



**UNIVERSIDAD
DE ANTIOQUIA**
1 8 0 3

MANUAL PARA LA GESTIÓN INTEGRAL DE RIESGOS

**DIRECCIÓN DE PLANEACIÓN Y DESARROLLO
INSTITUCIONAL
DIVISIÓN DE ARQUITECTURA DE PROCESOS**

**CÓDIGO: DI-AP-MA-07
VERSIÓN: 03 / 01-FEB-2019**

Contenido

1.	Introducción	4
2.	Definición	5
3.	Lineamientos generales.....	5
4.	Contenido	6
4.1.	Generalidades de la gestión de riesgos	6
4.2.	Bases para la gestión integral de riesgos	9
4.3.	Política para la gestión integral de riesgos	9
4.4.	Objetivos de la gestión integral de riesgos	10
4.5.	Principios de la gestión de riesgos	10
4.6.	Compromisos Institucionales frente a la gestión de riesgos	11
4.7.	Estructura de responsabilidad para la gestión de riesgos	11
4.8.	Marco de referencia para la gestión de riesgos.....	12
4.8.1.	Dirección y compromiso	13
4.8.2.	Diseño del marco de referencia para la gestión de riesgos.....	13
4.8.3.	Implementación de la gestión de riesgos.....	14
4.8.4.	Monitoreo del Marco de Referencia	16
4.8.5.	Mejora continua del Marco de Referencia	16
4.9.	Responsables de la gestión de riesgos	16
4.9.1.	Línea estratégica.....	17
4.9.2.	Primera línea de defensa	18
4.9.3.	Segunda línea de defensa	19
4.9.4.	Tercera línea de defensa	19
4.10.	Proceso de gestión de riesgos.....	19
4.10.1.	Establecimiento del contexto	20
4.10.2.	Valoración del riesgo.....	22
4.10.3.	Tratamiento de los riesgos.....	29
4.10.4.	Comunicación y consulta	36
4.10.5.	Monitoreo y revisión	36
4.11.	Gestión de riesgos de corrupción	37
4.11.1.	Política de Administración del Riesgo de Corrupción	38
4.11.2.	Construcción de Mapa de Riesgos de Corrupción	38
4.11.3.	Consulta y Divulgación.....	43
4.11.4.	Monitoreo y Revisión.....	43
4.11.5.	Seguimiento	43

5.	Documentos de referencia.....	44
6.	Glosario.....	44
6.1.	Definiciones generales.....	45
6.2.	Definiciones relacionadas con la gestión de riesgos.....	45
7.	Anotaciones y comentarios	46
8.	Notas de cambio.....	47
9.	Bibliografía.....	47

Ilustraciones

Ilustración 1. Estructura del Modelo Estándar de Control Interno - MECI.....	4
Ilustración 2. Componentes de la Gestión de Riesgos	7
Ilustración 3. Marco de Referencia para la Gestión de Riesgos	12
Ilustración 4. Niveles de Madurez de la Gestión de Riesgos.....	15
Ilustración 5. Responsables de la Gestión de Riesgos.....	17
Ilustración 6. Proceso para la Gestión de Riesgos.....	20
Ilustración 7. Categorías de Riesgos.....	23
Ilustración 8. Estructura de los Riesgos	24
Ilustración 9. Niveles de Criticidad de los Riesgos y su Marco Temporal para el Tratamiento	29
Ilustración 10. Aplicación de los Controles en los Riesgos	35
Ilustración 11. Elementos del Plan de Tratamiento de los Riesgos.....	36
Ilustración 12. Monitoreo y Revisión de los Riesgos.....	37
Ilustración 13. Ciclo de Mejora Continua para la Gestión de Riesgos de Corrupción	38
Ilustración 14. Secuencia para la Construcción del Mapa de Riesgos de Corrupción	39

Tablas

Tabla 1. Criterios de referencia para analizar la probabilidad	25
Tabla 2. Criterios de referencia para analizar los impactos	26
Tabla 3. Matriz Calificación de Riesgos	27
Tabla 4. Matriz Evaluación de Riesgos (Zonas de Criticidad)	28
Tabla 5. Matriz de Medidas de Tratamiento recomendadas de acuerdo al nivel del riesgo.....	33
Tabla 6. Valores para los impactos de los Riesgos de Corrupción	40
Tabla 7. Cuestionario para la calificación de los impactos de los Riesgos de Corrupción.....	40
Tabla 8. Matriz para determinar el Grado de Criticidad de los Riesgos de Corrupción.....	41

MANUAL PARA LA GESTIÓN INTEGRAL DE RIESGOS

1. Introducción

Debido a la globalización y a cambios en los factores externos, en las organizaciones se deben realizar ajustes a los planes, proyectos o procesos que éstas desarrollan, lo cual agrega gran incertidumbre sobre el cumplimiento de sus objetivos y les genera grandes riesgos.

La gestión de riesgos se ha convertido en un proceso crucial al momento de establecer la planeación estratégica y los planes de desarrollo, ejecutar un proceso, desarrollar un proyecto o evaluar la gestión; se ha entendido que la gestión de riesgos hace parte fundamental del ciclo administrativo y de control de cualquier institución.

En este sentido, el Sistema de Control Interno de las Entidades Públicas, definido a través del Modelo Estándar de Control Interno (MECI)¹, establece que la administración de riesgos es uno de sus componentes principales, en donde se busca asegurar, de una manera razonable, que la planeación y su ejecución, tendrán los controles necesarios.

Ilustración 1. Estructura del Modelo Estándar de Control Interno - MECI



Fuente: Elaboración propia adaptada de la norma INTOSAI GOV 9100

¹ El MECI proporciona una estructura de control de la gestión que especifica los elementos necesarios para construir y fortalecer el Sistema de Control Interno.

Dado lo anterior se hace necesario que la Universidad de Antioquia cuente con un proceso de Gestión de Riesgos robusto y bien estructurado que apoye las operaciones y brinde información valiosa para la planeación y la toma de decisiones.

2. Definición

El presente Manual tiene como objetivo describir el proceso de gestión de riesgos de la Universidad de Antioquia, sus objetivos, alcances, principios, políticas, su operación, y demás elementos cruciales para el desarrollo del mismo.

La premisa fundamental de la gestión de riesgos es que todas las entidades públicas existen para proporcionar valor a la sociedad, al tiempo que enfrentan una gran incertidumbre en el logro de sus objetivos. El reto de las administraciones es el de determinar cuánta incertidumbre se puede aceptar (riesgos y oportunidades). El objetivo de la gestión de riesgos es el de permitir a la administración el tratamiento efectivo de la incertidumbre y sus riesgos/oportunidades asociadas².

La gestión de riesgos es un proceso dinámico e interactivo que le permite a la institución identificar, evaluar y gestionar aquellos eventos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales. Su mirada sistémica contribuye a que la institución no solo asegure su gestión, sino que fortalezca el ejercicio del control interno como entidad pública³. Es un proceso basado en un enfoque integral y continuo que incluye el entendimiento de las interdependencias entre los diferentes riesgos para definir estrategias que contribuyan al logro de los objetivos de la entidad.

3. Lineamientos generales

- Desarrollar un Plan anual para la Gestión Integral de Riesgos que siga el modelo de madurez definido en el presente manual. Dicho Plan deberá estar alineado con el Plan Anticorrupción y de Atención al Ciudadano.
- Se generan tres reportes de avance al año (cada cuatro meses) los cuales se definen en el Plan Anticorrupción y de Atención al Ciudadano.
- La gestión de riesgos es responsabilidad de cada uno de los líderes de los procesos
- La División de Arquitectura de Procesos acompañará y orientará a cada una de las dependencias en su gestión.

² INTOSAI. INTOSAI GOV 9130. Guía para las Normas de Control Interno del Sector Público - Información Adicional sobre la Administración de Riesgos de la Entidad. Viena, 2016.

³ Departamento Administrativo de la Función Pública. Sistema de Gestión MIPG – Marco General. Bogotá, 2017.

- Las dependencias asignarán un funcionario para el desarrollo e implementación de la metodología de riesgos; éste será el enlace entre la División de Arquitectura de Procesos y las dependencias.

4. Contenido

4.1. Generalidades de la gestión de riesgos

Como se mencionó anteriormente, el objetivo de la gestión de riesgos es permitir a la administración el tratamiento efectivo de la incertidumbre y sus riesgos/oportunidades asociadas. Se desarrolla como un conjunto de acciones llevadas a cabo de forma estructurada e integral, que permite a la institución identificar y evaluar los riesgos que pueden afectar el cumplimiento de sus objetivos, con el fin de emprender de forma efectiva las medidas necesarias para responder a ellos.

En muchos aspectos, la gestión de riesgos de una institución puede ser vista como una evolución del modelo de control interno. El marco del sistema de control interno involucra la gestión de riesgos (ver Ilustración 1), generando así un sistema más robusto para la toma de decisiones respecto a posibles desvíos de la misión y objetivos de la institución⁴.

El punto de partida para la gestión de riesgos es la misión y visión. En el contexto de la misión, las directivas de la institución establecen los objetivos y las estrategias para alcanzarlos.

Una vez definidos los objetivos, la gestión de riesgos de la institución requiere la identificación de eventos que podrían tener algún impacto⁵ en el logro de dichos objetivos. Los eventos con impacto negativo representan riesgos que podrían dificultar el logro de los objetivos. Los eventos con impactos positivos representan oportunidades de forma tal que permitan a la institución el logro de sus objetivos de forma más eficiente. La gestión de riesgos permite que la institución formule planes tanto para aprovechar las oportunidades como para protegerse de los riesgos.

La gestión de riesgos consta de ocho componentes interrelacionados los cuales deben ser aplicados en todos los alcances de las actividades de todos los niveles de la institución, incluyendo nuevas iniciativas y proyectos (ver Ilustración 2).

⁴ INTOSAI. INTOSAI GOV 9130. Guía para las Normas de Control Interno del Sector Público - Información Adicional sobre la Administración de Riesgos de la Entidad. Viena, 2016.

⁵ Los eventos pueden tener impactos positivos, negativos o ambos a la vez.

Ilustración 2. Componentes de la Gestión de Riesgos



Fuente: Elaboración propia adaptada de la norma INTOSAI GOV 9130

LA GESTIÓN DE RIESGOS Y EL CONTROL INTERNO

De acuerdo a la Ley 87 de 1993 el Control Interno se define como un sistema integrado por el esquema de la organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

El Control Interno se desarrolla a través del Modelo Estándar de Control Interno – MECI, el cual fue actualizado a través del Marco General del MIPG. El control interno de una entidad se conforma por cinco componentes interrelacionados (ver Ilustración 1).

- Ambiente de control
- Gestión de riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

El entorno de control es la base para el control interno en conjunto, aquí se disponen las condiciones mínimas requeridas para el ejercicio de control interno. Está diseñado para brindar un nivel de certeza razonable sobre el logro de los objetivos institucionales, por lo que una definición de objetivos y metas claras es fundamental.

Una vez se establecen los objetivos y se conforma un entorno de control efectivo, la gestión de los riesgos a los cuales se enfrenta la institución en el desarrollo de su misión y logro de sus objetivos, determina la forma apropiada para responder ante ellos.

La mejor forma para responder a los riesgos es a través de actividades de control (diseño y evaluación de controles). La información y comunicación efectiva son vitales para que la institución ejecute y controle sus actividades. La dirección requiere de información y comunicación relevante, confiable, correcta y oportuna relacionada con los eventos internos y externos.

Finalmente, el control interno es una actividad dinámica que debe ser adaptada continuamente de acuerdo a los cambios y riesgos que la institución enfrenta. El monitoreo al sistema de control es necesario para asegurar que el sistema esté alineado con los objetivos, el entorno, los recursos y los riesgos.

