ACUERDO Nro. 004

25 de febrero de 2022

«Por medio del cual se actualiza y se aprueba la Política de Administración del Riesgo de la Institución Universitaria Colegio Mayor de Antioquia»

EL CONSEJO DIRECTIVO DE LA INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA, en uso de sus atribuciones legales y estatutarias, en especial las que le confieren la Ley 30 de 1992, Ley 489 de 1998 y el Acuerdo No. 002 del 09 de febrero de 2007 –Estatuto General–, y

CONSIDERANDO

Que el artículo 83 de la Constitución Política dispone que todas las actuaciones de los particulares y de las autoridades públicas deberán ceñirse a los postulados de la buena fe, la cual se presumirá en todas las gestiones que aquellos adelanten ante estas.

Que de conformidad con lo establecido en el Acuerdo No. 002 de 2007 Estatuto General de la Institución Universitaria Colegio Mayor de Antioquia, en el artículo 13 literal a) es función del Consejo Directivo definir las políticas académicas, administrativas, financieras y la planeación institucional.

Que mediante la Ley 87 de 1993 se establecen las normas para el ejercicio del Control Interno en todas las entidades y organismos del Estado.

Que la Ley 489 de 1998 crea el Sistema Nacional de Control Interno el cual tiene por objeto integrar de forma armónica, dinámica, efectiva, flexible y suficiente, el funcionamiento del control interno en las instituciones públicas

Que para la operatividad del Sistema de Control Interno se emite el Decreto 1599 de 2005 para la creación del Modelo Estándar de Control Interno – MECI, el cual define elementos similares de control para las entidades públicas.

Que la Ley 1474 de 2011 define el Estatuto Anticorrupción, en el cual se establece el Plan Anticorrupción y de Atención al Ciudadano en el que se debe incluir el mapa de riesgos de corrupción.

Que el Decreto 1499 de 2017 modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Que el Departamento Administrativo de la Función Pública – DAFP, publicó la Guía para la administración del riesgo y el diseño de controles en entidades públicas y la Cartilla Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

Que el DAFP, a través del Marco General del MIPG actualiza el MECI para armonizarlo con el Modelo Integrado de Planeación y Gestión – MIPG, e implementar las mejores prácticas en la materia.

Que la Resolución No. 090 de abril 29 de 2020, establece la conformación de las líneas de defensa al interior de la Institución Universitaria Colegio Mayor de Antioquia, y se asignan responsabilidades a las mismas, de acuerdo con el Modelo Estándar de Control Interno - MECI.

Que la Institución en la implementación del Sistema de Gestión Integrado debe dar cumplimiento al requisito 6.1 Acciones para abordar riesgos y oportunidades de las normas NTC ISO 9001:2015 Sistema de Gestión de la Calidad, NTC ISO 14001:2015 Sistema de Gestión Ambiental y NTC ISO 45001:2018 Sistemas de Gestión de la Seguridad y Salud en el Trabajo.

En mérito de lo expuesto.

ACUERDA:

ARTÍCULO PRIMERO. ACTUALIZAR la Política de Administración del Riesgo de la Institución Universitaria Colegio Mayor de Antioquia.

ARTÍCULO SEGUNDO. DEROGAR el Acuerdo 011 del 1 de octubre de 2020, "por medio del cual se actualiza la Política de Administración del Riesgo de la Institución Universitaria Colegio Mayor de Antioquia".

ARTÍCULO TERCERO. Las disposiciones prescritas en esta Política serán aplicadas a los objetivos estratégicos, los procesos y subprocesos de la Institución y a todas las actividades realizadas por los servidores durante el ejercicio de sus funciones y los contratistas en el cumplimiento del plan de trabajo asignado.

ARTÍCULO CUARTO. Difundir esta política institucional a la comunidad educativa y al público en general, a través de los diferentes medios de comunicación establecidos por la Institución Universitaria Colegio Mayor de Antioquia.

ARTÍCULO QUINTO. El presente acuerdo rige a partir del día siguiente de su publicación y deroga las demás disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

Dado en Medellín, el 25 de febrero de 2022.

MARTHA ALEXANDRA AGUDELO RUIZ
Presidente del Consejo Directivo.

