Pontificia Universidad
JAVERIANA
Bogotá

RESOLUCIÓN N° 722

Manual de Gestión de Riesgos

EL RECTOR DE LA PONTIFICIA UNIVERSIDAD JAVERIANA

CONSIDERANDO:

1. Que la Pontificia Universidad Javeriana en su dinámica, actividades y procesos, que se van ajustando a las realidades cambiantes, ha visto la necesidad de incorporar un sistema de gestión que le permita atender a esos contextos dinámicos de manera oportuna y eficiente, previendo situaciones que puedan llevar a la materialización de riesgos que generan impacto en la Institución.

2. Que la gestión de riesgos ha sido concebida como parte fundamental del control interno de la Universidad, en donde se busca proveer los mecanismos para que de forma sistemática se pueda adelantar la identificación, la valoración, el control y monitoreo de los riesgos.

3. Que la gestión de riesgos se considera un elemento fundamental en los procesos y actividades de la Universidad, dado que contribuye a su mejoramiento continuo y a la generación de un ambiente adecuado de control.

4. Que el Manual de Gestión de Riesgos tiene alcance para la Sede Central.

RESUELVE:

ARTÍCULO PRIMERO. Expedir el Manual de Gestión de Riesgos, como un elemento esencial que fortalece el buen gobierno institucional y el sistema de control interno.

ARTÍCULO SEGUNDO. El Manual de Gestión de Riesgos facilitará la identificación, la valoración, el control y monitoreo de los riesgos en la Universidad

ARTÍCULO TERCERO. La presente Resolución rige a partir de su expedición.

Dado en Bogotá, D.C., el 1 de febrero de 2024.

LUIS FERNANDO MÚNERA CONGOTE, S.J.
Rector

JAIRO H. CIFUENTES MADRID
Secretario General

PONTIFICIA UNIVERSIDAD JAVERIANA

MANUAL DE GESTIÓN DE RIESGOS

2024

CONTENIDO

1. MARCO GENERAL PARA LA GESTIÓN DE RIESGOS

1.1 INTRODUCCIÓN

La Universidad Javeriana en su dinámica, actividades y procesos que se van ajustando a las realidades cambiantes, ha visto la necesidad de incorporar un sistema de gestión organizacional que le permita atender a esos contextos dinámicos de manera oportuna y eficiente, previendo situaciones que puedan llevar a la materialización de riesgos que generen un impacto en la Institución.

De acuerdo con ello, se ha tomado como guía para la elaboración del presente Manual la norma técnica ISO 31000 en la cual se establecen principios y directrices para la gestión del riesgo. Este sistema permite identificar circunstancias que puedan afectar el logro de los objetivos y continuidad de las actividades, generando análisis puntuales para determinar la calificación de los riesgos en relación con su probabilidad de ocurrencia y su impacto, y con ello entender las dinámicas requeridas por la Universidad para aplicar el tratamiento eficiente y adecuado a través de la implementación de controles que permitan su mitigación.

La gestión de riesgos ha sido concebida como parte del control interno de la Universidad en donde se busca proveer los mecanismos para que de forma sistemática se pueda adelantar la identificación, la valoración, el control y monitoreo de los riesgos, sistema que contribuye al mejoramiento continuo de los procesos y a la generación de un ambiente adecuado de control.

1.2 ALCANCE

La gestión de riesgos comprende la identificación, valoración, control, seguimiento y monitoreo de los riesgos que puedan ser identificados y que estén asociados a todas las actividades y procesos desarrollados por la Universidad en todas sus dependencias.

1.3 OBJETIVO GENERAL

Establecer la metodología de gestión de riesgos, con el propósito que la Universidad pueda dar cumplimiento a los objetivos y metas institucionales.

1.4 OBJETIVOS DEL SISTEMA DE GESTIÓN DE RIESGOS

i. Establecer una metodología que permita realizar la gestión adecuada de las diferentes etapas que se contemplan en la gestión de los riesgos.
ii. Promover la gestión proactiva en la identificación, valoración, tratamiento y monitoreo de los riesgos asociados a las actividades y procesos.
iii. Realizar seguimiento a los riesgos identificados con el fin de establecer variaciones en su impacto y/o probabilidad que afecten la estabilidad de los procesos, o el cumplimiento de los objetivos.
iv. Analizar resultados comparables entre periodos que permitan realizar la medición de su desempeño.
v. Contribuir al control interno con el fin de que se estructuren procesos que permitan que la Universidad pueda anticiparse a eventos que pueden afectar el logro de sus objetivos.
vi. Establecer una estructura de gobierno que permita sostener el sistema de gestión de riesgos en la Universidad.
vii. Fomentar una cultura de prevención y administración del riesgo de manera transversal en la Universidad.

1.5 REFERENCIAS NORMATIVAS

1.5.1 **Norma Técnica Colombiana ISO 31000 – Gestión de Riesgos:** Incorpora los principios y directrices que ayudan a que la Universidad pueda implementar un sistema de gestión de riesgos. Su objetivo es la minimización del riesgo a través de su gestión y control. Para

implementar un sistema de gestión de riesgos, la Universidad deberá considerar los siguientes elementos:

a. Análisis del contexto
b. Evaluación de los riesgos
c. Evaluación de los controles
d. Tratamiento del riesgo
e. Seguimiento y revisión

1.5.2 Modelo COSO: Herramienta que permite guiar y crear un marco para que la Universidad pueda manejar sus riesgos a través de la identificación de los siguientes componentes:

a. Ambiente de control: Evaluación de las condiciones y capacidades internas de la Universidad.
b. Evaluación de riesgos: Valoración de los riesgos en relación con la probabilidad de su ocurrencia y el impacto.
c. Actividades de control: Evaluación de políticas y procedimientos de la Universidad a la luz de su interacción con la mitigación de los riesgos que se pueden llegar a materializar.
d. Información y comunicación: Promoción de informes con información relevante para la toma de decisiones.
e. Actividades y monitoreo: Actividades que adelanta la Universidad que tienen el propósito de observar y controlar los riesgos que se pueden presentar.