La premisa fundamental de la gestión de riesgos en la Universidad de Antioquia es que, en el desarrollo de sus objetivos misionales fundamentales, la Universidad se enfrenta a la incertidumbre y el gran desafío para las directivas de la institución es determinar cuánta incertidumbre están dispuestas a aceptar a medida que buscan el logro de tales objetivos.

Las capacidades inherentes a la gestión de riesgos le permiten a la dirección obtener una mejor gestión y lograr sus objetivos, así como prevenir la pérdida de recursos. La gestión de riesgos ayuda a cumplir efectivamente con los reportes y el cumplimiento de normas y prever el daño reputacional y las consecuencias asociadas. En resumen, la gestión de riesgos la ayuda a la institución a llegar donde quiere llegar evitando errores y sorpresas en el camino.

El control interno es un proceso integral desarrollado por todo el personal de la institución, incluyendo las directivas, diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que, en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos de la administración:

- Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones.
- Cumplimiento de las obligaciones de responsabilidad.
- Cumplimiento de las leyes y regulaciones aplicables.
- Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.

El control interno es un proceso integral dinámico que se adapta constantemente a los cambios que enfrenta la organización. La gerencia y el personal de todo nivel tienen que estar involucrados en este proceso para enfrentarse a los riesgos y para dar seguridad razonable del logro de la misión de la institución y de los objetivos generales.

4.2. Bases para la gestión integral de riesgos

La Universidad de Antioquia, con fundamento en su autonomía, define los siguientes lineamientos como bases para el desarrollo de la gestión integral de riesgos en la institución:

- Se considera riesgo como la posibilidad de que ocurra un evento que tendrá un impacto sobre los objetivos institucionales, la continuidad de sus operaciones, las personas, el medio ambiente y los recursos públicos.
- La gestión integral de riesgos es un instrumento para prevenir situaciones que puedan afectar el cumplimiento de la misión Universitaria en todos sus ámbitos de aplicación o mitigar los efectos negativos en caso de haberse materializado.
La política de gestión integral de riesgos será transversal a todos los procesos y de interés prioritario.
- Las decisiones asociadas con la gestión integral de riesgos darán prioridad a la protección de los miembros de la comunidad Universitaria y a los propósitos institucionales.
- La gestión integral de riesgos, se desarrollará en concordancia con la política y normatividad nacional e internacional que sobre esta temática sea aplicable a la Universidad en el marco de su autonomía.
- La gestión integral de riesgos se implementa de manera permanente, sistemática y homologada, bajo la estructura organizacional definida por la Universidad en el marco de su Sistema de Gestión Institucional.
- La orientación de la gestión integral de riesgos será responsabilidad de los órganos de gobierno universitario en el ámbito de su competencia y su aplicación, será responsabilidad de los demás servidores públicos en las actividades de docencia, investigación, extensión y administrativas.

4.3. Política para la gestión integral de riesgos

Mediante el Acuerdo Superior 453 del 29 de octubre de 2018, se establece la Política de Gestión Integral de Riesgos de la Universidad de Antioquia: *“La Universidad de Antioquia se compromete a gestionar de manera integral los riesgos institucionales y a emprender las acciones necesarias para proporcionar una seguridad razonable en el cumplimiento de su misión y en procura de la sostenibilidad, el desarrollo y el bien común”*.

4.4. Objetivos de la gestión integral de riesgos

El principal objetivo de la gestión de riesgos es maximizar las oportunidades y minimizar las pérdidas asociadas a los riesgos, busca un equilibrio entre riesgo y oportunidad, de acuerdo con la tolerancia al riesgo de la institución.

Algunos objetivos secundarios que se logran con la gestión de riesgos, son:

- Preservar la continuidad de la operación de la institución evitando pérdidas catastróficas, afectación a su imagen o sus planes de desarrollo.
- Facilitar, en caso de un siniestro, la recuperación de las actividades a través del establecimiento de planes de emergencia y contingencia.
- Proteger a los empleados y a quienes desarrollen actividades en la Universidad, contra accidentes que pueden causar lesiones, daños serios o muerte.
- Evitar que las operaciones de la institución produzcan daños al ambiente y que perjudiquen o resulten nocivas a la salud y el bienestar humano.
- Emplear eficiente y eficazmente los recursos humanos, físicos y financieros de la institución para el cumplimiento de sus objetivos.
- Utilizar eficientemente los recursos de la institución, buscando mejorar la efectividad, reducir sobrecostos y evitando pérdidas.
- Prevenir o mitigar cualquier pérdida económica que se puedan generar debido a la materialización de riesgos, disminuyendo el grado de inseguridad de las operaciones de la institución hasta lograr límites tolerables e implementando controles adecuados para prevenir las desviaciones en los objetivos previstos.
- Garantizar la calidad, disponibilidad y seguridad de la información necesaria en la institución para la administración y control de sus actividades.
- Lograr que las actividades de la institución se realicen dentro de las normas internas y externas que la rigen.
- Preservar el buen nombre y las relaciones de la institución con los diferentes públicos de interés que atienden y están interesados en su función, generando confianza y credibilidad en su manejo.

4.5. Principios de la gestión de riesgos

Para que la gestión de riesgos sea eficaz, la Universidad deberá cumplir con cada uno de los siguientes principios:

- a. La gestión de riesgos genera y cuida el valor de la institución.
- b. La gestión de riesgos es una parte integral de cada uno de los procesos de la institución.
- c. La gestión de riesgos hace parte del proceso de toma de decisiones de cada unidad de la Universidad.

- d. La gestión de riesgos trata directamente con la incertidumbre.
- e. La gestión de riesgos se desarrolla de forma sistemática, ordenada y oportuna.
- f. La gestión de riesgos se basa en la mejor información disponible.
- g. La gestión de riesgos se adapta al contexto interno y externo de la Universidad.
- h. La gestión de riesgos considera los factores humanos y culturales en los cuales se desarrolla.
- i. La gestión de riesgos es transparente e inclusiva.
- j. La gestión de riesgos es dinámica y responde continuamente al cambio.
- k. La gestión de riesgos impulsa la mejora continua en la Universidad.

4.6. Compromisos Institucionales frente a la gestión de riesgos

Con el fin de garantizar una gestión de riesgos eficaz, se establecen los siguientes compromisos:

- Se realizará una identificación y valoración de los riesgos para los procesos Institucionales.
- Se establecerán medidas de control y se desarrollarán acciones de tratamiento.
- Se establecerán mecanismos de seguimiento y monitoreo periódico a la gestión de riesgos con fines de mejora.
- Se revisará periódicamente la política y el cumplimiento de los objetivos de la gestión de riesgos en el contexto Institucional y normativo aplicable.
- Se incorporará la gestión de riesgos en las instancias de gobierno como insumo fundamental para la toma de decisiones.

4.7. Estructura de responsabilidad para la gestión de riesgos

Se establece la siguiente estructura de responsabilidad para la gestión de riesgos:

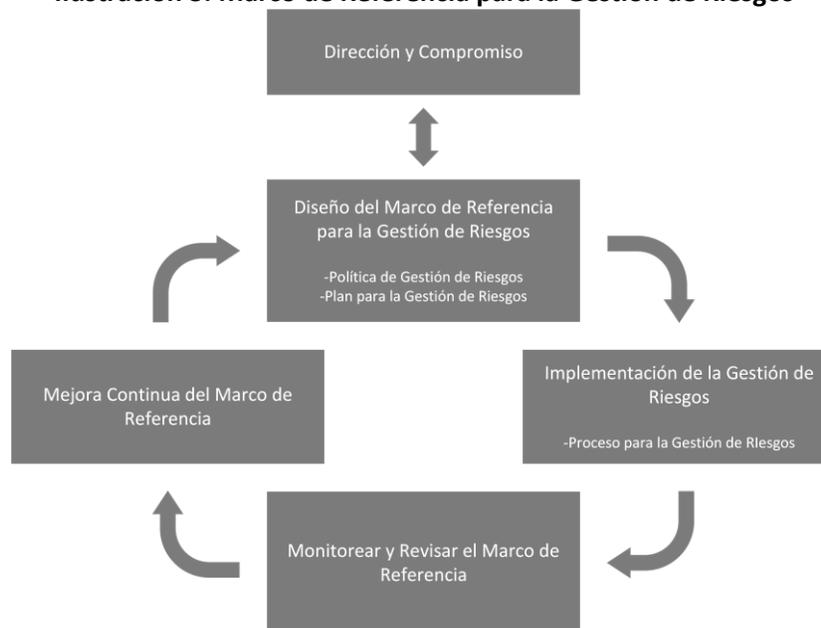
- Los Directivos y líderes de las dependencias universitarias serán responsables de dar cumplimiento a la política de gestión integral de riesgos en los procesos que lideran.
- La Dirección de Planeación y Desarrollo Institucional orientará el desarrollo metodológico para la gestión de riesgos.
- Los servidores públicos de los procesos, serán responsables del seguimiento y monitoreo permanente de los riesgos para efectos de evaluar la eficacia de los controles y advertir necesidades de fortalecimiento y mejora.
- La Oficina de Auditoría Institucional, evaluará de manera periódica e independiente la gestión integral de riesgos y advertirá cualquier necesidad de mejora.

4.8. Marco de referencia para la gestión de riesgos

Para realizar una gestión de riesgos eficaz, es necesario definir y establecer un Marco de Referencia para la Gestión de Riesgos⁶, el cual ayuda a la aplicación del proceso para la gestión de riesgos (ver Ilustración 6) en las diversas unidades y contexto específico de la Universidad. El marco garantiza que la información generada por el proceso de gestión de riesgos se reporte de manera adecuada y que ésta se utilice para la toma de decisiones y la rendición de cuentas a todos los niveles de la Universidad de Antioquia.

El Marco de Referencia está compuesto de una serie de etapas de carácter directivo (ver Ilustración 3). Su objetivo no es diseñar un nuevo sistema de gestión, sino facilitar la integración de la gestión de riesgos a los sistemas de gestión de la Universidad.

Ilustración 3. Marco de Referencia para la Gestión de Riesgos



Fuente: Elaboración propia adaptada de la norma ISO 31000

⁶ El Marco de Referencia para la Gestión de Riesgos es el conjunto de elementos que proporcionan los fundamentos y las disposiciones de la Universidad para el diseño, la implementación, el seguimiento, la revisión y la mejora continua de la gestión de riesgos en toda la institución.

4.8.1. Dirección y compromiso

Garantizar la adecuada y eficaz gestión de riesgo en la institución requiere de un compromiso fuerte y sostenido por parte de la dirección. La dirección deberá entre otros:

- Definir y aprobar los lineamientos para la gestión de riesgos.
- Fomentar una cultura de gestión de riesgos alineada a los principios y procedimientos de la organización.
- Definir indicadores de desempeño de la gestión de riesgos.
- Alinear los objetivos de la gestión de riesgos con los objetivos y estrategias de la institución.
- Garantizar la conformidad legal.
- Asignar responsabilidades en los niveles respectivos

4.8.2. Diseño del marco de referencia para la gestión de riesgos

Para el diseño continuo e implementación del marco de referencia de la gestión de riesgos es necesario evaluar y entender la organización, su contexto interno y externo, establecer la Política para la Gestión de Riesgos, conocer los mecanismos para la rendición de cuentas, cómo se integra con los demás procesos de la organización, cuáles son los recursos destinados para la gestión, y cuáles son los mecanismos establecidos para la comunicación y presentación de informes.

