



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD  
Y PRIVACIDAD DE LA INFORMACIÓN EN LA  
INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE  
ANTIOQUIA.**



## 1. INTRODUCCIÓN

La institución Universitaria Colegio Mayor de Antioquia ha implementado un enfoque lógico y sistemático con el objetivo de mejorar continuamente la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados al manejo de la información institucional. Esto se realiza para prevenir, controlar e incluir medidas para mitigar los riesgos y la aparición de los mismos. En todas las actividades y tareas diarias, la institución utiliza las Tecnologías de la Información y la Comunicación (TIC) para la captura, procesamiento y reporte seguro y oportuno de información tanto interna como externa. De esta manera, se evita la vulneración de la misma frente a posibles ataques o mala manipulación, lo que podría generar problemas legales, económicos y administrativos.

Con este documento, se busca establecer una línea de trabajo que garantice la seguridad y la correcta manipulación de los datos almacenados en las diferentes bases de datos institucionales.

## 2. ALCANCE

La vigencia del presente plan es 2023-2025 y aplica para los procesos evidenciados en el Mapa de Procesos Institucionales.

## 3. OBJETIVO

### 3.1 GENERAL

Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineado con la guía metodológica para la gestión del riesgo del Departamento Administrativo de la Función Pública y las disposiciones de la Ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

### 3.2. ESPECÍFICOS

- Obtener un diagnóstico preciso de la situación actual de la Institución Universitaria Colegio Mayor de Antioquia en relación a los riesgos de seguridad y privacidad de la información.
- Implementar metodologías, recomendaciones y mejores prácticas establecidas por el DAFP y Min Tic para abordar los riesgos de seguridad y privacidad de la información de manera efectiva.
- Contribuir al desarrollo y fortalecimiento del modelo integrado de planificación y gestión en las políticas de Gobierno Digital, Seguridad Digital, Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción, mediante la implementación de



medidas y acciones concretas.



4. incluir dentro del mapa de riesgos institucional los peligros relacionados con la seguridad y la privacidad de la información.

## 5. RECURSOS

RECURSOS	VARIABLE
Humanos	<ul style="list-style-type: none"><li>• El Grupo Interno de Trabajo de Seguridad y Privacidad de la Información</li><li>• Profesional de riesgos del Grupo Interno de Trabajo de Transformación Organizacional</li><li>• Líderes y gestores de procesos</li><li>• Dimensión de Seguridad informática de la Oficina de TI</li><li>• Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT</li><li>• Equipo de Trabajo de Seguridad y Privacidad de la Información de la Dirección de Gobierno Digital.</li></ul>
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en el GIT de Seguridad y Privacidad de la Información

## 6. RESPONSABLES

- La Alta Dirección
- Oficina Gestión Documental
- Equipo MIPG
- Oficina de Control Interno
- Talento Humano
- Líderes de Proceso
- Líder de Tecnología
- Planeación institucional
- Equipo de Comunicaciones

## 7. MARCO CONCEPTUAL

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.



- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española). Control Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Criticidad:** Ej. Catastrófico, Mayor, Moderado, Menor, Insignificante.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- **Eficacia:** Grado en el que se realizan las actividades planificadas y se logran los resultados planificados. NTC ISO 9000: 2015.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión o Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Parte interesada:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Revisión:** Acción para determinar la idoneidad, conveniencia y eficacia de la gestión del riesgo.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus



consecuencias.

- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de dirección para modificar su probabilidad o impacto. (primer análisis).
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas (dirección) de tratamiento del riesgo. (análisis final/permanece).
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguimiento:** Asegurar que las acciones establecidas se están llevando a cabo.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.
- **Trazabilidad:** Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## 8. MARCO NORMATIVO

- Ley 909 de 2004: “Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones”.
- Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Decreto Municipal 500 de 2013: “Por el cual se aprueba la misión, visión, valores, principios orientadores de la función pública y el modelo institucional de la Administración Central del Municipio de Medellín y se dictan otras disposiciones”.
- Decreto Ministerial 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.