1.5.3 Estándar Australiano AS/NZ 4360: Orientado a la implementación de procesos de administración de riesgos donde se involucra un contexto, la identificación de los riesgos y su valoración.

1.6 DEFINICIONES

Actividad: Acción que se lleva a cabo en cumplimiento de un propósito, tiene un principio y un fin, hacen parte de un proceso.

Amenaza: Es la posibilidad de que un evento que no ha sido planeado pueda acontecer, y debido a ello se originen consecuencias negativas.

Apetito de Riesgo: Es la cantidad de exposición al riesgo, o impacto adverso potencial de un evento, que la Universidad está dispuesta a aceptar/retener para el logro de sus objetivos de largo plazo.

Causa: Hace referencia al detonante de un evento ya sea de forma aislada o conjunta. También es conocida como falla o insuficiencia. Motivo que da origen a un riesgo.

Consecuencia: Hace referencia a cuál sería el impacto o efecto de un evento (favorable o adverso).

Control: Se refiere a toda medida tomada para mitigar o gestionar el riesgo, y para que aumente la probabilidad de que la institución / proceso logre sus metas y objetivos.

Descripción del riesgo: Es la explicación detallada de la forma en la que puede presentarse un riesgo.

Efectos del riesgo: Es la consecuencia que se genera cuando el riesgo se materializa.

Factor de riesgo: Se entiende por factores de riesgo las características, condiciones, comportamientos del entorno (interno o externo) que incrementa o reduce el riesgo. El factor de riesgo impacta en la fuente de riesgo. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los eventos externos.

Fuente de riesgo: Elemento que solo o en combinación con otro, puede generar un riesgo.

Gestión de riesgo: Actividades coordinadas para dirigir, controlar y monitorear a la Institución respecto de los riesgos identificados.

Gestionar el riesgo: Identificación, análisis y evaluación de los riesgos para determinar a través del tratamiento del riesgo (mitigarlo, eliminarlo, transferirlo o aceptarlo), si este puede modificarse para cumplir con los criterios.

Impacto: Corresponde a la evaluación del efecto y la consecuencia producida al materializarse un riesgo para la Institución.

Probabilidad: Es la variable que mide la posibilidad de que un riesgo se materialice.

Proceso: Secuencia de acciones o conjunto de actividades relacionadas de manera lógica, en donde se utilizan unos insumos o recursos para transformarlos en servicios o resultados que agregan valor en los servicios prestados.

Riesgo: Hace referencia al evento que podría ocurrir, positivo o negativo, que tenga un impacto directo sobre el logro de los objetivos. También se define como un hecho, una acción u omisión que podría afectar la capacidad de la institución para lograr sus objetivos de proceso, de negocio, o estrategias. Se puede entender como un obstáculo que impide el cumplimiento de los objetivos.

Riesgos Institucionales: Corresponden a aquellos eventos que podrían afectar la consecución de los objetivos estratégicos de la Universidad, definidos en su Planeación Estratégica. Consiste en definir por cada una de las Megas Institucionales, los riesgos que impedirían el cumplimiento de dichos propósitos, además de aquellos implícitos por la naturaleza jurídica de la institución y que per sé, se presentan en el mismo. Los riesgos institucionales estarán definidos como una única unidad de riesgos para las dos sedes.

Riesgo inherente: Riesgo asociado con la actividad económica o proceso, independientemente de los sistemas de control interno que allí se estén aplicando.

Riesgo residual: Riesgo resultante luego de evaluar los controles asociados a las actividades buscando mitigar los riesgos.

Categorías o Tipos de Riesgo[1]**:**

- **Riesgo Reputacional:** Se refiere al desprestigio de la institución que acarrea la pérdida de credibilidad y confianza en el público por fraude, insolvencia, conducta irregular de los empleados, rumores, errores cometidos en la ejecución de alguna operación por falta de capacitación del personal clave o deficiencia en el diseño de un procedimiento.

- **Riesgo Estratégico:** Tiene que ver con las pérdidas ocasionadas por las definiciones estratégicas inadecuadas y errores en el diseño de planes, programas, estructura, integración del modelo de operación con el direccionamiento estratégico y asignación de recursos.

- **Riesgo Operativo:** Consiste en la posibilidad de pérdidas ocasionales en la ejecución de los procesos y funciones de la Institución, por fallas en los procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos.

- **Riesgo Financiero:** Impactan los componentes financieros básicos de creación de valor como la rentabilidad, los ingresos y el nivel de inversión. Es el daño en los activos del proceso o en su capacidad para producir ingresos o administrar el presupuesto. Ejemplos: detrimento patrimonial, presupuesto, inventarios.

[1] Mejía Quijano, Rubi Consuelo. Administración de riesgos. Un enfoque empresarial. Editorial EAFIT. 2006.

- **Riesgo Legal:** Pérdida en caso de incumplimiento de la contraparte en un negocio y de la imposibilidad de exigirle jurídicamente el cumplimiento de los compromisos adquiridos. Error en interpretación jurídica u omisión en la documentación y en el incumplimiento de normas legales y disposiciones reglamentarias que pueden conducir a demandas o sanciones. Ejemplos: incumplimiento a normas, incumplimiento de políticas y manuales internos, incumplimiento de obligaciones y volatilidad de las normas.