Contexto Normativo Externo

- Mediante la Ley 87 de 1993 se establecen las normas para el ejercicio del Control Interno en todas las entidades y organismos del Estado.
- 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
- 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.
- 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.
- El Decreto 943 de 2014 actualiza el MECI para hacerlo más comprensible y facilitar su implementación.
- El Departamento Administrativo de la Función Pública – DAFP, publica la Guía para la Administración del Riesgo, la Guía para la Gestión del Riesgo de Corrupción y la

Cartilla Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

- 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.

Contexto Normativo Interno

- La Resolución Superior 041 de 1994 autoriza al Rector para desarrollar el sistema de control interno de la Universidad, la Resolución Rectoral 4800 del mismo año lo desarrolla y el Acuerdo Superior 072 de 1996 crea la oficina de Control Interno.
- La Resolución Rectoral 27137 de 2008 diseña e implementa el Modelo Estándar de Control Interno – MECI 2005 en la Universidad de Antioquia, el cual es actualizado por la Resolución Rectoral 39562 de 2014.
- Acuerdo Superior 453 del 29 de octubre de 2018, por el cual se establece la Política de Gestión Integral de Riesgos de la Universidad de Antioquia.
- Resolución Superior 2299 del 11 de diciembre de 2018, por la cual se actualiza el Sistema de Control Interno de la Universidad de Antioquia.

4.8.3. Implementación de la gestión de riesgos

La implementación de la gestión de riesgos en la Universidad sigue el modelo establecido por la norma NTC ISO 31000 (ver Ilustración 6), adaptándolo para cumplir con los requisitos legales a los que está sometida la Universidad.

El proceso de Gestión de Riesgos se desarrollará a través de un Plan para la Gestión de Riesgos, el cual se actualizará anualmente buscando la mejora continua y estará alineado con un Modelo de Madurez para la Gestión de Riesgos, el Plan de Acción y el Plan Anticorrupción y de Atención al Ciudadano en su componente Gestión de Riesgos de Corrupción.

Modelo de Madurez para la Gestión de Riesgos

La gestión de riesgos es un proceso dinámico con una estructura, gobierno y procedimientos bien definidos. Un modelo de madurez permite que la Universidad pueda comparar su estado contra las mejores prácticas en gestión de riesgos en diferentes estados⁷.

⁷ Implementing Enterprise risk management ...

El modelo de madurez propuesto por RIMS⁸ será adaptado y adoptado para el desarrollo de la gestión de riesgos en la Universidad de Antioquia. En este modelo están definidos cinco niveles y 7 atributos de madurez por nivel (ver Ilustración 4):

Ilustración 4. Niveles de Madurez de la Gestión de Riesgos



Fuente: Elaboración propia

- i. Enfoque de la Gestión de Riesgos: Grado de compromiso de la alta dirección en la gestión de riesgos.
- ii. Gestión del Proceso de Gestión de Riesgos: Grado de la integración del proceso de gestión de riesgos en los demás procesos de la institución.
- iii. Gestión del apetito por el riesgo: Grado de entendimiento de la relación riesgo-recompensa en los procesos de la institución.
- iv. Disciplina de causas-raíz: Grado de disciplina aplicada al entendimiento de las causas-raíz de los riesgos y problemas que enfrenta la institución.
- v. Descubrimiento de riesgos y oportunidades: Grado en el que la documentación y el conocimiento organizacional se gestiona y comparte.
- vi. Desempeño: Grado de ejecución de la estrategia y los objetivos institucionales y su desviación de los planes o metas iniciales.
- vii. Resiliencia y sostenibilidad: Medida en la que el proceso de gestión de riesgos se integra en la planeación de las operaciones del día a día

⁸ The Risk Management and Insurance Society.

4.8.4. Monitoreo del Marco de Referencia

Con el fin de garantizar una gestión de riesgos eficaz, la Universidad deberá medir el desempeño de la institución y su gestión de riesgos considerando lo siguiente:

- Establecer indicadores y metas, y medir su desempeño periódicamente.
- Medir el progreso del Plan para la Gestión de Riesgos y sus desviaciones.
- Revisar periódicamente si el Marco de Referencia, la Política y el Plan para la Gestión de Riesgos siguen siendo adecuados y requieren actualizarse de acuerdo al contexto.
- Presentar informes sobre los riesgos, el progreso del Plan y sobre el cumplimiento de la Política.

4.8.5. Mejora continua del Marco de Referencia

Con base en los resultados del monitoreo y revisión se deberán tomar decisiones sobre la forma cómo se podrá mejorar el Marco de Referencia, la Política y el Plan para la Gestión de Riesgos.

4.9. Responsables de la gestión de riesgos

Dada la importancia de la gestión de riesgos, se requiere un esfuerzo conjunto y coordinado entre todas las dependencias académicas y administrativas, sedes y seccionales de la Universidad.

La gestión de riesgos es uno de los principales componentes del Sistema de Control Interno, la responsabilidad y dirección del Sistema de Gestión de Riesgos se basa en el esquema de Tres Líneas de Defensa⁹ que proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y el control mediante la aclaración de funciones y deberes esenciales.

Las responsabilidades de la gestión de riesgos y el control están distribuidas en varias áreas y no se concentran únicamente en la Oficina de Auditoría Institucional o en la División de Arquitectura de Procesos por lo cual deben ser coordinadas cuidadosamente para asegurar que los controles operen adecuadamente¹⁰ (ver Ilustración 5).

⁹ The IIA. IIA Position Paper: The three lines of defense in effective risk management and control. 2013.

¹⁰ DAFP. Marco General MIPG. 2017.

Ilustración 5. Responsables de la Gestión de Riesgos



Fuente: Elaboración propia adaptada de *The IIA Position Paper: The Three Lines of defense in effective risk management and control*

4.9.1. Línea estratégica

La línea estratégica es la encargada de fijar los objetivos de la institución, definir las estrategias para alcanzar dichos objetivos y establecer las estructuras y procesos administrativos que mejor gestionan los riesgos asociados a dichos objetivos y estrategias. Ésta línea está conformada por la el Consejo Superior Universitario, Consejo Académico, Rectoría y el Comité Coordinador de Control Interno.

Consejo Superior Universitario

El artículo 29 del Estatuto General de la Universidad de Antioquia establece que el Consejo Superior Universitario es el máximo organismo de dirección y gobierno en la Universidad. De acuerdo con el Estatuto General de la Universidad, algunas de sus funciones son:

- Adoptar el Plan de Desarrollo Institucional.
- Definir y evaluar periódicamente las políticas administrativas.
- Velar para que la marcha de la institución esté acorde con las disposiciones constitucionales y legales, los estatutos y los reglamentos de la Universidad y las políticas institucionales

Consejo Académico

El artículo 34 del Estatuto General de la Universidad de Antioquia establece que el Consejo Académico es la máxima autoridad académica de la Universidad. De acuerdo con el Estatuto General de la Universidad, algunas de sus funciones son:

- Decidir sobre el desarrollo académico de la Institución, especialmente en cuanto a programas de investigación, de docencia y de extensión.
- Adoptar las políticas académicas referentes al profesorado y al estudiantado.
- Conceptuar ante el Consejo Superior sobre la propuesta de plan de desarrollo de la Institución presentada por el Rector y sugerir modificaciones e innovaciones al que se encuentre vigente.
- Considerar el proyecto de presupuesto de la Universidad preparado por la Vicerrectoría Administrativa y recomendarlo al Consejo Superior por medio del Rector.

Rectoría

El artículo 6 de la Ley 87 de 1993 establece que el diseño y desarrollo del Sistema de Control Interno en la Universidad es responsabilidad de su representante legal o máximo directivo. Al ser la gestión de riesgos un componente del Sistema de Control Interno, el Rector es el máximo responsable de la implementación y desarrollo del Sistema de Gestión de Riesgos. Algunas de sus funciones son:

- Dirigir el funcionamiento general de la Universidad.
- Adoptar procedimientos apropiados de planeación, programación, dirección, ejecución, evaluación y control de las actividades de la Institución.
- Cumplir y hacer cumplir las normas constitucionales, legales, estatutarias y reglamentarias vigentes.

Comité Coordinador de Control Interno

A través de la Resolución Superior 2299 del 11 de diciembre de 2018, se define que el Comité Coordinador de Control Interno es la instancia de más alto nivel al interior del Sistema de Control Interno, presidido por el Rector e integrado por los miembros de nivel directivo de la Rectoría de la Universidad.

4.9.2. Primera línea de defensa

La primera línea de defensa es la operación de la Universidad, está compuesta por diferentes líderes de procesos y dependencias que poseen y gestionan riesgos; son los responsables de diseñar, implementar y monitorear los controles y gestionar de manera directa los procesos y riesgos a su cargo.

La gestión académico-administrativa de todas las dependencias es la primera línea de defensa debido a que los controles se diseñan en los sistemas y procesos que están bajo la dirección de los líderes de procesos.

4.9.3. Segunda línea de defensa

La segunda línea de defensa se encarga de asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea estén diseñados apropiadamente y funcionen como se espera. Está compuesta por dependencias y funcionarios que tienen responsabilidades directas en el monitoreo y evaluación de los controles de los riesgos.

Está compuesta por la Dirección de Planeación y Desarrollo Institucional (División de Arquitectura de Procesos), los líderes de los procesos de seguridad y salud en el trabajo, gestión ambiental, gestión informática, el Comité de Contratación, Comité de Habilitación de Servicios de Salud, interventores de contratos y proyectos.

4.9.4. Tercera línea de defensa

La tercera línea de defensa está conformada por la Oficina de Auditoría Institucional. Proporciona información sobre la efectividad del Sistema de Control Interno de la Universidad de Antioquia. Sus funciones son la asesoría y acompañamiento en materia de control interno, el fomento de la cultura de control y proporcionar una evaluación independiente.

El rol principal de esta línea es proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. El alcance de este aseguramiento, realizado a través de la auditoría interna cubre todos los componentes del Sistema de Control Interno.

4.10. Proceso de gestión de riesgos

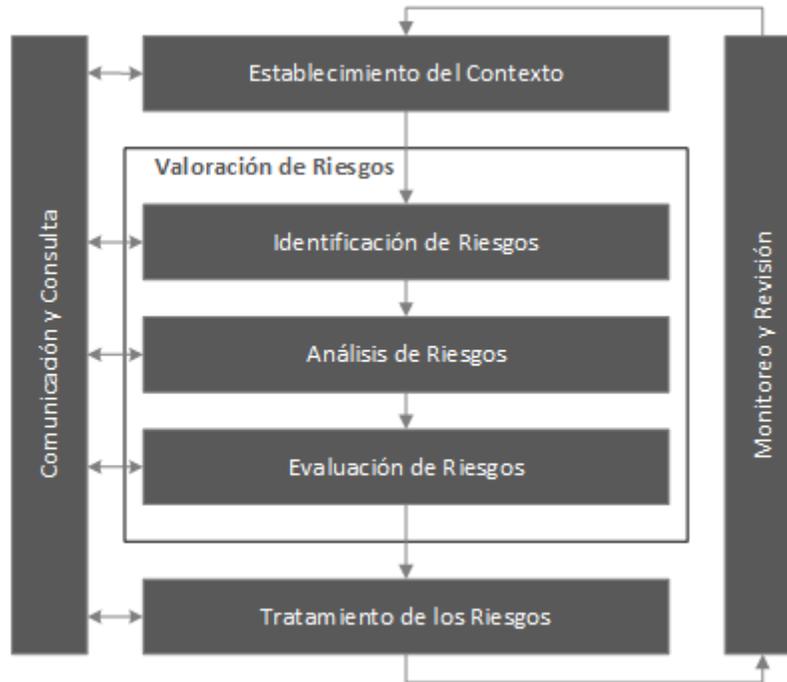
La gestión de riesgos es un proceso transversal y paralelo a todos los sistemas y demás procesos de la Universidad, sus unidades académicas, administrativas, y dependencias. Las etapas definidas para la gestión de riesgos deben ser parte integral de la gestión universitaria y estar incluidas en la cultura y prácticas organizacionales.