DIANA PATRICIA GÓMEZ RAMÍREZ
Secretario del Consejo Directivo.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Política de Administración del Riesgo es el marco de referencia para la gestión de los riesgos y pretende fortalecer la cultura institucional hacia el pensamiento basado en riesgos, buscando aumentar la probabilidad de alcanzar los objetivos institucionales.

Es el compromiso de la Alta Dirección frente a la gestión de los riesgos en la Institución, garantizando los recursos necesarios para implementar los controles que permitan mitigarlos y en caso de materialización, que estos conduzcan a reducir el impacto y evitar que estos se vuelvan a presentar.

1. OBJETIVO GENERAL

Establecer los elementos y el marco general de actuación para la gestión integral de los riesgos a los que se enfrenta la Institución y orientar las acciones necesarias que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el logro de su misión, objetivos institucionales y preparar la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo.

1.1 OBJETIVOS ESPECIFICOS

- Contribuir al cumplimiento de los objetivos estratégicos y de los procesos a través de una adecuada administración de los riesgos.
- Proteger los recursos de la Institución y del Estado, resguardándolos contra la materialización de los actos que vayan en detrimento del bien público.
- Involucrar a todos los servidores en la implementación de acciones eficaces encaminadas a prevenir y mitigar los riesgos que permitan garantizar la continuidad de la Institución.
- Fortalecer una cultura organizacional con un pensamiento basado en riesgos.

2. TÉRMINOS Y DEFINICIONES

- **Riesgo:**[1]
  Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

[1] Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 5 Pág. 12

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Riesgo de Corrupción:**[2]

  Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Fraude:** [3]

  Acción de engaño intencional, que ejecuta un servidor público o particular con funciones públicas, con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Riesgo de Fraude:** [4]

  Efecto que se causa sobre los objetivos de las entidades debido a una acción de engaño intencional, que un servidor público o particular con funciones públicas, ejecuta con el propósito de conseguir un beneficio o ventaja ilegal para sí mismo o para un tercero.
- **Riesgo de Seguridad de la Información:**[5]

  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).
- **Probabilidad:**[6]

  Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el período de 1 año.
- **Causa:**[7]

  Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:**[8]

  Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:**[9]

[2] Ídem anterior.
[3] Fuente: Buenas prácticas para el análisis de riesgos de fraude y corrupción FunciónPública.Pag.1
[4] Fuente: Buenas prácticas para el análisis de riesgos de fraude y corrupción FunciónPública.Pag.1
[5] Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 5 Pág. 12
[6] Ídem anterior.
[7] Ídem anterior.
[8] Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 5 Pág. 12
[9] Ídem anterior.

Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

- **Consecuencia:**[10]

  Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Impacto:**[11]

  Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Riesgo Inherente:**[12]

  Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:**[13]

  El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Control:**[14]

  Medida que permite reducir o mitigar un riesgo.
- **Factores de Riesgo:**[15]

  Son las fuentes generadoras de riesgo.
- **Apetito de riesgo:**[16]

  Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del órgano de gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Tolerancia del riesgo:**[17]

  Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad del riesgo:**[18]

  Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección y el órgano de gobierno que no sería posible el logro de los objetivos de la entidad.

---

[10] Ídem anterior.
[11] Ídem anterior
[12] Ídem anterior.
[13] Ídem anterior.
[14] Ídem anterior.
[15] Ídem anterior.
[16] Ídem anterior.
[17] Ídem anterior
[18] Ídem anterior

- **Nivel de riesgo:**[19]

  Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del nivel de riesgo puede ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- **Activo:**[20]

  En el contexto de la seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Confidencialidad:**[21]

  Propiedad de la información que la hace no disponible, o sea, divulgada a individuos, entidades o procesos no autorizados.
- **Vulnerabilidad:**[22]

  Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **Integridad:**[23]

  Propiedad de exactitud y completitud.
- **Disponibilidad:**[24]

  Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Plan Anticorrupción y de Atención al Ciudadano:**[25]

  Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementado por todas las entidades del orden nacional, departamental y municipal.

3. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

3.1 Metodología:

Para una adecuada administración de los riesgos, la Institución ha adoptado la metodología diseñada por el Departamento Administrativo de la Función Pública, a través de la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

Esta metodología comprende los siguientes pasos:

Paso 1. Política de Administración del riesgo

[19] Ídem anterior.
[20] Ídem anterior.
[21] Ídem anterior.
[22] Ídem anterior.
[23] Ídem anterior.
[24] Ídem anterior.
[25] Ídem anterior.

Paso 2. Identificación del riesgo
Paso 3. Valoración del riesgo

Paso 1. La Política de Administración del riesgo, se genera a partir de la dimensión "Direccionamiento Estratégico y Planeación" del Modelo Integrado de Planeación y Gestión – MIPG, la establece la Alta Dirección con el liderazgo del Representante Legal y con la participación del Comité Institucional de Coordinación de Control Interno y se constituye en la base para la gestión del riesgo en todos los niveles de la Institución. Se consideran los siguientes elementos:

1.1 Lineamientos de la Política
1.2 Marco conceptual para el apetito del riesgo.
Se debe considerar en este punto los conceptos de apetito del riesgo, tolerancia del riesgo y capacidad del riesgo que deben ser definidos por la Alta Dirección teniendo en cuenta los objetivos y el marco legal de la Institución.

Paso 2. Identificación del riesgo, corresponde al análisis de todos los factores para identificar los riesgos, se consideran las siguientes fases:

2.1 Análisis de los objetivos estratégicos y de los procesos
2.2 Identificación de los puntos de riesgos,
2.3 Identificación de áreas de impacto
2.4 Identificación de áreas de factores de riesgo
2.5 Descripción del riesgo
2.6 Clasificación del riesgo

Paso 3. Valoración del riesgo, consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto. Se desarrolla en las siguientes fases:

3.1 Análisis de riesgos,
3.2 Evaluación de riesgos
3.3 Estrategias para combatir el riesgo
3.4 Herramientas para la gestión del riesgo
3.5 Monitoreo y revisión.

3.2 Contexto:

Para la comprensión del contexto estratégico es importante considerar las situaciones externas e internas que puedan impactar el cumplimiento de la misión, los objetivos institucionales y los procesos.

El contexto se estableció utilizando la metodología PESTAL, donde se analizaron los factores: político, económico, social, tecnológico, ambiental y legal para establecer el

contexto externo. Se analizaron las capacidades de cada proceso: capacidad directiva, capacidad tecnológica, capacidad del talento humano, capacidad competitiva, capacidad financiera, cultura y comunicación organizacional para establecer el contexto interno. De igual manera el contexto del proceso, donde se analizó el objetivo, alcance, requisitos, interrelación con otros procesos, normatividad y procedimientos asociados.

El contexto debe ser revisado mínimo una vez al año o de acuerdo con los cambios en los factores internos o externos que afecten la Institución.

3.3 Responsabilidades por Línea de Defensa:

Una adecuada administración del riesgo implica la participación de todas las instancias de la Institución, en este sentido, se presenta en la tabla 1. Responsabilidades frente a los riesgos, tomando como referente su relación con las líneas de defensa[26]:

3.3.1 Línea Estratégica:

- Alta Dirección (Consejo Directivo, Rector, Secretario General, Vicerrectores)
- Comité Institucional de Coordinación de Control Interno

3.3.2 Primera Línea de Defensa:

- Los decanos de facultad,
- Los directores de la Institución,
- Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la Institución).

3.3.3 Segunda Línea de Defensa:

- Jefes de Planeación o quienes hagan sus veces
- Coordinadores de equipos de trabajo
- Comités de riesgos (donde existan)
- Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación.

3.3.4 Tercera Línea de Defensa:

Jefe de Control interno o quien haga sus veces.

Tabla 1. Responsabilidades frente a los riesgos por Líneas de Defensa

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta Dirección (Consejo	• "Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los Planes Estratégicos, así como definir el marco general para la gestión del riesgo (Política de Administración del

[26]Resolución 090 de abril de abril 29 de 2020 Por Medio de la cual se establece la conformación de las líneas de defensa al interior de la Institución Universitaria Colegio Mayor de Antioquia, y se asignan responsabilidades a las mismas, de acuerdo con el Modelo Estándar de Control Interno - MECI.