- **Riesgo Tecnológico:** Hace referencia al riesgo en el uso de la tecnología como los virus, fraude, intrusiones, colapso de telecomunicaciones y riesgo que se genera con el desarrollo tecnológico que somete a la organización a cambios, en donde puede que no esté preparada para adoptarlos, y responder a las necesidades del medio. La dependencia tecnológica respecto a un proveedor. Ejemplos: ciberseguridad, infraestructura tecnológica, pérdida en el servicio y la información no confiable.

- **Riesgo Laboral:** Accidentes de trabajo y enfermedades profesionales que pueden causar daños a las personas y a la institución.

- **Riesgo Físico:** Afectan los recursos materiales; como corto circuito, explosiones, daño en equipos

- **Riesgo de Servicio**: Afectan el nivel de la calidad en la prestación del servicio. Para su identificación se involucran elementos como el cliente, el producto, la satisfacción del servicio y los tiempos de entrega del servicio.

- **Riesgo de lavado de activos:** El lavado de activos se define como "(…) el proceso mediante el cual las organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero sucio parezca limpio, haciendo que las organizaciones criminales o delincuenciales puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mimos (…)"[2].

- **Riesgo de financiación de terrorismo:** La Financiación del Terrorismo está definida por el Código Penal como aquella actividad realizada directa o indirectamente para proveer, recolectar, entregar, recibir, administrar, aportar, custodiar o guardar fondos, bienes o recursos o promover, organizar, apoyar, mantener, financiar o sostener económicamente a grupos de delincuencia organizada, o grupos al margen de la ley o sus integrantes o a grupos terroristas nacionales o extranjeros.

- **Riesgo de financiamiento de proliferación de armas de destrucción masiva:** Es todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, trasferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable[3].

- **Riesgo de Fraude:** Puede entenderse como la apropiación indebida de bienes o recursos de la Universidad mediante acciones falsas o mal intencionadas.

2. POLÍTICA DE GESTIÓN DEL RIESGO

La Pontificia Universidad Javeriana en su carácter de Institución Católica de Educación Superior fundada y regentada por la Compañía de Jesús, sin fines de lucro, con personería jurídica de derecho eclesiástico y reconocida por el Estado Colombiano para su funcionamiento y expedición de títulos universitarios, ha definido niveles y tipos de riesgo que está dispuesta a asumir prudentemente, para dar cumplimiento a la planeación, organización y control de las actividades académicas y administrativas que se derivan de la docencia, investigación y el servicio.

---

[2] Tomado de: Unidad de información y Análisis Financiero – UIAF. www.uiaf.gov.co

3 Superintendencia de Sociedades. Circular Externa 100-00004 del 2021

El Consejo Directivo Universitario es responsable de la aprobación y el Secretario General de la revisión de la Política de Gestión de Riesgo, al menos cada dos años, en donde se deberán considerar las actualizaciones que se estimen necesarias en el marco de garantizar el perfil de riesgo efectivo para la Universidad.

La Política de Gestión de Riesgo será desarrollada e implementada en toda Universidad a través de la Oficina de Riesgos y Compliance, independiente de las otras autoridades de gobierno a quienes corresponde la dirección de las actividades académicas, del medio universitario y administrativas, pero con total interacción y comunicación con estas. Esta instancia, además, llevará a cabo seguimiento a los riesgos e informará periódicamente de su evolución, elevando las propuestas que considere adecuadas para su mejor desarrollo. Para el desarrollo de las actividades se dispondrá de los recursos que considere necesarios.

3. ASPECTOS DE LA GESTIÓN DEL RIESGO

Dentro de la estructura de la gestión del riesgo, la Universidad incorporará el "Modelo de las tres líneas de Defensa"[4], el cual está enfocado en que las organizaciones deben considerar roles necesarios para un gobierno corporativo eficaz que ayude a fomentar el éxito a través de la comprensión profunda de los roles y su interacción para el respaldar el logro de los objetivos.

A continuación, se presenta la interacción de las tres líneas de defensa y los proveedores externos de aseguramiento dentro de una estructura de gobierno:

De acuerdo con el anterior modelo, la Universidad lo incorporará así:

3.1 Primera Línea de Defensa

Estará a cargo de la primera línea de defensa la Rectoría, Secretaría General, Vicerrectoría Administrativa, Vicerrectoría Académica, Vicerrectoría del Medio Universitario, Vicerrectoría de Investigación, Vicerrectoría de Extensión y Relaciones Interinstitucionales, Facultades e Institutos, cada una de ellas con las unidades y dependencias que los componen.

Tendrán a cargo las siguientes responsabilidades relacionadas con la gestión del riesgo:

[4] El Modelo De Las Tres Líneas Del IIA 2020.

a. Identificar, valorar y evaluar los riesgos asociados a los procesos y actividades que lleva a cabo cada unidad.
b. Validar que los riesgos identificados estén asociados con los objetivos
c. Identificar y definir los controles asociados a cada uno de los riesgos
d. Realizar el seguimiento y monitoreo de los riesgos y los controles con el fin de mantener la matriz de riesgo actualizada
e. Identificar planes de acción que permitan fortalecer la gestión de los controles y la mitigación del riesgo
f. Identificar riesgos materializados e identificar planes de acción asociados a su contención y un posterior tratamiento
g. Realizar la actualización de las matrices de riesgo por lo menos una vez cada dos años.