El proceso comprende las siguientes etapas y actividades:

1. Establecimiento del contexto.
2. Valoración de Riesgos.
3. Tratamiento de Riesgos.
4. Comunicación y Consulta.
5. Monitoreo y Revisión.

Estas etapas son cíclicas y deben aplicarse periódicamente debido a los cambios que se generan, tanto por los cambios en el entorno a la Universidad, como por cambios en los factores internos, que pueden propiciar la evolución de riesgos diferentes a los identificados y controlados inicialmente.

Ilustración 6. Proceso para la Gestión de Riesgos



Fuente: Adaptación de la norma ISO 31000

Adicionalmente el proceso de gestión de riesgos debe establecer los criterios generales para la identificación y prevención de los riesgos de corrupción de la institución, permitiendo a su vez la generación de alarmas y la elaboración de mecanismos orientados a evitarlos; previniéndolos o mitigándolos. Para mayor profundidad ver el numeral 4.11

4.10.1. Establecimiento del contexto

Establecer el contexto significa que la Universidad articula sus objetivos, define los parámetros internos y externos que se van a considerar para la gestión de riesgos y define el alcance y los criterios de riesgos para el resto del proceso.

4.10.1.1. Contexto externo

Entender el contexto externo es importante para garantizar que los objetivos y las preocupaciones de las partes externas involucradas se consideren al desarrollar los criterios de los riesgos. Establecer el contexto externo es un ejercicio de planeación que se desarrolla a lo largo y ancho de la Universidad según el Acuerdo Superior 255 del 11 de marzo del 2003.

4.10.1.2. Contexto interno

El contexto interno es el ambiente interno en el cual la Universidad busca alcanzar sus objetivos con respecto a la gestión de riesgos. El proceso debe estar alineado con la cultura, los procesos, la organización y la estrategia de la Universidad.

4.10.1.3. Contexto de la gestión de riesgos

Corresponde al establecimiento de los objetivos, estrategias, alcances y parámetros de las actividades de la Universidad, o unidades de la Universidad, donde se aplicará el proceso para la gestión de riesgos. El contexto involucra:

- Definición de las metas y los objetivos de las actividades de la gestión de riesgos.
- Definición de las responsabilidades del proceso de gestión de riesgos.
- Definición del alcance del proceso de gestión de riesgos.
- Definición de la actividad, proceso, proyecto, función, servicio o activo.
- Definición de las relaciones entre el proceso, actividad, servicio, proyecto, etc. y otros procesos, actividades, servicios o proyectos de la Universidad.
- Definición de las metodologías para la valoración de los riesgos.
- Definición de las formas para evaluar el desempeño y la eficacia de la gestión de riesgos.

La definición de lo anterior ayuda a garantizar que el proceso de gestión de riesgos que se ha adoptado es el adecuado para la Universidad.

4.10.1.4. Contexto del proceso

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se deben considerar factores como:

- Objetivo(s) del proceso.
- Alcance del proceso.
- Entradas y salidas del proceso
- Relación con otros procesos.

- Procedimientos y trámites asociados.
- Líderes y responsables del proceso.

4.10.2. Valoración del riesgo

La valoración de riesgos es el proceso total de identificación, análisis y evaluación de riesgos. Su propósito es suministrar información y análisis con base en evidencias con el fin de estimar la zona de riesgo inicial (Riesgo Inherente) y tomar decisiones informadas sobre la manera de tratar los riesgos encontrados.

Los riesgos se pueden valorar en el ámbito de la Universidad, una unidad, una dependencia, un proceso, un proyecto o una actividad específica.

4.10.2.1. Identificación de riesgos

Es una de las etapas más importantes en el proceso de gestión de riesgos. Permite poner al descubierto situaciones y tomar consciencia de las posibilidades y peligros que pueden enfrentar en su actuar. Es el proceso para hallar, reconocer y registrar los riesgos.

La identificación es determinar los posibles eventos que con su materialización puedan impactar objetivos, estrategias, planes, proyectos, servicios, productos u operaciones de la dependencia. De su correcta identificación dependen las acciones posteriores, mientras que con su omisión la unidad puede quedar sujeta al vaivén de las circunstancias.

Los beneficios de una buena identificación de riesgos se pueden dividir en dos: primero con lo que se puede prevenir y segundo con lo que se puede aprovechar. Si se identifican a tiempo y se estudia cómo gestionarlos, se pueden transformar a favor de la institución. Su evaluación puede llevar a vislumbrar decisiones (en ocasiones poco obvias) que permiten proteger y generar valor para la comunidad universitaria.

Consecuencias de no identificar los riesgos

- Si un riesgo no es identificado es como si no existiera, lo cual equivale a aceptar las consecuencias de su materialización.
- Si no se identifican los riesgos no se puede planear su control, no se pueden definir medidas para disminuir su probabilidad de ocurrencia, minimizar su impacto, transferirlos, eliminar la actividad que los genera o asumirlos, si es el caso.

Responsables de la identificación de riesgos

Como la identificación de riesgos tiene un amplio alcance, en esta actividad participan diferentes actores, unos como responsables directos o propietarios de los riesgos y otros como personal de apoyo. En general, participan los líderes de los procesos, proyectos,

servicios o productos, con el apoyo de los Gestores de Riesgos y la División de Arquitectura de Procesos.

Clasificación de riesgos Universidad de Antioquia

Para identificar los riesgos, se hace necesario tener claridad acerca de los tipos de riesgos inherentes a la Universidad, con el fin de que su gestión sea integral. Por tal motivo se establecen 3 niveles para la clasificación de los riesgos: Categoría de Riesgos, Subcategoría de Riesgos y Riesgos Específicos.

En la Guía para la Clasificación de Riesgos (DI-AP-GU-07) se presentan y describen las diferentes categorías, subcategorías y riesgos definidos por la Universidad.

Ilustración 7. Categorías de Riesgos



Fuente: Elaboración propia

Descripción de los riesgos

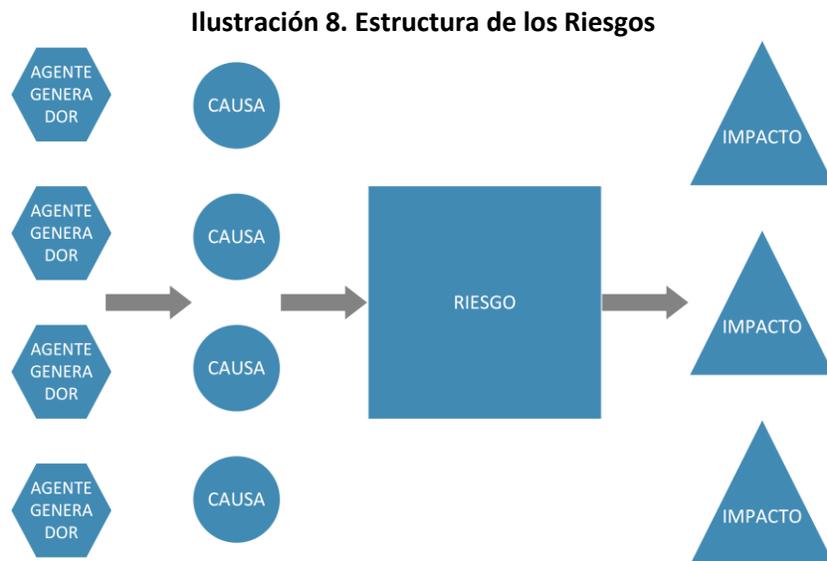
La identificación de los riesgos no se limita únicamente a asignar un nombre al riesgo, también busca dar respuesta a las siguientes preguntas con respecto a los riesgos listados anteriormente:

DI-AP-MA-07, Versión: 03

<La impresión o copia digital de este documento se considera "COPIA NO CONTROLADA". Solo se garantiza la actualización de la documentación en el sitio <http://www.udea.edu.co>>

- ¿Cómo puede suceder?
- ¿Quién puede generarlo?
- ¿Por qué se puede presentar?
- ¿Cuándo puede ocurrir?

Una vez descritos los riesgos se pasa a identificar y describir los agentes generadores, sus causas y los efectos.



Fuente: Elaboración propia

4.10.2.2. Análisis de riesgos

El análisis de riesgos implica el desarrollo y comprensión de los riesgos, busca establecer su probabilidad de ocurrencia y las consecuencias (impacto) de su materialización, calificándolos y evaluándolos para determinar la zona de riesgo inicial (Riesgo Inherente).

Genera información sobre si es necesario o no tratar los riesgos y cuáles son las estrategias y métodos más adecuados para su tratamiento.

El primer paso para el análisis de riesgos consiste en desarrollar los criterios que se tendrán en cuenta, definiendo las escalas de medición tanto para la probabilidad como para el impacto. Definir las escalas es un paso supremamente importante ya que permite establecer estándares de comparación, sin éstos sería imposible comparar, agregar y tomar decisiones informadas acerca de los riesgos. Las escalas deben permitir la diferenciación y clasificación de los riesgos.

Para el caso de la Universidad de Antioquia se establecen 5 niveles para cada uno. Cada institución es diferente, por lo que las escalas se deben establecer para la Universidad considerando sus particularidades y contexto.

Probabilidad

La probabilidad representa la posibilidad de que un evento de riesgo ocurra, la probabilidad se debe determinar basada en un marco temporal, en el caso de la Universidad de Antioquia, se definen unos criterios de referencia para la medición de la probabilidad, empleando la frecuencia de ocurrencia o el número de veces en el año que puede presentarse el riesgo (ver **¡Error! No se encuentra el origen de la referencia.**).

Tabla 1. Criterios de referencia para analizar la probabilidad

VALOR	NIVEL	DESCRIPCIÓN	FRECUENCIA	
5	Casi seguro	El evento ocurre en la mayoría de las circunstancias. Probabilidad muy alta	Se ha presentado más de una vez al año	El evento se ha presentado en un porcentaje mayor o igual al 80% del total de los eventos potenciales
4	Probable	El evento posiblemente ocurrirá en la mayoría de circunstancias. Probabilidad alta	Se presentó una vez en el último (1) año	El evento se ha presentado en un porcentaje mayor o igual al 60% y menor al 80% de los eventos potenciales
3	Posible	El evento podría ocurrir en algún momento. Probabilidad media	Se presentó una vez en los últimos dos (2) años	El evento se ha presentado en un porcentaje mayor o igual al 40% y menor al 60% de los eventos potenciales.
2	Improbable	El evento puede ocurrir en algún momento. Probabilidad baja	Se presentó una vez en los últimos cinco (5) años	El evento se ha presentado en un porcentaje mayor al 20% y menor al 40% de los eventos potenciales.
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepciones. Probabilidad muy baja	No se ha presentado en los últimos cinco (5) años	El evento se ha presentado en un porcentaje menor o igual al 20% de los eventos potenciales.

Fuente: Elaboración propia

Impacto

El impacto o consecuencia se refiere al grado en el que un evento de riesgo puede afectar a la Institución. Los criterios para medir el impacto pueden ser diversos, en el caso de la Universidad de Antioquia se establecen seis (6) dimensiones a tener en cuenta:

- Económico
- Reputacional
- Operativo
- Humano
- Información
- Ambiental

Las dimensiones anteriores se establecen ya que hay riesgos que pueden afectar a la Institución de diversas formas. Para seleccionar el nivel de impacto del riesgo, se selecciona el valor más alto obtenido entre todas las dimensiones (ver Tabla 2).