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
	Directivo, Rector, Secretario General, Vicerrectores) y Comité Institucional de Coordinación de Control Interno - CICCI	Riesgo) y el cumplimiento de los planes de la entidad."[27]. • Hacer seguimiento de manera periódica a los riesgos institucionales. • Analizar los cambios tanto en el contexto interno como externo, que puedan tener un impacto significativo en la operación de la Institución y que puedan generar cambios en la estructura de riesgos y controles. • Informar al Comité Institucional de Gestión y Desempeño sobre los ajustes que deban hacerse frente a la Administración del Riesgo. • "Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes".[28]
Primera Línea	Los decanos de facultad, Los directores de la Institución, Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la Institución)	• "La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos." [29] • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • "Mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día

[27] Idem anterior
[28] Idem anterior
[29] Idem anterior

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
		a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol".[30] • Informar a la segunda línea sobre los riesgos materializados en los procesos. Así mismo establecer los planes de acción de los riesgos materializados, con el objetivo de que se tomen las medidas oportunas, y eficaces para evitar en lo posible la repetición del evento. • Realizar seguimiento a los planes de acción implementados para los riesgos materializados.
Segunda Línea	Jefes de Planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo. Comités de riesgos (donde existan). Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación	• Asegurar que los controles y procesos de gestión del riesgo de la Primera Línea de Defensa sean apropiados, funcionen correctamente y supervisan la implementación de prácticas de gestión de riesgo eficaces. • "Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos".[31] • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. • Acompañar técnicamente a los líderes de los procesos en la identificación, análisis, valoración, implementación y mantenimiento de los riesgos asociados a sus procesos, programas, planes y proyectos. • Suministrar los resultados del análisis de los avances de la administración del riesgo en la Institución. • Presentar informe de la gestión de los riesgos institucionales y eficacia de los controles ante el Comité Institucional de Coordinación de Control Interno y el Comité Institucional de Gestión y Desempeño.
Tercera	Jefe de Control	• "Liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes

[30] Ídem anterior
[31] Ídem anterior

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Línea	interno o quien haga sus veces.	externos de control y el de evaluación y seguimiento."[32] • "Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo."[33] • "Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos."[34] • "Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos."[35] • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

