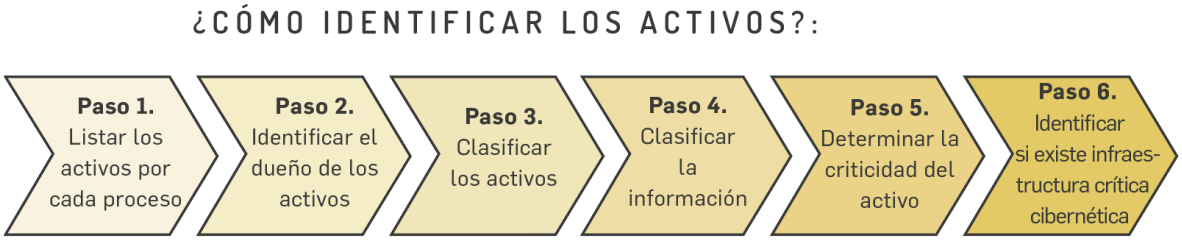

Ilustración 3. Identificación de activos
Fuente. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas DAFP

6.1.2 Identificación de amenazas

La identificación de amenazas en el Colegio de Boyacá tiene como propósito reconocer aquellas situaciones que puedan generar daños sobre los activos de información institucionales, comprometiendo procesos académicos, administrativos, financieros o de apoyo. Las amenazas pueden ser de origen interno o externo y, por tanto, ninguna debe ser descartada en el análisis. Se clasifican en tres categorías principales:

- Deliberadas (D): acciones intencionales orientadas a afectar los activos de información.
- Accidentales (A): situaciones derivadas de errores humanos no intencionados.
- Ambientales (E): eventos externos asociados a condiciones naturales o del entorno.

6.2. ESTIMACIÓN DEL RIESGO

La estimación del riesgo permite valorar en detalle el impacto que las amenazas identificadas pueden tener sobre los activos de información de la institución. Este ejercicio puede desarrollarse bajo dos enfoques:

- **Cualitativo:** emplea escalas descriptivas (alto, medio, bajo) para determinar la probabilidad de ocurrencia y las consecuencias.
- **Cuantitativo:** utiliza valores numéricos para precisar la magnitud del impacto y la probabilidad de ocurrencia.

6.3. EVALUACIÓN DEL RIESGO

La evaluación de riesgos consiste en comparar los riesgos estimados con los criterios definidos por la institución, considerando factores como consecuencias, probabilidad de ocurrencia y nivel de confianza del análisis. Es importante atender a los riesgos acumulativos, pues la combinación de varios riesgos de nivel bajo o medio puede constituir una amenaza significativa para la continuidad institucional.

6.4. TRATAMIENTO DEL RIESGO

El tratamiento de los riesgos será realizado a partir de la evaluación obtenida, priorizando las medidas en función de los costos, beneficios e impacto en los procesos institucionales. Para ello, se aplicarán de manera estratégica las siguientes opciones:

Reducción: aplicación de controles que disminuyan la probabilidad o el impacto del riesgo.

Retención: aceptación del riesgo y asunción de las posibles consecuencias.

Evitar: adopción de medidas preventivas para eliminar la causa del riesgo.

Transferir: traslado total o parcial de las consecuencias del riesgo a un tercero.

Igualmente, se diseñará un plan de implementación que contemple actividades específicas, responsables definidos y mecanismos de seguimiento, con el fin de asegurar la protección de los activos de información de la institución.

6.5. ACEPTACIÓN DEL RIESGO

La aceptabilidad de los riesgos estará determinada por su nivel, de acuerdo con los siguientes criterios:

- **Bajo:** riesgo aceptable.
- **Medio**: riesgo mejorable, requiere medidas de ajuste.
- **Alto:** riesgo no aceptable, salvo que existan controles específicos que lo mitiguen adecuadamente.
- **Crítico**: riesgo no aceptable bajo ninguna circunstancia.