Tabla 2. Criterios de referencia para analizar los impactos

VALOR	NIVEL	DESCRIPCIÓN					
		Dimensión Económica	Dimensión Humana	Dimensión Operacional / Nivel de Servicio	Dimensión Información	Dimensión Ambiental	Dimensión Reputacional
5	Catastrófico	Pérdidas o daños superiores a 50 SMLMV por evento	Víctima(s) letal(es)	Suspensión mayor a 10 días	Pérdida de más del 30% de información crítica	Contaminación grave e irreversible	De conocimiento externo a nivel nacional
4	Severo	Pérdidas o daños entre 20 y 50 SMLMV por evento	Víctima(s) grave(s) hospitalizada(s) sin víctimas letales	Suspensión entre 5 y 10 días	Pérdida entre el 10% y 30% de información crítica	Contaminación es inaceptable y se requieren acciones inmediatas y efectivas para recuperarlo	De conocimiento externo a nivel local
3	Moderado	Pérdidas o daños entre 5 y 20 SMLMV por evento	Lesiones leves que generan incapacidad	Suspensión entre 1 y 5 días	Pérdida de más del 30% de información no crítica o hasta el 10% de información crítica	Contaminación es preocupante y requiere acciones para mitigarlo	De conocimiento interno para toda la comunidad universitaria
2	Leve	Pérdidas o daños entre 1 y 5 SMLMV por evento	Lesiones leves sin incapacidad	Suspensión entre 4 horas y 1 día	Pérdida entre 10% y 30% de información no crítica	Contaminación es menor, pero requiere acciones preventivas para mitigarlo	Sólo es de conocimiento en ciertos grupos de la Universidad
1	Insignificante	Pérdidas o daños inferiores a 1 SMLMV por evento	Sin lesiones	Suspensión menor a 4 horas	Pérdida hasta un 10% de información no crítica	Contaminación es insubstancial y no requiere mitigarlo	Sólo es de conocimiento en la dependencia

Nivel de Riesgo

Para estimar el nivel del riesgo los valores determinados para la probabilidad y el impacto o consecuencias del riesgo analizado se cruzan en la siguiente matriz (ver Tabla 3), y es allí donde se determina la zona en la cual se ubica el riesgo.

Calificación del Riesgo = Probabilidad x Impacto

Tabla 3. Matriz Calificación de Riesgos

PROBABILIDAD	VALOR	NIVEL	PROBABILIDAD POR IMPACTO				
	5	Casi seguro	5	10	15	20	25
4	Probable	4	8	12	16	20	
3	Posible	3	6	9	12	15	
2	Improbable	2	4	6	8	10	
1	Rara vez	1	2	3	4	5	
			Insignificante	Leve	Moderado	Severo	Catastrófico
			1	2	3	4	5
			IMPACTO				

Fuente: Elaboración propia

A partir de la matriz de calificación de riesgo se establecen las zonas para determinar la gravedad del riesgo; a cada zona se le asocia un código de color tipo semáforo, lo cual permite determinar las acciones que se deben tomar para gestionarlo. Para evaluar y determinar la gravedad de los riesgos de la Universidad se establecieron 4 zonas: Baja (verde), Moderada (amarillo), Alta (naranja), Extrema (rojo).

- **Zona BAJA (Verde)**

La zona A se presenta sólo cuando el impacto del riesgo es insignificante y la ocurrencia no es mayor a probable. Aquí se ubican los riesgos que tienen impactos no significativos y que en general se presentan poco durante el año.

Los riesgos ubicados en esta clasificación no se consideran importantes para la Institución y por lo tanto se aceptan.

- **Zona MODERADA (Amarillo)**

Los riesgos ubicados en la categoría moderada son riesgos cuyos impactos son moderados a lo máximo. Son riesgos importantes para la institución, pero no se consideran críticos por lo que se deben tratar en el mediano plazo una vez se hayan tratado riesgos más importantes. Los controles que principalmente se aplican a la categoría son de orden preventivo.

- **Zona ALTA (Naranja)**

Son riesgos muy importantes para la institución, sus impactos son principalmente moderados y severos. Son riesgos que deben ser tratados en el corto plazo y se deben implementar controles preventivos y de protección sobre ellos.

- **Zona EXTREMA (Roja)**

Esta es la zona de los riesgos más críticos para la institución debido a que tienen altos impactos y se presentan frecuentemente. Se deben tratar inmediatamente. Las medidas recomendadas contemplan una mezcla de controles preventivos y de protección; estos riesgos son tan críticos que incluso en algunos casos especiales se debe evitar realizar la tarea o actividad que genera el riesgo.

4.10.2.3. Evaluación de riesgos

El propósito de la evaluación de riesgos es facilitar la toma de decisiones, basada en sus resultados, acerca de cuáles riesgos necesitan tratamiento y cuál es el nivel de prioridad para aplicar dicho tratamiento.

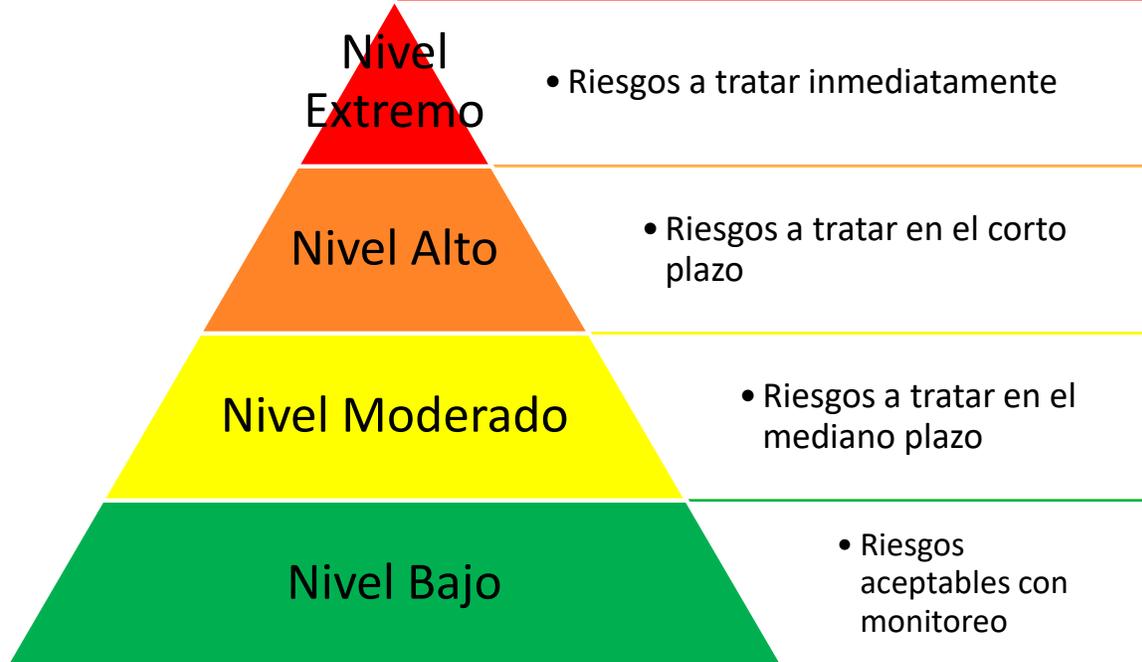
En este punto se evalúan las calificaciones obtenidas en la etapa anterior y se establece la situación en la que se encuentra el riesgo analizado para el proceso, dependencia, unidad o proyecto sobre el cuál se esté realizando el análisis (ver Tabla 4), y se ubica en una de las zonas establecidos para determinar la gravedad de los riesgos. Este primer análisis del riesgo se denomina *Riesgo Inicial o Inherente* y se define como aquél al que se enfrenta una entidad en ausencia de acciones por parte de la Dirección para modificar la probabilidad o impacto del riesgo.

Tabla 4. Matriz Evaluación de Riesgos (Zonas de Criticidad)

PROBABILIDAD	5	Casi seguro	Moderada 5	Alta 10	Alta 15	Extrema 20	Extrema 25
	4	Probable	Baja 4	Moderada 8	Alta 12	Extrema 16	Extrema 20
	3	Posible	Baja 3	Moderada 6	Alta 9	Extrema 12	Extrema 15
	2	Improbable	Baja 2	Moderada 4	Alta 6	Alta 8	Extrema 10
	1	Rara vez	Baja 1	Moderada 2	Moderada 3	Alta 4	Extrema 5
			Insignificante	Leve	Moderado	Severo	Catastrófico
			1	2	3	4	5
IMPACTO							

Fuente: Elaboración propia

Ilustración 9. Niveles de Criticidad de los Riesgos y su Marco Temporal para el Tratamiento



Fuente: Elaboración propia

4.10.3. Tratamiento de los riesgos

Una vez valorados los riesgos, se deciden las medidas de tratamiento con las cuales se van a gestionar los riesgos. Para hacerlo existen principalmente dos opciones: una relacionada con el manejo del riesgo como tal, y otra relacionada con la disponibilidad de fondos para subsanar las pérdidas asociadas. La primera opción se conoce como control del riesgo.

4.10.3.1. Medidas de tratamiento de los riesgos

Las medidas de control de riesgos son:

EVITAR

Se parte del principio de que su probabilidad es alta y representa un alto peligro para la Institución porque podría traer consecuencias serias en caso de que ocurriera.

Para evitar un riesgo hay dos opciones: 1) eliminar su probabilidad de ocurrencia y 2) disminuir totalmente su impacto. En la primera opción se debe eliminar la actividad que genera el riesgo o reubicar los recursos que están siendo amenazados; para la opción 2) se deben tomar medidas de protección extremas que en algunos casos pueden resultar inviables debido al costo de implementar dichas medidas.

Evitar o eliminar un riesgo se da en casos extremos, en los que el beneficio de eliminar la actividad o la implementación de las medidas de protección, sea mayor que el costo que implica no hacer o dejar de hacer la actividad

PREVENIR

Significa anticiparse y actuar antes de que ocurra algo. En el caso de la gestión de riesgos se toman medidas para que su probabilidad de ocurrencia disminuya.

La prevención se basa en la anticipación, estableciendo políticas, normas, controles y procedimientos encaminados a que el evento no ocurra o disminuya su probabilidad (frecuencia) de ocurrencia. Algunas de las medidas para prevenir los riesgos son:

- Inspecciones y pruebas de seguridad
- Entrenamiento
- Aumentar el nivel de información disponible para tomar decisiones
- Diversificar
- Disminuir el nivel de exposición
- Segregar o dispersar la actividad
- Mantenimiento preventivo
- Expedir políticas y normas internas de seguridad

PROTEGER O MITIGAR

En la gestión de riesgos, esta medida de tratamiento busca proteger los recursos que amenazan los riesgos (personas, materiales, información, etc.) para evitar pérdidas en el evento de ocurrir un riesgo. La protección actúa sobre los efectos de los riesgos. Al igual que la prevención, la protección se logra a través del diseño y aplicación de políticas, normas, controles y procedimientos que buscan disminuir el impacto negativo sobre la institución que generan los riesgos en caso de su materialización.

Existen muchas formas de protección aplicadas, algunas son activas y otras pasivas; las activas requieren de la intervención humana para su funcionamiento y control, las pasivas actúan sin necesidad de intervención.

- Sistemas automáticos de protección
- Equipos de protección personal
- Plan de emergencia
- Plan de contingencia
- Planes de comunicaciones
- Sistemas de información redundante

ACEPTAR

Se asumen las pérdidas que ocasionen los riesgos. Por lo general los riesgos se asumen cuando la frecuencia es baja y el impacto es leve y no ponen en peligro a la institución. Cuando se determina que la medida más adecuada para tratar un riesgo es aceptarlo,

significa que no es necesario desarrollar medidas adicionales de prevención o protección del riesgo analizado.