3.2 Segunda Línea de Defensa

Estará a cargo la segunda línea de defensa la Oficina de Riesgos y Compliance, que con su equipo tendrá la función de apoyar y supervisar los elementos asociados a la gestión del riesgo en las unidades, incluyendo el acompañamiento en la actualización de las matrices, implementar elementos enfocados a la mejora continua y realizar el seguimiento a la identificación y ejecución de controles y su desarrollo.

Cada dos años presentará informes sobre la eficacia y eficiencia del programa de gestión de riesgos de la Universidad ante el Secretario General. Así mismo, cuando éste lo estime pertinente, se presentará un informe ante el Comité de Auditoría o Comité de Rectoría.

Así mismo, harán parte de ésta línea las unidades que lideren los controles de riesgo financiero, de seguridad, calidad y cumplimiento.

3.3 Tercera Línea de Defensa

La tercera línea de defensa será liderada por el Comité de Auditoría y la Auditoría Interna, quienes tendrán a cargo las siguientes responsabilidades:

a. Realizar la evaluación a los procesos de la Universidad identificando riesgos y controles asociados y su eficiencia y efectividad
b. Realizar recomendaciones a través de las oportunidades de mejora que sean identificadas en los procesos
c. Realizar seguimiento a la aplicación de planes de acciones definidos con los líderes de procesos y unidades
d. Asesorar al Rector y al Consejo Directivo Universitario en materia de controles y del fortalecimiento del sistema de control interno

Es esencial que la tercera línea de defensa sea independiente dentro del desarrollo de sus actividades, fomentando la objetividad, autoridad y credibilidad.

3.4 Proveedores de Aseguramiento Externo

Como parte del aseguramiento externo, la Universidad cuenta con una Revisoría Fiscal el cual tiene a cargo funciones de validación y evaluación independiente a diferentes procesos de la Universidad, estando en la obligación de atender las solicitudes puntuales para cerrar el ciclo de aseguramiento.

4. MARCO OPERATIVO PARA LA GESTIÓN DEL RIESGO

El modelo de gestión de riesgos adoptado por la Universidad Javeriana se fundamenta en lo dispuesto por la Norma Tánica Colombiana NTC ISO 31000, la cual sugiere una gestión de riesgo basada en el establecimiento del contexto estratégico del riesgo, la valoración y tratamiento, seguido por el monitoreo y comunicación, como se muestra a continuación:

4.1 Interacción entre los riesgos institucionales y los riesgos operativos

La identificación de los riesgos institucionales debe ser realizada por el equipo directivo de la Universidad en donde se establece una gestión integral entre la Sede Central y la Seccional de Cali. Los riesgos institucionales definidos y valorados deben presentarse al Consejo Directivo Universitario. Estos riesgos deberán de ser actualizados cada dos años.

Los riesgos institucionales parten de las Megas definidas en el Plan Estratégico Institucional. Estos riesgos están relacionados con los riesgos de procesos y de las actividades, los cuales son identificados a partir de los objetivos de cada una de las unidades de la Rectoría y de las Vicerrectorías. Los objetivos de cada una de las unidades están relacionados con el cumplimiento de las Megas.

Los controles están definidos en cada uno de los riesgos operativos identificados, los cuales ayudan a mitigar su materialización.

La Auditoria Interna, ayudará al monitoreo y seguimiento de la adecuada ejecución de los controles dentro de la institución.

4.2 Factores internos y externos en la gestión de riesgos

El marco de la gestión de riesgos se establecen las condiciones internas y del entorno que pueden generar eventos que afecten el cumplimiento de la misión y objetivos de la Universidad. De acuerdo con ello, a continuación, se describen algunos factores internos como externos que deben ser considerados al realizar el análisis de los riesgos:

Externo	Interno
Sociales: Demografía, responsabilidad social, acciones insurgentes, crisis de valores, desempleo, protestas, paros, pandemias.	**Recurso humano:** Comunidad Educativa Javeriana, conformada por estudiantes, profesores, personal administrativo, egresados.
Económicos: Disponibilidad de capital, liquidez, competencia, financiación y cambios en la solvencia, valor de mercado de una cartera de activos, movimientos desfavorables de los tipos de interés.	**Cultura:** Pluralismo ideológico y el ecumenismo religioso que caracteriza la comunidad educativa javeriana.
Medio Ambientales: Agentes contaminantes físicos, químicos, biológicos por causas naturales o derivado de actividades humanas.	**Procesos:** Capacidad, diseño, ejecución, proveedores, entradas, actividades, salidas, conocimiento, relaciones contractuales
Políticos: Cambios y decisiones políticas de los gobiernos, políticas fiscales, políticas	**Tecnología y sistemas de información:** Integridad de datos, disponibilidad de datos y sistemas.

monetarias, conflicto armado, intereses de grupos empresariales locales o nacionales.	
Tecnológicos: Interrupciones, producción, datos externos, tecnología, obsolescencia.	**Organización:** Estructuras organizacionales de las Vicerrectorías, autoridades de colegiadas y de gobierno con atribuciones y proceso de toma de decisiones definido por los estatutos de la Universidad.

4.3 Eventos de Riesgo

Un evento de riesgo es una situación que podría ocurrir en un lugar particular en un momento determinado y que puede llevar a su materialización. Son eventos de riesgo aquellos que tienen un impacto significativo en el logro de las estrategias institucionales, provocando pérdidas económicas o reputacionales, entre otras.