7. CRONOGRAMA DE ACTIVIDADES PARA LA EJECUCIÓN DEL PLAN

El cronograma de actividades del Plan de Tratamiento de Riesgos de Seguridad de la Información del Colegio de Boyacá establece la programación de las acciones que se desarrollarán durante la vigencia 2025, con el propósito de garantizar la protección, integridad, disponibilidad y confidencialidad de los activos de información de la institución. Este cronograma organiza las actividades por ejes estratégicos, define responsables y tiempos de ejecución, y permite realizar un seguimiento ordenado y sistemático al cumplimiento de cada tarea, asegurando así la continuidad de los procesos académicos, administrativos y de apoyo en condiciones de seguridad y confianza.

Tabla 2. Cronograma de ejecución de actividades 2025

N°	Eje	Actividad	Responsable	Tiempo estimado
1	Diagnóstico inicial	Levantar inventario de activos de información en cada proceso institucional y clasificarlos por nivel de criticidad.	Responsables de Procesos / subdirectora Adm. y Financiera	2 meses
2	Identificación de riesgos	Analizar amenazas, vulnerabilidades y consecuencias sobre los activos de información; elaborar la matriz de riesgos.	Responsables de Procesos	2 meses
3	Plan de tratamiento	Actualizar y consolidar el plan de tratamiento de riesgos con base en los lineamientos del MinTIC e ISO 27005.	Subdirectora Adm. y Financiera	2 meses
4	Implementación de controles	Aplicar medidas preventivas (copias de seguridad, contraseñas seguras, control de accesos físicos y digitales).	Responsables de Procesos / Profesional de Sistemas	3 meses
5	Capacitación y sensibilización	Desarrollar jornadas de capacitación para funcionarios, docentes y contratistas sobre manejo seguro de la información.	Responsables de Procesos / Profesional de Sistemas	1 mes
6	Gestión de incidentes	Atender y registrar incidentes de seguridad que se presenten, garantizando trazabilidad y acciones correctivas.	Responsables de Procesos	Permanente
7	Seguimiento y mejora continua	Revisar trimestralmente la efectividad de los controles, actualizar la matriz de riesgos y generar reportes a la dirección.	Subdirectora Adm. y Financiera	2 seguimientos

8. EVALUACIÓN Y SEGUIMIENTO

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Colegio de Boyacá será evaluado y monitoreado a través del indicador de avance del plan, calculado como el porcentaje de actividades ejecutadas frente al total programado.

Este seguimiento permitirá medir el cumplimiento, identificar oportunidades de mejora y asegurar la protección de los activos de información.

Tabla 3. Indicador de gestión.

<table>
<tr><th colspan="6">NOMBRE DEL INDICADOR</th></tr>
<tr><td colspan="6">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD 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 GRADO DE CUMPLIMIENTO DE LAS ACTIVIDADES PROGRAMADAS EN EL CRONOGRAMA DEL PLAN DURANTE LA VIGENCIA 2025.</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>TRIMESTRAL</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>

9. PLAN DE COMUNICACIONES

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

- Socialización del Plan de Tratamiento de Riesgos de Seguridad 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

- ISO/IEC 27001:2013. Tecnología de la información–Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos.
- ISO/IEC 27002:2013. Tecnología de la información – Técnicas de seguridad – Código de buenas prácticas para los controles de seguridad de la información.
- ISO/IEC 27005:2011. Tecnología de la información – Técnicas de seguridad – Gestión del riesgo en seguridad de la información.
- Constitución Política de Colombia (1991), Artículo 15. Derecho a la intimidad y protección de datos personales.
- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades del Estado.
- Ley 1266 de 2008. Régimen de habeas data en información financiera, crediticia, comercial y de servicios.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, creando delitos informáticos y contra la protección de datos.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1377 de 2013. Reglamenta parcialmente la Ley 1581 de 2012 en materia de autorización para el tratamiento de datos.
- Decreto 612 de 2018. Lineamientos para integrar la planeación y la gestión en las entidades públicas (MIPG).
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. Guía de Gestión de Riesgos de Seguridad de la Información.
- Departamento Administrativo de la Función Pública – DAFP. Guía de Administración del Riesgo.
- MinTIC. Política de Gobierno Digital.
- Modelo Integrado de Planeación y Gestión – MIPG. Instrumento para la gestión y desempeño institucional en el sector público.