La decisión de aceptar un riesgo viene acompañada de un estudio que justifique tal decisión, por lo que no es permitido aceptar riesgos sin una justificación apropiada. En todos los casos los riesgos aceptados deben ser revisados periódicamente, considerando los cambios en el entorno y sus implicaciones en la frecuencia o impacto del riesgo.

Cuando se acepta un riesgo, las pérdidas generadas por la materialización de este son asumidas por la operación. En caso de aceptar riesgos por desconocimiento o error en su identificación, las pérdidas pueden ser considerables; de ahí la importancia de realizar el proceso identificación, análisis y evaluación de forma juiciosa y estructurada.

RETENER

Consiste en afrontar los riesgos de forma planeada a través de la creación de un fondo, cuenta de gastos, una provisión contable, crédito, etc. para responder ante las pérdidas causadas por un riesgo.

Con la retención se decide afrontar las consecuencias de los riesgos en forma planeada, previo al diseño de alternativas que faciliten responder ante ellos. La diferencia entre aceptar y retener un riesgo es que, en el caso de aceptarlo, no se dispone de medidas para afrontar las pérdidas que la ocurrencia implica, y en el caso de retenerlo, se establecen diferentes formas para afrontarlas. A continuación, se presentan varias formas para la retención de riesgos:

- Creación de un fondo
- Presupuestar el gasto
- Provisión contable

TRANSFERIR

Consiste en trasladar las pérdidas a otra entidad, a través de la firma de contratos o seguros en los cuales el asegurador se hace responsable de las pérdidas que ocasionen los riesgos. La forma más común es a través de un contrato de seguros, aunque existen otras formas que requieren conocimiento especializado.

Al transferir el riesgo vía contrato de seguros, no se entiende que el riesgo se reduzca, sino que las pérdidas asociadas son asumidas por la compañía aseguradora.

4.10.3.2. Selección de medidas de tratamiento

La selección de las opciones más adecuadas para el tratamiento de los riesgos implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios obtenidos.

Las medidas de tratamiento a aplicar pueden ser individuales o una combinación de varias medidas, por lo general esto es lo más recomendable para obtener mejores resultados disminuyendo los costos del tratamiento al tiempo.

En la Tabla 5 se combinan los resultados de la calificación de los riesgos, sus valoraciones y las zonas de gravedad junto con una serie de tratamientos recomendados. Si bien las medidas de tratamiento son recomendadas se definen los siguientes lineamientos que orientan la selección de los tratamientos.

- Sólo se pueden aceptar riesgos que se encuentren en la zona baja.
- Cuando el impacto es catastrófico y la ocurrencia es probable o casi segura se debe considerar la opción de eliminar la actividad que genera el riesgo.
- Se sugiere prevenir los riesgos cuando la ocurrencia de éstos es posible, probable o casi segura.
- Se sugiere proteger cuando el impacto es moderado, severo o catastrófico.
- Se aconseja retener cuando el impacto es insignificante, leve o moderado.
- Se aconseja transferir cuando el impacto es severo, catastrófico o moderado con altas frecuencias, siempre y cuando existan seguros para dichos riesgos.

Finalmente, la(s) medida(s) de tratamiento seleccionada(s) dependerán de las particularidades del proceso, la dependencia o la unidad que esté realizando el análisis pues no siempre se podrán emplear los tratamientos recomendados debido a restricciones en los recursos.

Tabla 5. Matriz de Medidas de Tratamiento recomendadas de acuerdo al nivel del riesgo

PROBABILIDAD	5	Casi seguro	5 Nivel Moderado -Retener -Prevenir	10 Nivel Alto -Retener -Prevenir	15 Nivel Alto -Transferir el riesgo -Prevenir -Proteger	20 Nivel Extremo -Transferir el riesgo -Prevenir -Proteger	25 Nivel Extremo -Eliminar la actividad -Prevenir -Proteger
	4	Probable	4 Nivel Bajo -Aceptar	8 Nivel Moderado -Retener -Prevenir	12 Nivel Alto -Transferir el riesgo -Prevenir -Proteger	16 Nivel Extremo -Transferir el riesgo -Prevenir -Proteger	20 Nivel Extremo -Eliminar la actividad -Prevenir -Proteger
	3	Posible	3 Nivel Bajo -Aceptar	6 Nivel Moderado -Retener -Prevenir	9 Nivel Alto -Retener -Prevenir -Proteger	12 Nivel Extremo -Transferir el riesgo -Prevenir -Proteger	15 Nivel Extremo -Transferir el riesgo -Prevenir -Proteger
	2	Improbable	2 Nivel Bajo -Aceptar	4 Nivel Moderado -Retener	6 Nivel Alto -Retener -Proteger	8 Nivel Alto -Transferir el riesgo -Proteger	12 Nivel Extremo -Transferir el riesgo -Proteger
	1	Rara vez	1 Nivel Bajo -Aceptar	2 Nivel Moderado -Retener	3 Nivel Moderado -Retener -Proteger	4 Nivel Alto -Transferir el riesgo -Proteger	5 Nivel Extremo -Transferir el riesgo -Proteger
				Insignificante	Leve	Moderado	Severo
			1	2	3	4	5
IMPACTO							

4.10.3.3. Diseño e implementación de medidas para el tratamiento de los riesgos

Una vez definidas las medidas de tratamiento que se quieren implementar, es necesario diseñarlas y establecer planes y acciones para la implementación de éstas en los procesos y dependencias de la Universidad.

DISEÑO DE CONTROLES

Los controles corresponden a las medidas de tratamiento de los riesgos (Prevenir o Proteger), los cuales permiten reducir los riesgos porque actúan sobre los dos componentes de los riesgos: la frecuencia y el impacto. Con la prevención se actúa sobre las causas y agentes generadores y por lo tanto se disminuye su frecuencia o probabilidad de ocurrencia; y con la protección se actúa sobre los efectos de los riesgos a la vez que disminuye su impacto.

Para efectuar una implementación exitosa, que responda a las necesidades y recursos de la Universidad, se requiere establecer un programa que garantice que los planes se aprueben, se analicen y se les asigne prioridades en su implementación. También es importante establecer los resultados esperados del plan de tratamiento y la forma cómo se van a medir.

Para que los controles actúen tal como fueron diseñados y contribuyan a la detección y reducción de los riesgos, deben cumplir con las siguientes características:

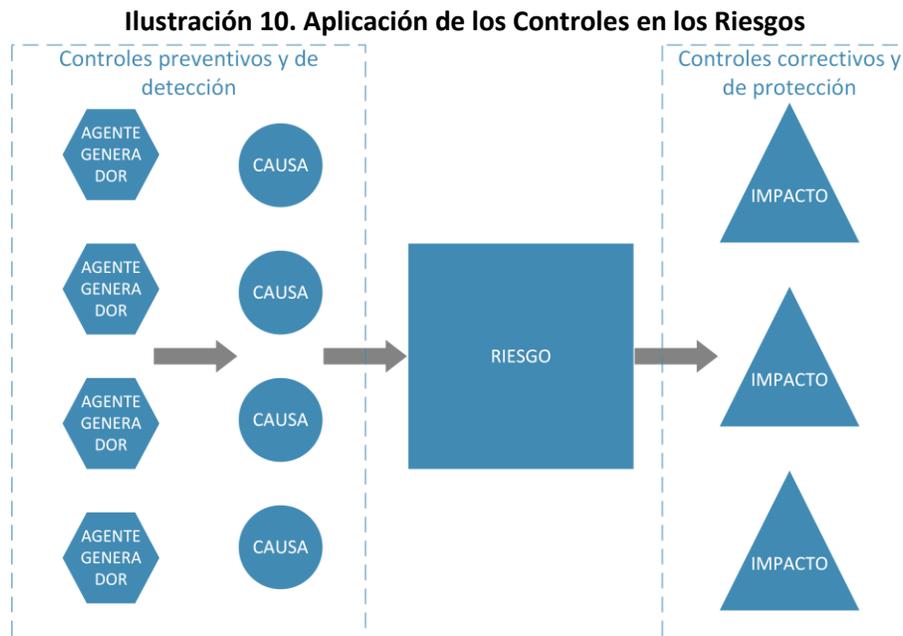
- Suficientes: La cantidad de controles implementados debe ser la estrictamente necesaria.
- Comprensibles: Controles claros, sencillos y fáciles de interpretar e implementar.
- Económicos: El costo de los controles debe ser menor que el beneficio que aportan.
- Eficaces: La acción de los controles debe permitir disminuir el impacto o frecuencia del riesgo.
- Eficientes: Deben hacer una correcta utilización de los recursos involucrados en su aplicación.
- Efectivos: Debe ser eficaz y eficiente al tiempo.
- Oportunos: Que actúen cuando realmente se necesiten.
- Inmersos en los procesos: Que la ejecución de alguna de las actividades que componen el proceso contenga el control.

Existen muchos tipos de controles, pero si se clasifican de acuerdo a su propósito se tienen cuatro categorías:

- Controles preventivos: Son controles que actúan sobre las causas de los riesgos y los agentes generadores, con el propósito de disminuir la probabilidad de ocurrencia de

los riesgos identificados. Corresponden a la primera barrera de seguridad que se establece para reducir los riesgos.

- Controles de detección: Corresponden a la segunda barrera de seguridad para reducir los riesgos. Se establecen para detectar, registrar e informar los eventos negativos que pueden afectar a la institución. Generalmente sirven para supervisar la ejecución del proceso y verificar la eficacia de los controles preventivos.
- Controles de protección: Son la tercera barrera de seguridad para reducir los riesgos. Su objetivo es neutralizar o disminuir el efecto inmediato que traen consigo la materialización de los riesgos.
- Controles correctivos: Son controles que se implementan una vez el riesgo ya ha ocurrido y buscan mejorar los demás controles si se determina que su funcionamiento no es el esperado. Permiten corregir las desviaciones y prevenir de nuevo la ocurrencia de un riesgo.



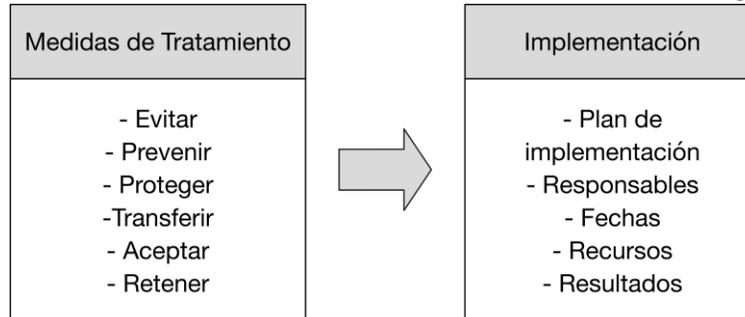
Fuente: Elaboración propia

Los planes de tratamiento deben incluir como mínimo:

- Las razones para la selección de las opciones de tratamiento, incluyendo los beneficios que se esperan obtener con éstas.
- Responsables de la aprobación del plan y de su implementación.
- Las acciones propuestas.
- Recursos requeridos para desarrollar el plan.
- Requisitos de monitoreo y reporte de información.

- Tiempo y cronograma de implementación.

Ilustración 11. Elementos del Plan de Tratamiento de los Riesgos



Fuente: Elaboración propia

Se recomienda que los planes de tratamiento se integren con los planes de gestión de la dependencia responsable del proceso analizado.

4.10.4. Comunicación y consulta

La comunicación y consulta con las partes involucradas tanto interna como externamente están consideradas en el sistema de gestión de riesgos y en su proceso, por tal motivo, se debe establecer un plan de consulta y comunicaciones con las partes interesadas para que éstas entiendan las bases sobre las cuales se toman las decisiones y las razones por las cuales se requieren acciones particulares en materia de gestión de riesgos.