Los eventos de riesgo podrán tipificarse de la siguiente forma:

Evento (Nivel 1)	Descripción	Evento (Nivel 2)
1. Fraude interno	Actos intencionales que buscan apropiarse indebidamente de recursos de la Universidad.	1.1 Actividades no autorizadas 1.2 Hurto y Fraude
2. Fraude Externo	Actos realizados por clientes o terceros que buscan apropiarse indebidamente de activos o de información confidencial de la Universidad.	2.1 Hurto y Fraude 2.2 Vulnerabilidad de los sistemas
3. Relaciones laborales	Actos incompatibles con la legislación laboral, con la reglamentación interna formulada sobre este aspecto y en general con la normatividad vigente sobre la materia.	3.1 Fallas en las relaciones laborales 3.2 Fallas en la seguridad del entorno laboral 3.3 Discriminación
4. Clientes	Omisiones voluntarias o involuntarias de las obligaciones con los clientes de la Universidad que impidan constituir una obligación profesional frente a estos.	4.1 Administración indebida de activos y revelación de información del cliente 4.2 Prácticas inapropiadas de negocios o de mercado 4.3 Fallas en los productos 4.4 Fallas en la selección y gerenciamiento de los clientes 4.5 Fallas en la asesoría a los clientes
5. Daños de activos Físicos	Pérdidas ocasionadas por daños o perjuicios a los activos fijos de la institución tanto por personas internas o externas.	5.1 Desastres y otros eventos
6. Fallas tecnológicas	Interrupciones voluntarias o involuntarias de los servicios tecnológicos e informáticos que afecten el funcionamiento académico y administrativo de la Universidad.	6.1 Fallas en los sistemas 6.2 Ciberataques 6.3 Incidentes de seguridad

Evento (Nivel 1)	Descripción	Evento (Nivel 2)
7. Ejecución y administración de procesos	Pérdidas ocasionadas por omisiones voluntarias o involuntarias en la ejecución de los procesos.	7.1 Fallas en el diseño, ejecución y mantenimiento de los procesos 7.2 Inoportunidad o inexactitud en la generación de información y reportes 7.3 Ausencia de documentación o documentación incompleta de los clientes 7.4 Inadecuada administración de las cuentas de clientes 7.5 Fallas de contrapartes comerciales 7.6 Fallas de proveedores o outsourcing
8. Lavado de activos	Posibilidad de pérdida o daño que puede sufrir la Universidad de ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.	
9. Reputacional	Pérdida en que se incurre por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.	
10. Legal	Probabilidad de ocurrencia de daños o perjuicios como consecuencia de: - Imposibilidad para ejercer los derechos radicados en cabeza de la Universidad, o exigir el cumplimiento de obligaciones en cabeza de terceros, por ausencia del cumplimiento de los requisitos legales; - Actuaciones de funcionarios de la Universidad sin facultad estatutaria, reglamentaria o legal para vincular a la Universidad; - Incumplimiento de leyes, pronunciamientos judiciales y administrativos, hechos, negocios y/o actos jurídicos, y de normas internas; - Aplicación errada de la ley o errores en la interpretación de la misma; - Falta de aplicación oportuna de los cambios normativos; - Falta de respuesta a requerimientos de las autoridades.	

4.4 Apetito de Riesgo

Corresponde al nivel de riesgo que la Universidad quiere aceptar, aquel con el que se siente cómoda. Se basa en la interacción entre los diferentes riesgos asociados a sus objetivos estratégicos y sus capacidades internas y externas para manejar dichos riesgos.

El Apetito de Riesgo se define y/o actualiza en la Universidad cada dos años, teniendo en cuenta que éste es la relación riesgo / retorno que desea asumir de acuerdo con su situación actual y el dinamismo del mercado en el cual actúa la Institución.

El apetito de riesgo puede ser definido con base en los siguientes criterios: ingresos operacionales, ingresos totales, patrimonio total, patrimonio promedio, excedentes del ejercicio y Ebida.

4.5 Criterios para la gestión de riesgos

Los criterios adoptados por la Universidad para gestión de riesgos están clasificados de la siguiente forma:

Clasificación	Frecuencia	Impacto
Nivel	Alta Frecuente Moderado Ocasional Remoto	5. Muy Alto 4. Alto 3. Moderado 2. Bajo 1. Mínimo

Los criterios que se detallan en la tabla anterior, deberán ser revisados y actualizados por lo menos una vez cada dos años y cuando se considere necesario según los eventos o evaluaciones posteriores.

Los criterios serán incluidos en el análisis de riesgos durante la definición de frecuencia e impacto de cada riesgo de acuerdo con el soporte de calificación registrado en la matriz.

4.5.1 Clasificación del Criterio de Impacto

A continuación, se describe la clasificación del impacto de ocurrencia del riesgo y sus categorías:

IMPACTO	FINANCIERO	CUMPLIMIENTO	REPUTACIONAL	OPERACIONAL
5. INACEPTABLE	Más de $13.855 millones	Intervención administrativa de la Universidad por parte de los órganos de control y vigilancia por incumplimientos legales y/o contractuales	El hecho tiene despliegue de alta cobertura en redes sociales, medios masivos de comunicación a nivel nacional y/o internacional	Inhabilidad para operar los procesos misionales mayor a 2 días
4. MAYOR	De $4.381 millones hasta $13.855 millones	Sanciones o multas impuestas por órganos de control y vigilancia por incumplimientos legales, contractuales y/o medio ambiente e infraestructura	El hecho tiene despliegue en la comunidad educativa y partes interesadas con cobertura en redes sociales y medios masivos a nivel nacional	Inhabilidad para operar los procesos misionales de la Universidad hasta por 2 días
3. MODERADO	De $1.385 millones hasta $4.381 millones	Observaciones o solicitudes de aclaración por parte de los órganos de control y vigilancia con plazo para cumplimiento de acciones	El hecho tiene despliegue en la comunidad educativa y partes interesadas con cobertura en redes sociales	Inhabilidad para operar los procesos misionales por menos de 4 horas y/o procesos de apoyo entre 1 y 2 días
2. BAJO	De $438 millones hasta $1.385 millones	Solicitud de aclaraciones por parte de entes de control u otras entidades por incumplimientos legales, contractuales y/o medio ambiente	El hecho tiene despliegue en la cominidad educativa sin cobertura en redes sociales	Inhabilidad para operar los procesos de apoyo o de la Universidad hasta por 12 horas
1. MÍNIMO	Hasta $438 millones	Quejas y solicitud de aclaración interna por parte de la comunidad educativa por incumplimientos de políticas y lineamientso internos	El hecho tiene despliegue a nivel administrativo	Inhabilidad para operar los procesos de apoyo o de la Universidad por menos de 4 horas