- Decreto Presidencial 1083 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- Decreto Municipal 883 de 2015: “Por el cual se adecúa la Estructura de la Administración Municipal de Medellín, las funciones de sus organismos, dependencias y entidades descentralizadas, se modifican unas entidades descentralizadas y se dictan otras disposiciones”.
- Decreto Presidencial 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”.
- Decreto Municipal 0863 de 2020: “Por el cual se modifica la estructura orgánica y funcional del nivel central del Municipio de Medellín”.
- Decreto Presidencial 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Resolución Ministerial 00500 de 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital”.
- ISO/IEC 27001:2013: Tecnología de la información-Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos.
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
- Ley 87 de 1993 Literal a) Proteger los recursos de la organización buscando su adecuada administración ante los posibles riesgos



que los afectan

Literal f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir desviaciones que se presentan en la organización y que puedan afectar el logro de los objetivos.

- Decreto 1537 de 2001 Artículo 4. La administración de los riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades publicas
- Ley 1474 de 2011 Estatuto anticorrupción Art. 73. “Plan anticorrupción y atención al ciudadano” que debe elaborarse anualmente, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.
- Decreto 1499 de 2017 Dimensión 7 – Control Interno Atributo de calidad 5.: Riesgos identificados y gestionados que permiten asegurar el cumplimiento de los objetivos.
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información
- Decreto 1759 de 8 de noviembre de 2016 por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo
- Resolución 670 de 14 de diciembre de 2017 de la Procuraduría General de la Nación, por medio de la cual se adopta el manual de políticas y procedimientos para la protección de datos personales.
- Ley 1915 de 12 de julio de 2018, por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de Derecho de Autor y Derechos Conexos.
- Ley 1928 de 24 de julio de 2018, por medio de la cual se aprueba el “Convenio sobre la ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
- Proyecto de ley 300 de 2020, del 11 de marzo de 2020, por medio de la cual se dictan disposiciones generales para el fortalecimiento de la protección de datos personales, con relación al reconocimiento de las garantías de los derechos digitales, y se dictan otras disposiciones.
- Decreto 1287 de 24 de septiembre de 2020, por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.





## 9. TRATAMIENTO DE RIESGOS SEGURIDAD DE LA INFORMACIÓN

Conociendo los activos de información, su criticidad, y las implicaciones económicas, legales y reputacionales que puedan surgir por verse afectada la disponibilidad, integridad y confidencialidad de la información, se deben tomar algunas de las siguientes acciones para el tratamiento del riesgo:

### **Aceptar el riesgo**

La entidad decide después de un análisis no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Esta opción se puede considerar para riesgos con nivel bajo, sin embargo, se pueden presentar riesgos con otro nivel a los cuales la entidad no puede aplicar controles o planes para reducir el riesgo y es necesario aceptarlo. El hecho de aceptarlo no implica que se olvide, sino que se debe hacer un seguimiento continuo del riesgo.

### **Reducir el riesgo**

Se generan controles y/o planes de mejora que permitan reducir la probabilidad y/o el impacto del riesgo, estos controles están relacionados con la implementación de la ISO/IEC 27002, los cuales permiten una segregación de funciones, registros, entre otros que permitan la reducción prevista sobre el riesgo.

### **Evitar el riesgo**

En este caso la entidad deja de realizar las actividades que dan lugar al riesgo.

### **Compartir el riesgo**

En este caso existen dos maneras de compartir el riesgo y es tercerizar la operación de la actividad que conlleva la probabilidad del riesgo y la otra manera es por medio de la adquisición de un seguro.

## **9.1. ACTIVIDADES Y ENTREGABLES DE LAS FASES DE LA METODOLOGÍA DE IMPLEMENTACIÓN**

### **9.1.1. Fase I – Caracterización de los sistemas de gestión y de los procesos de la Entidad**

Dentro de esta fase se realizan las siguientes actividades:

- 9.1.1.1. Listado Maestro de Registros en el SIG Actualizado
- 9.1.1.2. Identificación de procedimientos actualizados
- 9.1.1.3. Inventario de activos de información



### 9.1.2 Fase II – Identificación de riesgos

Dentro de esta fase se realizan las siguientes actividades:

- 9.1.1.4. Identificación de causas
- 9.1.1.5. Identificación de riesgo.
- 9.1.1.6. Establecer las consecuencias
- 9.1.1.7. Tipificar y valorar el riesgo
- 9.1.1.8. Determinar el impacto
- 9.1.1.9. Determinar la probabilidad
- 9.1.1.10. Determinar el nivel de riesgo inherente y residual

### 10 Fase III – Valoración de controles

- Cálculo estimado del riesgo residual
- Selección de la opción de tratamiento
- Determinar las acciones de mitigación del riesgo

#### 10.1. Fase V – Seguimiento y Evaluación.

- Realizar seguimiento a la autoevaluación de la gestión por áreas
- Realizar monitoreo de los riesgos a través de la evaluación independiente que realiza la Entidad y el líder del sistema de gestión de seguridad y privacidad de la información.
- Determinar las alertas que se generen a partir de los resultados de las mediciones anteriores
- Aplicar acciones de mejora continua. resultado de las auditorías, de los mapas de riesgos y planes de acción.
- Socialización de resultados

### 11 METODOLOGÍA DE IMPLEMENTACIÓN

La metodología para la implementación de riesgos del DAFP (Departamento Administrativo de la Función Pública) se basa en tres pasos principales: Política de administración del riesgo, identificación del riesgo y valoración del riesgo



Paso	Descripción
Política de administración del riesgo	Declaración de la Dirección y las intenciones generales de una organización con respecto a la administración del riesgo <sup>2</sup> .
Identificación del riesgo	Proceso de encontrar, reconocer y describir los riesgos que podrían afectar la consecución de los objetivos de la organización <sup>2</sup> .
Valoración del riesgo	Evaluar la probabilidad y el impacto de cada riesgo identificado <sup>2</sup> .

Esta metodología proporciona un marco estructurado para la gestión de riesgos en entidades públicas, con el fin de identificar, evaluar y mitigar los riesgos de manera efectiva

Fuente: Cartilla de administración de riesgos del DAFP ISO 31000:2018

### 11.1. Metodología para la administración del riesgo



#### 11.1.1. Etapas de metodología

#### 11.1.2. Identificación del riesgo

Proceso para encontrar, reconocer y describir el riesgo.

¿Qué busca?: Establecer **factores o fuentes** de riesgo, los **eventos o riesgos**, sus



**causas y sus consecuencias.**

**Con apoyo de:** Datos históricos, análisis teóricos, opiniones informadas, expertos, proveedores, partes interesadas.

**¿Cómo hacerlo?:** Entrevistas, reunión con directivos y/o diferentes niveles de la entidad, lluvia de ideas, diagramas de flujo, revisión factores económicos y /o tecnológicos que afecten la entidad.

**Factores o fuente generador:** Aquello que tiene el potencial intrínseco para hacer daño o generar oportunidades.

Entorno, equipo, relaciones legales y comerciales, personas, equipos, entorno e instalaciones. Guía para la Admón. del riesgo 5.2.2 literal b) fuente o agente generador)

**Evento o riesgo:** Aquello que ocurre, de manera que la fuente de riesgo genera un impacto.

**Causa:** El qué y por qué de la presencia del peligro o evento que ocurre.

**Consecuencia:** Resultado o impacto sobre un grupo de partes involucradas y recursos.

**11.1.3. Análisis del riesgo**

Establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial. **(Riesgo Inherente).**