La comunicación y la consulta deben facilitar el intercambio de información veraz, pertinente, precisa y fácil de entender, teniendo en cuenta aspectos de confidencialidad cuando sea el caso.

4.10.5. Monitoreo y revisión

El monitoreo y revisión debe ser una parte planificada del proceso de gestión de riesgos y deberá incluir una verificación y vigilancia regular. Se debe realizar un seguimiento al estado de los riesgos, el progreso de los planes de tratamiento establecidos y el avance y efectividad del proceso en general. Para el caso de los riesgos de corrupción el seguimiento se realizará según lo establecido en el numeral 4.10.5 del presente manual.

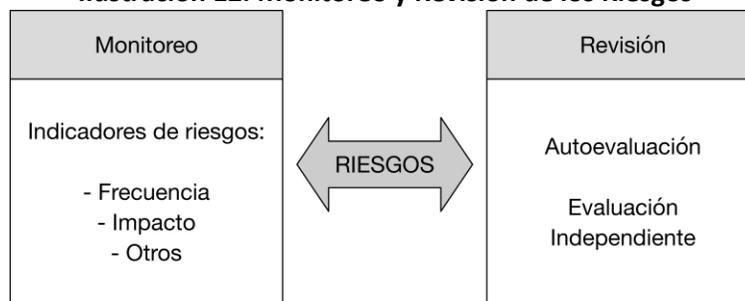
El monitoreo y revisión son necesarios debido a los cambios que se generan en el entorno y en la Universidad, pues estos cambios traen consigo nuevas oportunidades, pero también nuevos riesgos. Otra razón importante es que con el tiempo se pueden revisar las decisiones

tomadas y encontrar errores en la identificación, calificación o evaluación de los riesgos, lo cual permite reorientar el plan y las medidas de tratamiento.

El monitoreo de los riesgos lo realizan los responsables de los riesgos, a través de la evaluación permanente del comportamiento de éstos y la efectividad de los controles establecidos. Adicionalmente la Oficina de Auditoría Institucional realizará una evaluación independiente.

Para realizar el monitoreo permanente de los riesgos se hace necesario tener información actualizada y disponible sobre la ocurrencia de los riesgos, los impactos que generan a la Universidad cuando se presentan e información adicional que se obtiene al diseñar los indicadores de riesgos.

Ilustración 12. Monitoreo y Revisión de los Riesgos



Fuente: Elaboración propia

Los indicadores de riesgos miden el comportamiento de los riesgos identificados respecto a la frecuencia con que ocurren y el impacto o gravedad de las consecuencias que su ocurrencia tiene sobre la Universidad. Los controles siempre deben asociarse a los indicadores pues éstos son los que alertan sobre desviaciones de la efectividad de su desempeño.

4.11. Gestión de riesgos de corrupción

Con el Artículo 73 de la Ley 1474 del 2011 se establece que cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano. La metodología para construir dicha estrategia está a cargo del Programa Presidencial de Modernización, Eficiencia, Transparencia y Lucha contra la Corrupción (hoy Secretaría de Transparencia).

El Plan Anticorrupción y de Atención al Ciudadano está integrado por seis componentes:

- Gestión del riesgo de corrupción – Mapa de riesgos de corrupción
- Racionalización de trámites
- Rendición de cuentas
- Mecanismos para mejorar la atención al ciudadano, lineamientos generales para la atención de peticiones, quejas, reclamos, sugerencias y denuncias

- Mecanismos para la transparencia y acceso a la información
- Iniciativas adicionales

COMPONENTE 1: Gestión del Riesgo de Corrupción – Mapa de Riesgos de Corrupción.

La Gestión de Riesgos de Corrupción sigue una secuencia de mejora continua, definida a continuación:

Ilustración 13. Ciclo de Mejora Continua para la Gestión de Riesgos de Corrupción



Fuente: Cartilla Estrategias para la Elaboración del Plan Anticorrupción y de Atención al Ciudadano

4.11.1. Política de Administración del Riesgo de Corrupción

La institución se compromete a gestionar de manera integral los riesgos institucionales (incluyendo los riesgos de corrupción) y a emprender las acciones necesarias para proporcionar una seguridad razonable en el cumplimiento de su misión y en procura de la sostenibilidad, el desarrollo y el bien común, según lo expresado en el Acuerdo Superior 453 del 29 de octubre de 2018, que aprueba la política de gestión integral de riesgos.

4.11.2. Construcción de Mapa de Riesgos de Corrupción

La construcción del mapa de riesgos de corrupción de la institución sigue el mismo proceso para la gestión de riesgos descritos en el numeral 3.3, pero haciendo ciertos énfasis o

análisis diferenciados para los riesgos de corrupción.

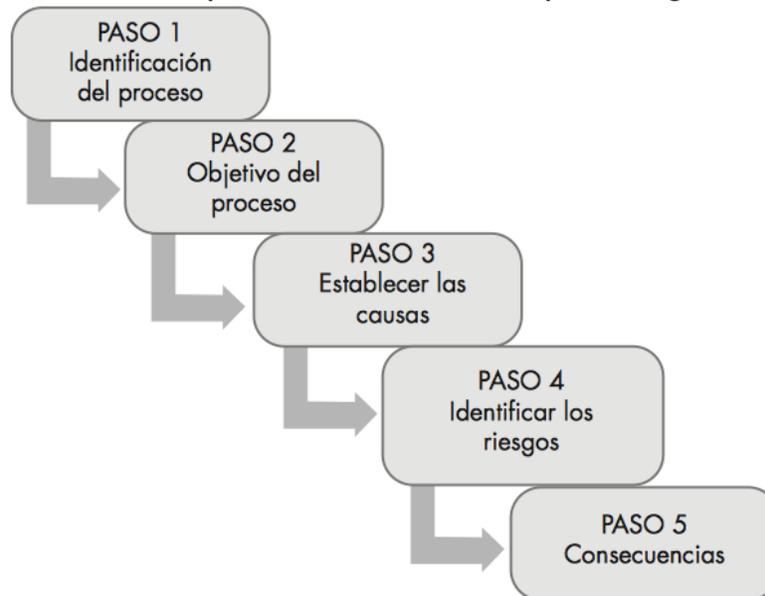
- Establecimiento del contexto externo e interno

Inicialmente se hace necesario establecer la relación que existe entre la institución y el ambiente (interno y externo) en el que opera; estableciendo las fortalezas, debilidades, oportunidades y amenazas relacionadas con los riesgos de corrupción de la institución y los agentes generadores de éstos.

- **Identificación de riesgos de corrupción**

La identificación de los riesgos de corrupción parte de la construcción del riesgo de corrupción; éstos se construyen a partir de los procesos o actividades que desarrolla la institución.

Ilustración 14. Secuencia para la Construcción del Mapa de Riesgos de Corrupción



Fuente: Cartilla Estrategias para la Elaboración del Plan Anticorrupción y de Atención al Ciudadano

Se debe considerar que en ocasiones los riesgos de corrupción pueden ser muy similares a los riesgos operacionales de la institución; por tal motivo, para la identificación de los riesgos de corrupción se deben incorporar los siguientes elementos que están presentes en la definición de riesgos de corrupción:

Descripción del riesgo:

- ¿El riesgo incorpora algún acto de acción u omisión de algún funcionario público?
- ¿El riesgo incorpora el uso del poder de algún funcionario público?
- ¿El riesgo incorpora la desviación de la gestión de lo público?

- ¿El riesgo busca algún beneficio particular?

Si en la identificación y descripción del riesgo se contestan de forma afirmativa todas las preguntas anteriores, entonces se está al frente de un riesgo de corrupción y no operativo.

- **Análisis de riesgos de corrupción**

El objetivo se centra en la medición del riesgo, determinando tanto su probabilidad como su impacto.

Para la calificación de la probabilidad se adopta la misma tabla definida para todos los riesgos (ver Tabla 6 **Error! No se encuentra el origen de la referencia.**); para el impacto se adopta la siguiente escala definida por el Departamento Administrativo de la Función Pública:

Tabla 7. Valores para los impactos de los Riesgos de Corrupción

VALOR	NIVEL	DESCRIPCIÓN
20	Catastrófico	Genera consecuencias catastróficas para la institución
10	Mayor	Genera altas consecuencias negativas para la institución
5	Moderado	Genera como máximo consecuencias medias para la institución

Fuente: Cartilla Estrategias para la Elaboración del Plan Anticorrupción y de Atención al Ciudadano

Para determinar la clasificación del riesgo se responde el siguiente cuestionario y de acuerdo con el número de respuestas afirmativas, se determina el valor del impacto.

Tabla 8. Cuestionario para la calificación de los impactos de 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 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?		

No.	Pregunta: Si el riesgo de corrupción se materializa podría:	Respuesta	
		Si	No
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?		

Fuente: Cartilla Estrategias para la Elaboración del Plan Anticorrupción y de Atención al Ciudadano

Impacto catastrófico: Si hay entre 12 a 18 respuestas afirmativas

Impacto mayor: Si hay entre 6 y 11 respuestas afirmativas

Impacto moderado: si hay entre 1 y 5 respuestas afirmativas

- Evaluación de riesgos**

Con los valores de impacto y probabilidad, se determina el nivel del riesgo de acuerdo con la siguiente matriz:

Tabla 9. Matriz para determinar el Grado de Criticidad de los Riesgos de Corrupción

PROBABILIDAD	5	Casi seguro	N.A.	N.A.	Moderada 25	Alta 50	Extrema 100
	4	Probable	N.A.	N.A.	Moderada 20	Alta 40	Extrema 80
	3	Posible	N.A.	N.A.	Moderada 15	Alta 30	Extrema 60
	2	Improbable	N.A.	N.A.	Baja 10	Moderada 20	Alta 40
	1	Rara vez	N.A.	N.A.	Baja 5	Baja 10	Moderada 20
			Insignificante	Leve	Moderado	Mayor	Catastrófico
			N.A	N.A	5	10	20
IMPACTO							

- Tratamiento de los riesgos**

El tratamiento de los riesgos de corrupción se realizará de acuerdo con el nivel en el que se encuentre el riesgo.

Zona Baja

Puntaje: De 5 a 10 puntos.

Frecuencia / Probabilidad: Rara vez o improbable.

Impacto: Moderado y Mayor.

Tratamiento: Los riesgos de corrupción de las zonas baja se encuentran en un nivel que puede eliminarse o reducirse fácilmente con los controles establecidos en la entidad.

Zona Moderada

Puntaje: De 15 - 25 puntos.

Frecuencia / Probabilidad: Rara vez, Improbable, Posible, Probable y Casi Seguro.

Impacto: Moderado, Mayor y Catastrófico.

Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Baja o eliminarlo.

Nota: En todo caso se requiere que las unidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.

Zona Alta

Puntaje: De 30 - 50 puntos.

Frecuencia / Probabilidad: Improbable, Posible, Probable y Casi Seguro.

Impacto: Mayor y Catastrófico.

Tratamiento: Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de Riesgo Moderada, Baja o eliminarlo.

Nota: En todo caso se requiere que las unidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.

Zona Extrema

Puntaje: De 60 - 100 puntos.

Frecuencia / Probabilidad: Posible, Probable y Casi Seguro.

Impacto: Catastrófico.

Tratamiento: Los riesgos de corrupción de la Zona de Riesgo Extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos y tomar las medidas de protección.

Nota: En todo caso se requiere que las unidades propendan por eliminar el riesgo de corrupción o por lo menos llevarlo a la Zona de Riesgo Baja.