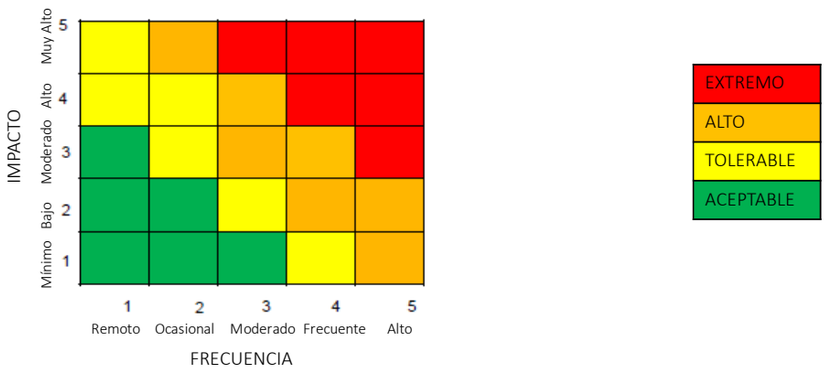
4.5.2 Clasificación del Criterio de Frecuencia

A continuación, se describe la clasificación de la frecuencia de ocurrencia del riesgo y sus categorías:

NIVEL	FRECUENCIA
Alta	Se puede presentar más de 12 veces al año
Frecuente	Se puede presentar hasta 12 veces al año
Moderada	Se puede presentar hasta 4 veces al año
Ocasional	Se puede presentar 1 vez al año
Remota	Se puede presentar menos de una vez al año

4.6 Mapa de Calor

El mapa de calor que ha sido adoptado por la Universidad es una matriz de 5 X 5, la cual se encuentra dividida en cuatro colores, así:



Explicación de la colorimetría[5]:

- **Riesgo Extremo:** Riesgo representado en color rojo. Es una situación que es inaceptable para la Universidad, dado que representa un grave peligro, pues su frecuencia y su impacto es alto. Las medidas de tratamiento deben ser inmediatas, debido a que si el peligro se materializa la estabilidad de la institución puede verse afectada debido a la gravedad de las pérdidas.

- **Riesgo Alto:** Riesgo representado en color anaranjado. Es una situación a la cual debe prestársele atención, debiendo generar planes de acción a corto plazo.

- **Riesgo Tolerable:** Riesgo representado en color amarillo. Es una situación que no representa un alto peligro para la Institución, sin embrago, es importante que se generen planes de mediano plazo.

- **Riesgo Aceptable**: Riesgo representado en color verde. Son situaciones en las cuales la Institución no debería desarrollar medidas de prevención o protección frente a los riesgos analizados.

4.7 Severidad del Riesgo: Clasificación del riesgo de acuerdo con el impacto y frecuencia

IMPACTO	FRECUENCIA	SEVERIDAD DEL RIESGO
Muy Alto	Moderada	Extremo
Muy Alto	Frecuente	
Muy Alto	Alta	
Alto	Frecuente	
Alto	Alta	
Moderado	Alta	
Muy Alto	Ocasional	Alto
Alto	Moderada	
Moderado	Moderada	
Moderado	Frecuente	
Bajo	Frecuente	
Bajo	Alta	
Mínimo	Alta	
Muy Alto	Remota	Tolerable
Alto	Remota	
Alto	Ocasional	
Moderado	Ocasional	
Bajo	Moderada	
Mínimo	Frecuente	
Moderado	Remota	Aceptable

[5] Mejía Quijano, Rubi Consuelo. Administración de riesgos. Un enfoque empresarial. Editorial EAFIT. 2006.

Bajo	Remota	
Mínimo	Remota	
Bajo	Ocasional	
Mínimo	Ocasional	
Mínimo	Moderada	

5. METODOLOGÍA PARA LA IDENTIFICACIÓN Y GESTIÓN DE RIESGOS

5.1 Identificación del Riesgo

Para la identificación de los riesgos el área responsable deberá conformar un equipo interdisciplinar que pueda dar cuenta de los eventos de riesgo que podrían tener un impacto en el objetivo del proceso que se analiza.

En las sesiones que se conformen, podrán considerar los siguientes aspectos:

- La participación del líder del proceso, ejecutores, clientes o usuarios del proceso, así como proveedores quienes podrán aportar una visión global de los riesgos y favorecer la identificación de causas y consecuencias.

- Como base para la identificación de los riesgos deberá elaborarse la caracterización del proceso, de forma que pueda contextualizarse sobre el objetivo, alcance, actividades, entradas, salidas y partes interesadas del proceso sujeto de análisis.

- La lista de los riesgos debe ser exhaustiva de forma que se contemple eventos que podría crear, aumentar, prevenir, degradar acelerar o retrasar el logro de los objetivos.