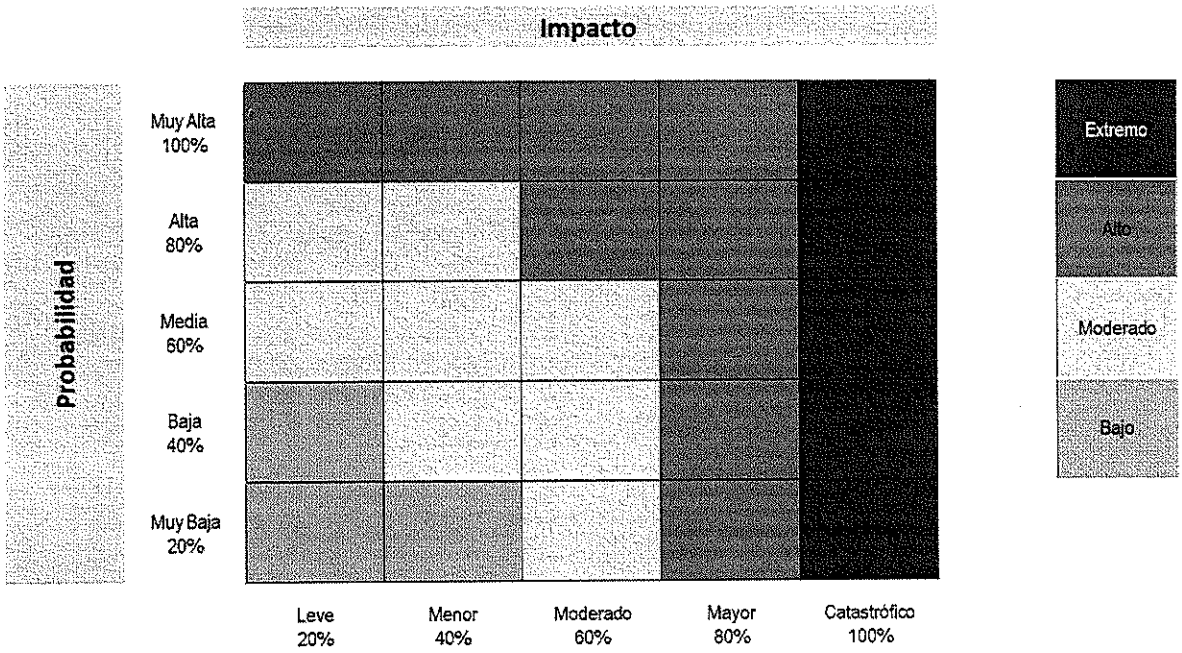
3.4 Niveles de Aceptación del Riesgo

3.4.1 Riesgos de Gestión y Seguridad de la información

Una vez se evalúa la probabilidad de ocurrencia y el impacto que tendría en el cumplimiento de los objetivos, se determina el nivel de severidad del riesgo. Se definen cuatro (4) niveles de severidad en la matriz de calor (ver figura 1).

Figura 1. Matriz de calor - Niveles de severidad del riesgo

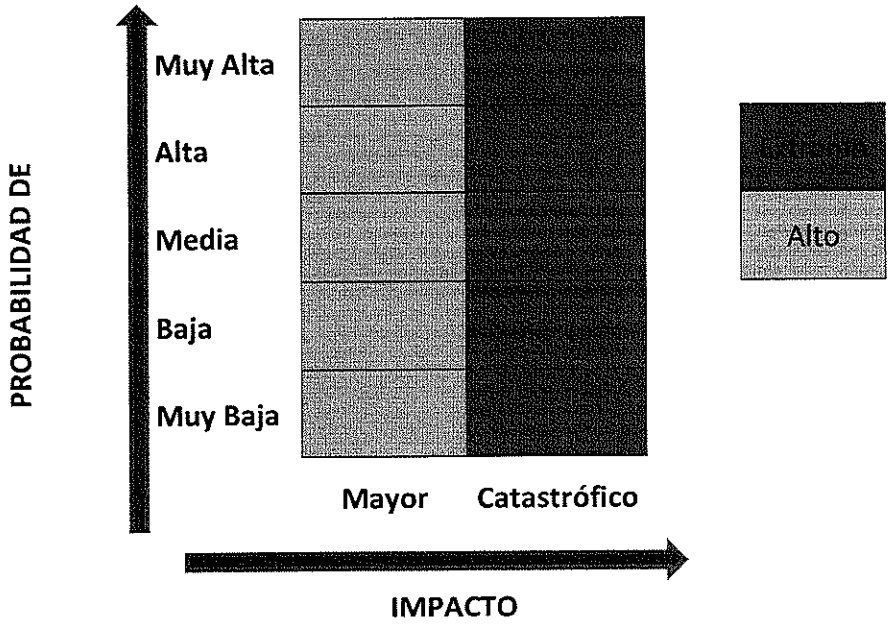
[32] Ídem anterior
[33] Ídem anterior
[34] Ídem anterior
[35] Ídem anterior



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 5. Página 42

3.4.2 Riesgos de Corrupción

Para los riesgos de corrupción se definen solo dos niveles de severidad, Alto y Extremo, como se muestra a continuación:



La tabla 2. Niveles de aceptación del riesgo, determina la estrategia o la decisión que se debe tomar frente a un determinado nivel de riesgo, después de la aplicación de controles (riesgo residual). Las estrategias para abordar los riesgos se definen como:

ACEPTAR: después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización. Para los riesgos de corrupción no aplica esta estrategia.

EVITAR: después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

REDUCIR (MITIGAR): después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel del riesgo. No necesariamente es un control adicional.