**Ejemplo tabla para determinar el impacto:**

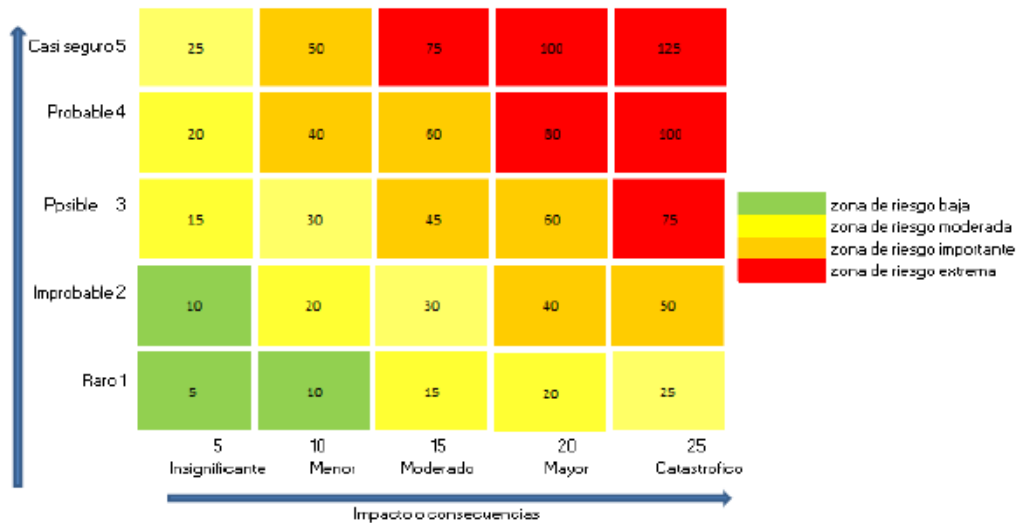
**Ejemplo** tabla para determinar la probabilidad:

Valor probabilidad	Nivel Probabilidad	Frecuencia: Se ha presentado..
5	Casi cierto	Más de una vez al año
4	Probable	Al menos una vez en el ultimo año
3	Posible	Al menos una vez en los ultimos dos (2) años
2	Improbable	Al menos una vez en los ultimos cinco (5) años
1	Raro	No se ha presentado en los último cinco (5) años

Tipo de Impacto	Niveles de Impacto/Valor
Incumplimiento de Metas.	Catrástófico - 25
Perdida Presupuestal. Pérdidas Económicas. Sanciones Legales.	Mayor - 20
Afectación en la Prestación de los servicios de la Entidad. Pérdida de Imagen y Credibilidad.	Moderado - 15
Inoperabilidad de los Sistemas de información Crítica. Pérdida o Alteración de Información Crítica.	Menor - 10
	Insignificante - 5

**- Calificación del riesgo**

Calificar o valorar el riesgo significa establecer su Probabilidad e Impacto:



Ejemplo Niveles del Calificación Riesgo

#### 11.1.4. Evaluación del riesgo


Confrontar los resultados del análisis del riesgo inicial a los controles establecidos, con el fin de determinar la zona de riesgo final – **Riesgo residual**.

##### - Acciones para valorar el riesgo

- Identificar los controles existentes.
- ¿Quién lleva a cabo el control? Responsable.
- ¿Qué busca hacer el control? Objetivo.
- ¿Cómo se lleva a cabo el control? Procedimiento.
- Evidencia de la ejecución del control
- ¿Tipo de control? Manual o automático.
- ¿Cuándo se realiza el control? Periodicidad.

##### - Naturaleza del control

- **Preventivo:** Evitan que el evento suceda. Ej.: Capacitación del personal, evitar la producción de errores.
- **Detectivo:** Permiten registrar un evento después de que ha sucedido. Ej.: Programa de auditoría, para evidenciar errores que no fueron corregidos con controles preventivos.
- **Correctivo:** No prevén que un evento suceda, pero permiten enfrentar la

 <b>INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA</b>	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GT-MA-004</b>		
	Versión: 01	Fecha: 01-02-2022	Página 14 de 14

situación una vez ha sucedido. Ej.: Pólizas de seguro, recuperar la operación.

#### **11.1.5. Revisión y seguimiento**

Determinar Eficacia de la implementación, realizar revisiones periódicas, lecciones aprendidas, detectar cambios en el contexto externo e interno, criticidad de los riesgos, acciones de tratamiento.

## **12 DESARROLLO DEL PLAN**

El seguimiento del presente plan se realiza conforme a los diferentes informes y tiempos establecidos en el Plan de Acción por proceso, y es registrado en un documento de control de avance del mismo, y a su vez quedará registrado el resultado en el mapa de riesgos institucional con su debida identificación como “Riesgo de Seguridad y Privacidad de la Información”.