- La identificación debe incluir los riesgos independientemente de si su origen está o no bajo control del área.

- Definir las fuentes de riesgo, áreas de impacto y eventos, causas y consecuencias potenciales.

- Debe influir efectos o consecuencias particulares, incluyendo efectos en cascada y acumulativos.

- Identificar las causas y los escenarios posibles que muestren que las consecuencias se podrían presentar

- Considerar todas las causas y consecuencias significativas.

De acuerdo con lo anterior, se deberá llegar a redactar una descripción completa del riesgo identificado, identificando el agente generador y las causas del mismo. Es importante que se tenga en cuenta que un solo riesgo puede tener asociada una o más causas, por lo cual se podrán a consideración todas ellas.

5.1.1 Elementos de la identificación del riesgo:

Son elementos que permiten identificar el riesgo, los siguientes:

- Macroproceso al cual está asociado
- Proceso al cual está asociado
- Tipo de riesgo
- Descripción del riesgo
- Agente generador (recurso humano, proceso, tecnología, evento externo)
- Causas

5.2 Valoración del riesgo: evaluación del riesgo inherente

Implica la consideración de las fuentes de riesgo y las consecuencias positivas y negativas de cada uno de ellos. El análisis se realiza en la perspectiva de valoración del riesgo inherente, de acuerdo con la valoración de la frecuencia, entendida como la posibilidad de que el evento ocurra, y el impacto, el cual determina el efecto de la ocurrencia. Para realizar la valoración se deberá tener en cuenta la información interna, externa, cualitativa y cuantitativa asociada al riesgo y a su materialización.

Para realizar un análisis y valoración se tendrá en cuenta la clasificación del criterio de impacto y la clasificación del criterio de frecuencia.

La valoración de riesgos permite establecer su grado de severidad con el fin de establecer prioridades y acciones tendientes a prevenir su ocurrencia o mitigar sus efectos.

Una vez el riesgo ha sido valorado, se tendrá el resultado de su ubicación en el mapa de calor de riesgos inherentes.

Para la valoración del riesgo se tendrá que tener en cuenta el mapa de calor, y la clasificación del riesgo de acuerdo con el impacto y frecuencia relacionado en el presente manual.

5.3 Tratamiento del Riesgo:

5.3.1 Identificación de controles

Con el propósito de mitigar la posible materialización de los riesgos identificados, la Universidad deberá aplicar medidas de prevención y de control que estén enfocadas a disminuir la probabilidad del impacto y de la frecuencia en el evento en el que el riesgo se llegue a materializar.

De acuerdo con lo anterior, la matriz de riesgo deberá contemplar aquellos controles que permitan mitigar los riesgos identificados, por lo cual se deberá establecer: i) la metodología para definir las medidas de control; ii) las medidas de control y iii) el perfil del riesgo residual. La Universidad deberá decidir si transfiere, acepta, mitiga o evita el riesgo en los casos en que ello sea posible.

5.3.2 Características de los controles:

Las opciones de tratamiento de los riesgos, también llamados controles, deberán tener las siguientes características[6]:

- Deben ser suficientes, es decir que deben implementarse aquellos que son necesarios, ni muchos que entorpezcan la operación ni pocos que sean insuficientes para la mitigación del riesgo.
- Comprensibles: Deben ser claros y sencillos, fáciles de interpretar.
- Económicos: El costo de la implementación del control debe ser menor que el beneficio que está aportando.
- Eficaz: Debe permitir detectar el riesgo y disminuir su probabilidad de ocurrencia o su impacto.
- Oportuno: Deben actuar en el momento en que efectivamente son necesarios.
- Dentro del proceso: Deben hacer parte del proceso.

Los controles pueden ser de diferentes tipos[7]:

- Manuales: Realizados por las personas
- Automatizados: Parametrizados a través de sistemas tecnológicos
- Obligatorios: Establecidos en las leyes o normas
- Voluntarios: Se requieren y se aplican de manera voluntaria para el manejo de los riesgos

[6] Mejía Quijano, Rubi Consuelo. Administración de riesgos. Un enfoque empresarial. Editorial EAFIT. 2006.
[7] Mejía Quijano, Rubi Consuelo. Administración de riesgos. Un enfoque empresarial. Editorial EAFIT. 2006.

- Preventivos: Acción sobre la causa del riesgo y del agente generador, para disminuir la probabilidad de ocurrencia
- Detectivos: Alarma que se acciona cuando se descubre una situación no normal
- Correctivos: Corrigen desviaciones y previenen nuevamente la ocurrencia

El tratamiento de los riesgos deberá estar asociado a planes de acción y a su seguimiento, toda vez que se debe realizar una evaluación por lo menos una vez al año para validar que los controles estén generando, sobre el riesgo y su causa, el efecto correcto para mitigarlo previniendo su materialización.

5.3.3. Elementos de los controles

Se deberán identificar los siguientes elementos para cada uno de los controles definidos:
- Descripción completa del control (preventivo, detectivo, correctivo)
- Tipo de control Periodicidad (diario, semanal, quincenal, mensual, bimensual, trimestral, semestral, anual, esporádico, cuando se requiera)
- Naturaleza (manual, automático o que depende de tecnologías de la información)
- Diseño
- Funcionalidad

5.3.4 Evaluación de los controles

Para realizar la evaluación del control se deberá tener en cuenta la cobertura y la oportunidad, dado que estos criterios llevan a determinar la eficiencia del control.