REDUCIR (TRANSFERIR): después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Tabla 2. Niveles de aceptación del riesgo y estrategias para abordarlo

Tipo de Riesgo	Nivel de Riesgo	Nivel de Aceptación
Riesgos de Gestión	Bajo	**ACEPTAR** el riesgo. Se administra por medio de las actividades propias del proceso a cargo de cada líder. Se debe realizar seguimiento tres veces al año.
	Moderado	**ACEPTAR** el riesgo. Se administra por medio de las actividades propias del proceso a cargo de cada líder. Se debe realizar seguimiento tres veces al año.
	Alto	**REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) o EVITAR** el riesgo. El líder del proceso debe implementar un plan de acción a mediano plazo. Se debe realizar seguimiento tres veces al año.
		REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) o EVITAR el riesgo. El líder del proceso debe implementar un plan de acción a corto plazo. Se debe realizar seguimiento tres veces al año.
Riesgos de Corrupción	Alto	**EVITAR, REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) el** riesgo, pero no se puede transferir su responsabilidad. Los líderes de proceso y equipo de trabajo deben realizar seguimiento permanente y enviar esta información en los meses de abril, agosto y diciembre a la segunda línea de defensa.

Tipo de Riesgo	Nivel de Riesgo	Nivel de Aceptación
		EVITAR, REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) el riesgo, pero no se puede transferir su responsabilidad. Los líderes de proceso y equipo de trabajo deben realizar seguimiento permanente, implementar plan de acción a corto plazo y enviar la información del seguimiento en los meses de abril, agosto y diciembre a la segunda línea de defensa.
Riesgos de Seguridad de la información	Bajo	**ACEPTAR** el riesgo. Se administra por medio de las actividades propias del proceso a cargo de cada líder. Se debe realizar seguimiento tres veces al año.
	Moderado	**ACEPTAR** el riesgo. Se administra por medio de las actividades propias del proceso a cargo de cada líder. Se debe realizar seguimiento tres veces al año.
	Alto	**REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) o EVITAR** el riesgo. El líder del proceso debe implementar un plan de acción a mediano plazo. Se debe realizar seguimiento tres veces al año.
		REDUCIR (MITIGAR), REDUCIR (TRANSFERIR) o EVITAR el riesgo. El líder del proceso debe implementar un plan de acción a corto plazo. Se debe realizar seguimiento tres veces al año.

3.5 Criterios para definir la probabilidad

La probabilidad se entiende como la posibilidad de ocurrencia del riesgo y corresponde al número de veces que se pasa por el punto de riesgo en el período de un (1) año. En la tabla 3 se establecen los criterios para definir el nivel de probabilidad para los Riesgos de Gestión, Riesgos de Corrupción y los Riesgos de Seguridad de la información.

Tabla 3. Criterios para definir el nivel de probabilidad

NIVEL	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%

[illegible]	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas pág. 39

3.6 Criterios para definir el nivel de Impacto

Para determinar el impacto se definen dos grandes grupos: el impacto económico y el impacto reputacional. En la tabla 4 se establecen los criterios para definir el impacto en los Riesgos de Gestión y de Seguridad de la información:

Tabla 4. Criterios para definir el nivel de impacto en los Riesgos de Gestión y Seguridad de la información.

NIVEL	AFECTACIÓN ECONÓMICA	REPUTACIONAL
Leve 20%	Afectación menor a 10 SMMLV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMMLV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMMLV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMMLV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
[illegible]	Mayor a 500 SMMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas pags.40.

Para determinar el impacto frente a la posible materialización de los riesgos de corrupción se debe dar respuesta al siguiente cuestionario, ver la tabla 5:

Tabla 5. Criterios para calificar el impacto en los Riesgos de Corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría...	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		

8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNO A DIEZ preguntas genera un impacto MAYOR. Responder afirmativamente de ONCE A DIECINUEVE preguntas genera un impacto CATASTROFICO.			

MAYOR	Genera altas consecuencias sobre la entidad
CATASTROFICO	Genera consecuencias desastrosas para la entidad

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas. Pág. 72

4. Acciones a seguir en caso de materialización de un riesgo

Tabla 6. Acciones a seguir en caso de materialización de un riesgo

Tipo de riesgo	Responsable	Acción a realizar
Riesgos de Gestión (Zonas Moderada, Alta y Extrema)	**Línea Estratégica** (Alta Dirección (Consejo Directivo, Rector, Secretario General, Vicerrectores) y Comité Institucional de Coordinación de Control Interno).	Revisar las acciones correctivas implementadas y/o Plan de mejoramiento implementado.
	Primera Línea de Defensa	Informar a Planeación Institucional sobre el hallazgo o riesgo materializado y las acciones tomadas.