4.11.3.Consulta y Divulgación

La consolidación de los mapas de riesgo de la institución corresponde a la Dirección de Planeación y Desarrollo Institucional quien será la encargada de asesorar y facilitar el proceso de gestión de riesgo de corrupción con las diferentes unidades y dependencias de la Universidad. Concluida la construcción de los mapas con diferentes actores, la Universidad procederá a publicar en la página web institucional el mapa consolidado de riesgos de corrupción.

Es muy importante publicar y divulgar el Mapa de Riesgos de Corrupción de tal manera que los funcionarios y contratistas de la institución, y demás partes interesadas, conozcan cómo se estructuraron los riesgos de corrupción.

El mapa de riesgos de corrupción se publicará una vez al año, a más tardar el 31 de enero de cada año; y se realizarán tres seguimientos anuales los cuales los publicará la Oficina de Auditoría Institucional en las siguientes fechas:

- Primer seguimiento: Primeros diez días hábiles del mes de mayo.
- Segundo seguimiento: Primeros diez días hábiles del mes de septiembre.
- Tercer seguimiento: Primeros diez días hábiles del mes de enero.

4.11.4.Monitoreo y Revisión

Los líderes de los procesos, sus equipos y los propietarios de los riesgos deben monitorear y revisar periódicamente sus Mapas de Riesgos de Corrupción y ajustarlo si es el caso.

Los objetivos de esta fase son:

- Garantizar que los controles son eficaces y eficientes.
- Obtener información adicional que permita mejorar la valoración del riesgo.
- Analizar y aprender lecciones a partir de los eventos, los cambios, las tendencias, los éxitos y los fracasos.
- Detectar cambios en los contextos externo e interno.
- Identificar riesgos emergentes.

4.11.5.Seguimiento

La Oficina de Auditoría Institucional de la Universidad de Antioquia debe realizar el seguimiento al Mapa de Riesgos de Corrupción. El seguimiento se realiza tres veces al año en las siguientes fechas:

- Primer seguimiento: Con corte al 30 de abril.

- Segundo seguimiento: Con corte al 31 de agosto.
- Tercer seguimiento: Con corte al 31 de diciembre.

El seguimiento realizado se publicará en la página web de la Universidad de Antioquia.

Para el seguimiento se realizarán las siguientes actividades y análisis:

- Publicación del mapa de riesgos de corrupción de la institución.
- Revisión de las causas de los riesgos.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y funcionen de forma oportuna y efectiva.

Una vez realizado el seguimiento se definirá un Plan de Mejoramiento en el caso en el cual se materialice un riesgo de corrupción.

5. Documentos de referencia

- Resolución Superior 041 del 19 de mayo de 1994, por la cual se Autoriza al Rector para Desarrollar el Sistema de Control Interno Según la Ley 87 de 1993.
- Resolución Rectoral 4800 del 27 de mayo de 1994, por la Cual se Desarrolla el Sistema de Control Interno de la Universidad de Antioquia.
- Resolución Rectoral 39562 del 19 de diciembre de 2014, por la Cual se Actualiza el Modelo Estándar de Control Interno MECI 1000:2014 en la Universidad de Antioquia.
- Acuerdo Superior 453 del 29 de octubre de 2018, por el cual se establece la Política de Gestión Integral de Riesgos de la Universidad de Antioquia.
- Resolución Superior 2299 del 11 de diciembre de 2018, por la cual se actualiza el Sistema de Control Interno de la Universidad de Antioquia.

6. Glosario

La palabra riesgo puede tener diferentes significados para diferentes personas. Tiene connotaciones de probabilidad, incertidumbre, daño y peligro. Éstas incluyen la posibilidad de pérdidas, lesiones o algún otro evento negativo. Dadas estas consecuencias negativas, es natural asumir que se deben minimizar o evitar los riesgos completamente, de hecho, el riesgo se ha entendido como una barrera para el cumplimiento de los objetivos institucionales, emprender un proyecto o ejecutar un proceso, y el objetivo de la gestión de riesgos se ha enfocado a limitar los riesgos.

En un contexto institucional, los riesgos presentan un lado positivo y otro negativo; sin riesgo no habría oportunidad de mejores resultados. Por lo que una adecuada definición de riesgo debe reconocer tanto su causa (una variable o factor de incertidumbre) como sus

efectos (desviaciones positivas o negativas del resultado esperado). Considerando lo anterior se presentan las siguientes definiciones relacionadas con la gestión de riesgos en general:

6.1. Definiciones generales

- **Apetito por el riesgo:** Grado de riesgo que se está dispuesto a aceptar en contraprestación de un beneficio.
- **Modelo Estándar de Control Interno (MECI):** El Modelo Estándar de Control Interno (MECI) es un estándar que determina las generalidades y la estructura necesaria para establecer, documentar, implementar y mantener un Sistema de Control Interno en las entidades del Estado Colombiano.
- **Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales, la continuidad de sus operaciones, las personas, el medio ambiente y los recursos públicos.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.
- **Sistema de Control Interno:** Conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por la universidad con el fin de procurar que todas las actuaciones de la Universidad se realicen de acuerdo con las normas constitucionales, legales y estatutarias vigentes.
- **Tolerancia al riesgo:** Voluntad de correr riesgos en busca de mejores consecuencias.

6.2. Definiciones relacionadas con la gestión de riesgos

- **Comunicación y consulta:** Procesos continuos y repetitivos que la universidad realiza para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes interesadas con respecto a la gestión de riesgos.
- **Establecimiento del contexto:** Definición de los parámetros internos y externos que se deben considerar cuando se gestionan los riesgos y se establecen el alcance y los criterios de los riesgos para definir la política para la gestión de riesgos.
- **Mapa de riesgos:** Herramienta organizacional que facilita la visualización y comprensión de los riesgos y la definición de una estrategia para su gestión.
- **Marco de referencia para la gestión de riesgos:** Conjunto de componentes que brindan las bases y las disposiciones para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la institución. Incluye:
 - La política para la Gestión de Riesgos
 - Los objetivos

- Las instancias o dirección del Sistema de Gestión de Riesgos.
- Los planes, programas, rendición de cuentas, recursos, procesos y actividades.
- **Monitoreo y revisión:** Proceso de verificación, supervisión, observación crítica o determinación continua del estado del riesgo con el fin de identificar cambios en el nivel de desempeño requerido o esperado.
- **Política para la gestión de riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la Gestión de Riesgos.
- **Plan para la gestión de riesgos:** Esquema dentro del Marco de Referencia para la Gestión de Riesgos que especifica el enfoque, los componentes, y los recursos que se van a aplicar a la Gestión de Riesgos.
- **Propietarios de los riesgos:** Son los líderes de los procesos, proyectos y/o programas con sus respectivos equipos de trabajo que tienen la responsabilidad de rendir cuentas y gestionar un riesgo.
- **Proceso de gestión de riesgos:** Aplicación sistemática de las políticas, procedimientos, y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, identificación, análisis, evaluación y monitoreo y revisión de los riesgos.
- **Identificación de riesgos:** Proceso para encontrar, reconocer y describir los riesgos.

NOTA 1: La identificación implica reconocer los agentes generadores de los riesgos, los eventos, sus causas y sus efectos.

NOTA 2: La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

- **Análisis de riesgos:** Proceso para comprender la naturaleza de un riesgo. El análisis de riesgos proporciona las bases para la evaluación de riesgos y las decisiones sobre el tratamiento de los riesgos.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis de riesgos con los criterios de los riesgos, para determinar si el riesgo y su nivel son aceptables o inaceptables.
- **Tratamiento de riesgos:** Proceso para modificar los riesgos aplicando diversas medidas de tratamiento.
- **Valoración de los riesgos:** Proceso general de identificación de riesgos, análisis de riesgos y evaluación de riesgos.

7. Anotaciones y comentarios

La gestión de riesgos en la Universidad de Antioquia comienza formalmente con la Resolución Rectoral 21862 del 20 de diciembre del 2005 cuando la institución adopta el MECI 1000:2005 reglamentado mediante el Decreto 1599 del 20 de mayo de 2005. A partir

de ese momento la Universidad adelantó un proceso de diseño del sistema de gestión de riesgos el cual culmina con la publicación de la primera versión del presente Manual el 30 de septiembre de 2009.

Esta actualización al Manual se presenta a raíz del Decreto 943 del 21 de mayo de 2014 por el cual se actualiza el MECI 1000:2014 y el Decreto 1499 de 2017 con el cual se establece el Modelo Integrado de Planeación y Gestión.

8. Notas de cambio

Este documento reemplaza el Manual Institucional de Gestión del Riesgo (M-5200-001), Versión 01.

▪ **Con relación a la versión 01:**

Este documento incorpora elementos del Modelo Estándar de Control Interno – MECI, el Modelo Integrado Planeación y Gestión – MIPG, la norma ISO 31000 y las normas COSO Integrated Framework y COSO ERM Integrated Framework.

Se hace un mayor énfasis a una gestión de riesgos enfocada en los riesgos operacionales a nivel de dependencias y procesos.

▪ **Con relación a la versión 02:**

Este documento incorpora bases para la gestión de riesgos y compromisos institucionales con la gestión de riesgos, en coherencia con la política institucional de gestión integral de riesgos.

9. Bibliografía

- COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 87. (29, noviembre, 1993). Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. En: Diario Oficial. Noviembre, 1993. Nro. 41120.
- COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Marco General MIPG. Bogotá.: El Departamento, 2017.
- THE INSTITUTE OF INTERNAL AUDITORS. IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control. Altamonte Springs (Florida). The IIA, 2013. 10 p.
- LAM, James. Implementing Enterprise Risk Management. From Methods to Applications. Hoboken (New Jersey): John Wiley & Sons, 2017. ISBN 9780471745198.

- DELOITTE, 2012. Risk Assessment in Practice. Durham: Committee of Sponsoring Organizations of the Tread Way Commission. Thought Leadership in ERM.
- COSO, 2013. Internal Control Integrated Framework (Executive Summary). Durham: Committee of Sponsoring Organizations of the Tread Way Commission. ISBN 978-1-93735-239-4.
- COSO, 2004. Enterprise Risk Management - Integrated Framework (Executive Summary & Framework). Durham: AICPA.
- INTOSAI GOV 9100 Guía para las Normas de Control Interno del Sector Público. 2016. Viena, Austria: INTOSAI.
- Departamento Administrativo de la Función Pública. (2014). Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI 2014. Bogotá.
- DAFP. (2011). Guía para la Administración del Riesgo. Bogotá: Departamento Administrativo de la Función Pública (DAFP).
- DAFP. (2015). Guía para la Gestión del Riesgo de Corrupción. Bogotá: Departamento Administrativo de la Función Pública (DAFP).
- Departamento Administrativo de la Presidencia de la República. (2015). Guía para la Gestión del Riesgo de Corrupción. Bogotá.
- Deloitte. (2012). Risk Assessment in Practice (Thought Leadership in ERM). Thought Papers. Committee of Sponsoring Organizations of the Tread Way Commission (COSO).
- Mejía, R. C. (2013). Identificación de Riesgos (1st ed.). Medellín: Fondo Editorial Universidad EAFIT.
- Mejía, R. C. (2006). Administración de Riesgos. Un Enfoque Empresarial (1st ed.). Medellín: Fondo Editorial Universidad EAFIT.
- ISO. NTC-ISO31000 Gestión del Riesgo. Principios y Directrices (2009).

Elaboró: Gloria Lucia Jiménez Valdés Profesional 6 División de Arquitectura de Procesos	Revisó: Julio César García Castrillón Profesional especializado 3 División de Arquitectura de Procesos	Aprobó: John Jairo Tirado Quintero Jefe División de Arquitectura de Procesos
Fecha: 28-ENE-2019	Fecha: 01-FEB-2019	Fecha: 01-FEB-2019