La cobertura es evaluada con relación al riesgo que está mitigando; es importante para realizar esa evaluación con un enfoque que esté dirigido a la disminución del impacto y/o de la frecuencia del riesgo identificado. En el evento en que se evidencie que el control definido no permite reducir el impacto o la frecuencia del riesgo, se deberá establecer un nuevo control o controles complementarios sobre el riesgo.

La oportunidad del control se refiere a los elementos que permiten establecer su calificación dentro del proceso con base en los siguientes elementos: i) ejecución efectiva del control, ii) diseño y funcionalidad del control dentro del proceso; iii) si la ejecución del control se está llevando a cabo conforme a los procedimientos y actividades asociadas a su diseño; iv) si hay una asignación de responsable; iv) si su periodicidad es adecuada y v) evaluar el propósito y determinar si es adecuado.

Con el fin de que se pueda llevar a cabo una evaluación completa del control, es importante que se cuente con el equipo que tenga experiencia en el desarrollo del proceso, con el fin de que puedan ser identificados los controles y sus elementos asociados, permitiendo realizar una evaluación objetiva para establecer su efectividad.

5.3.5 Opciones de Tratamiento del Riesgo

Las opciones de tratamiento del riesgo que la Universidad considera, son las siguientes:

- Evitar: Eliminar las actividades que generan el riesgo. Con esta acción se elimina la consecuencia y la probabilidad de ocurrencia del riesgo evaluado.

- Reducir: Se deben llevar a cabo acciones para disminuir la probabilidad de ocurrencia y su impacto.

- Compartir y/o transferir: Se busca la disminución de la probabilidad de ocurrencia y su impacto sin que ello implique la eliminación de la actividad de riesgo que genera el riesgo, dado que se está trasladando o compartiendo el riesgo.

- Aceptar: La organización acepta el riesgo, lo que implica que no se ejecute acciones en relación con la probabilidad o el impacto; se asume la exposición al riesgo.

5.4 Evaluación del Riesgo Residual

El riesgo residual es aquel riesgo que se identifica después de que se han implementado los controles. Para realizar la evaluación del mismo, es necesario contar con la información sobre la solidez de los controles asociados y la efectividad del control en relación con su aplicación. Se valida si el riesgo inherente disminuye en su frecuencia y/o en su impacto.

En el ámbito del riesgo residual se incluirá la evaluación de aquellos eventos de riesgo que se han materializado.

5.5 Materialización del riesgo

En el evento en que un riesgo se materialice, éste podrá ser identificado por el líder del área o el responsable del proceso y también a través de la Auditoría Interna.

Una vez se ha identificado la materialización, el responsable del proceso o líder de área deberá:

i. Identificar las actividades tendientes a contener los efectos del riesgo materializado;
ii. Establecer un plan de choque que permita continuar con las actividades asociadas al proceso;
iii. Identificar acciones de mejora que puedan ser incorporadas al plan de acción enfocadas a la mitigación y prevención de la materialización del riesgo nuevamente;
iv. Identificar si se requiere una actualización de la matriz de riesgos y
v. Validar la pertinencia, diseño y funcionalidad de los controles asociados al riesgo.

Los riesgos materializados deberán tener un seguimiento, a efectos de evaluar su evolución y mitigación en relación con los planes de acción definidos.

5.6 Monitoreo, revisión y actualización de riesgos

El seguimiento de los riesgos, la evaluación de la efectividad del plan de acción previsto para los riesgos identificados, las estrategias y, en general, la gestión de riesgos, deberán ser revisados anualmente para identificar:

- Cambios en el factores externos o internos que afecten a la Universidad
- Cambios en las necesidades o expectativas de las partes interesadas
- Materialización de eventos que no se tienen identificados en los procesos y tuvieron una afectación negativa en la operación
- Nuevos riesgos institucionales o cambios a los existentes.
- Cambios en los procesos que puedan afectar el cumplimiento de los objetivos (políticas, cambios regulatorios, cambios en sistemas de información, entre otros)
- Directrices provenientes de los órganos de administración y control en materia de gestión de riesgos.
- Recomendaciones provenientes del ejercicio de auditoría interna.
- Lecciones aprendidas a partir de los eventos, cambios, tendencias, éxitos y fracasos.

La identificación y valoración de todos los riesgos de la matriz de riesgos de cada una de las áreas de la Universidad deberán actualizarse por lo menos una vez cada dos años; el seguimiento a los planes de acción, de acuerdo con los cronogramas y medidas de desempeño determinados de forma que permitan definir la efectividad de los controles es esencial en la gestión de riesgos, por lo cual cada área estará a cargo de realizar el seguimiento a sus planes de acción bajo el compromiso de cumplimiento de los mismos en las fechas que establezca cada una de las unidades.

Todas las áreas deberán reportar a través del informe de gestión anual la gestión que se ha realizado con respecto a los riesgos identificados y los controles implementados.

Así mismo, cada dos años la Oficina de Riesgos y Compliance deberá presentar un informe al Secretario General sobre el análisis general de los riesgos a nivel transversal en la Universidad. Adicionalmente, cuando éste lo estime pertinente, se presentará un informe ante el Comité de Auditoría o Comité de Rectoría.

6. SENSIBILIZACIÓN Y CAPACITACIÓN

La Universidad entiende que la gestión de riesgos hace parte esencial del desarrollo de la operación de la Universidad, por lo cual, se incorporará dentro del proceso de inducción un curso general de conceptos sobre gestión del riesgo y el modo de actuar de la Universidad en ellos, y adicionalmente, un curso que será promovido anualmente para todos los empleados de la Universidad en donde se les sensibilizará sobre los principales conceptos de riesgos y controles.