	(Los decanos de facultad, Los Directores de la Institución, Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la Institución)).	Iniciar el análisis de causas, determinar acciones correctivas y replantear los controles asociados al riesgo.
		Analizar y actualizar el mapa de riesgos.
		Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso).
	Segunda Línea de Defensa (Jefes de Planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo. Comités de riesgos (donde existan). Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación.	Informar al líder del proceso sobre el hallazgo o riesgo materializado, en caso de que no haya sido reportado.
		Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para mitigar el riesgo.
		Verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
		Verificar que se hayan tomado las acciones correspondientes y que se actualice el mapa de riesgos.
		Informar a la tercera línea de defensa con el objetivo de realizar el respectivo seguimiento al plan de mejoramiento y mapa de riesgos.
	Tercera Línea de Defensa (Jefe de Control interno o quien haga sus veces)	Verificar si se tomaron las acciones y se actualizó el mapa de riesgos.
		Realizar evaluación independiente.

Tipo de riesgo	Responsable	Acción a realizar
Riesgos de Gestión (Zona Baja)	**Primera Línea de Defensa** (Los decanos de facultad, Los Directores de la Institución, Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la Institución)).	Informar a Planeación Institucional sobre el hallazgo o riesgo materializado.
		Realizar análisis de causas y determinar acciones correctivas y replantear los controles asociados al riesgo.
		Analizar y actualizar el mapa de riesgos.

Tipo de riesgo	Responsable	Acción a realizar
	Segunda Línea de Defensa (Jefes de Planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo. Comités de riesgos (donde existan). Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación.	Informar al líder del proceso sobre el hallazgo o riesgo materializado, en caso de que este no haya sido reportado.
		Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para mitigar el impacto.
		Verificar la calificación y ubicación del riesgo para su modificación en el mapa de riesgos.
		Verificar que se hayan tomado las acciones correspondientes y que se actualice el mapa de riesgos.
		Informar a la tercera línea de defensa con el objetivo de realizar el respectivo seguimiento al plan de mejoramiento y mapa de riesgos.
	Tercera Línea de Defensa (Jefe de Control interno o quien haga sus veces)	Verificar si se tomaron las acciones y se actualizó el mapa de riesgos.
		Realizar evaluación independiente.

Tipo de riesgo	Responsable	Acción a realizar
Riesgos de Corrupción	**Línea Estratégica** (Alta Dirección (Consejo Directivo, Rector, Secretario General, Vicerrectores) y Comité Institucional de Coordinación de Control Interno).	Revisar las acciones correctivas implementadas y/o Plan de mejoramiento implementado.
	Primera Línea de Defensa (Los decanos de facultad, Los Directores de la Institución, Líderes de programas, procesos y proyectos y de sus	Informar a Planeación Institucional sobre el riesgo materializado.
		Iniciar el análisis de causas, determinar acciones correctivas y replantear los controles asociados al riesgo.
		Actualizar el mapa de riesgos de corrupción, en particular las causas, riesgos y controles.

	equipos de trabajo (en general servidores públicos en todos los niveles de la Institución)).	Una vez surtido el conducto regular establecido por la Institución y dependiendo del alcance (normatividad asociada al riesgo de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente (Procuraduría, Personería, Secretaría General).
	Segunda Línea de Defensa (Jefes de Planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo. Comités de riesgos (donde existan). Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación.	Informar al Líder del proceso, (en caso de que no haya sido reportado) quien analizará la situación y definirá las acciones a que haya lugar.
		Apoyar al líder del proceso en el análisis de las causas de la materialización del riesgo y definición de planes de acción o acciones correctivas.
		Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.
		Informar a la tercera línea de defensa con el objetivo de realizar el respectivo seguimiento al plan de mejoramiento y mapa de riesgos.
	Tercera Línea de Defensa (Jefe de Control interno o quien haga sus veces)	Acciones encaminadas a determinar la efectividad de los controles.
		Acciones encaminadas a mejorar la valoración de los riesgos.
		Acciones encaminadas a mejorar los controles.
		Analizar el diseño e idoneidad de los controles, si son adecuados para prevenir o mitigar los riesgos de corrupción.
		Determinar si se adelantaron acciones de monitoreo.
		Revisar las acciones del monitoreo.

Tipo de riesgo	Responsable	Acción a realizar
Riesgos de Seguridad de la Información	**Línea Estratégica** (Alta Dirección (Consejo Directivo, Rector, Secretario General, Vicerrectores) y Comité Institucional de Coordinación de Control Interno).	Revisar las acciones correctivas implementadas y/o Plan de mejoramiento implementado.

Primera Línea de Defensa (Los decanos de facultad, Los Directores de la Institución, Líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la Institución)).	Informar a Planeación Institucional y al responsable de la seguridad de la información sobre el hallazgo o riesgo materializado y las acciones tomadas.
	Iniciar el análisis de causas y determinar acciones correctivas y replantear los controles asociados al riesgo.
	Analizar y actualizar el mapa de riesgos.
	Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso).
Segunda Línea de Defensa y responsable de la Seguridad de la Información (Jefes de Planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo. Comités de riesgos (donde existan). Comité de contratación. Áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación.	Informar al líder del proceso sobre la materialización del riesgo, en caso de que no haya sido reportado.
	Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para mitigar el impacto.
	Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.
	Informar a la tercera línea de defensa con el objetivo de realizar el respectivo seguimiento al plan de mejoramiento y mapa de riesgos.
Tercera Línea de Defensa (Jefe de Control interno o quien haga sus veces)	Verificar si se tomaron las acciones y se actualizó el mapa de riesgos.
	Realizar evaluación independiente.

5. Periodicidad del seguimiento

La Línea Estratégica, debe realizar seguimiento una vez al año sobre el perfil del riesgo residual y los planes de mejoramiento implementados en caso de materialización del riesgo, incluyendo los riesgos estratégicos, de gestión, corrupción y seguridad de la información.

La Primera Línea de Defensa, junto con su equipo de trabajo deben realizar monitoreo y evaluación permanente a la gestión de riesgos de corrupción y si es el caso ajustarla y enviar en los meses de abril, agosto y diciembre, la información del monitoreo realizado a la segunda

línea de defensa.
Para los riesgos de gestión se establece que cada líder debe realizar seguimiento tres veces al año, en los meses de abril, agosto y diciembre y enviar la información a la segunda línea de defensa. Este seguimiento debe obedecer a lo expresado en el numeral 3.3 Responsabilidades por línea de defensa.

La Segunda Línea de Defensa debe consolidar los informes enviados por la primera línea de defensa y presentar dos veces al año un informe sobre la gestión de los riesgos y el análisis de los eventos y riesgos críticos a la alta dirección.

La Oficina de Control Interno – **Tercera Línea de Defensa** - en su rol de Evaluador de la Gestión del Riesgo, realizará seguimiento cada cuatro meses al Plan Anticorrupción y de Atención al Ciudadano - PAAC, conforme a las disposiciones establecidas por el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia, atendiendo a la normatividad aplicable. Los resultados de tales seguimientos serán publicados en la página web de la Institución.

Según las "Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano" se define los siguientes cortes de seguimiento a los riegos de corrupción:

- **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- **Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

6. Comunicación y Consulta

La Institución promoverá diferentes canales de comunicación que permitan que la comunidad institucional, conozca la Política y los Mapas de Riesgos. Así mismo, cada líder deberá promover acciones de participación de los diferentes equipos de trabajo para la identificación, análisis y valoración del riesgo, esta participación permitirá la adecuada identificación, para garantizar que se toman en consideración los diferentes puntos de vista.

De igual forma, se promoverán espacios de socialización y capacitación para la adecuada aplicación de la metodología para la administración del riesgo a cargo de Planeación Institucional.

Los Mapas de Riesgos serán consolidados y publicados por Planeación Institucional en la página web de la Institución para cada vigencia.

7. Revisión de la Política de Administración del Riesgo

La Política para la Administración del Riesgo, debe ser revisada periódicamente, mínimo una vez al año, o, cada vez que se requiera ante cambios estructurales, operacionales y/o normativos con el fin de verificar que esté alineada con los objetivos estratégicos de la Institución, los niveles de responsabilidad frente al manejo de los riesgos y los niveles para calificar el impacto y asegurar que se ajuste a las necesidades de la institución.