MANUAL DE GESTION DE RIESGOS

UNIVERSIDAD DE LOS ANDES

Contenido

1. DISPOSICIONES GENERALIDADES

1.1. Introducción

Dando alcance a la Política de Gestión de Riesgos aprobada por el Comité Directivo, se estructuró el presente Manual de Gestión de Riesgos, el cual se encuentra alineado a la metodología para el mantenimiento del sistema de control interno de la Universidad, buscando proveer los mecanismos para la identificación, valoración, tratamiento y seguimiento de los riesgos, contribuyendo a la mejora continua de los procesos académicos y administrativos, y al cumplimiento de los objetivos Institucionales.

1.2. Alcance

El alcance de este manual cubre todos los procesos académicos y administrativos y aplica para cualquier miembro de la Universidad que realice o tenga riesgos a su cargo, incluyendo la participación o relación en cualquiera de las etapas de los procesos de gestión de riesgo contempladas en este manual.

1.3. Objetivo

Proporcionar guías, procedimientos y formatos, para la adecuada gestión de riesgos, asegurando mejora y optimización de los procesos, así como generando valor a nivel Institucional.

Por otra parte, el manual busca: a) ser un mecanismo de capacitación para cualquier miembro de la universidad y demás vinculados que gestionen riesgos en la ejecución de sus proceso y b) fomentar la calidad al momento de la identificación, valoración, tratamiento y seguimiento de los riesgos, mediante:

- Reducir la probabilidad de incumplimientos de los objetivos Institucionales mediante la gestión proactiva de los riesgos.
- Asignar eficazmente los recursos y responsabilidades para el tratamiento de los riesgos.
- Definir políticas, procedimientos y metodologías estructuradas.
- Determinar las acciones adecuadas para el tratamiento del riesgo *(aceptar, perseguir, reducir, trasladar o evitar),* esperando el menor impacto posible.
- Garantizar que los riesgos sean gestionados de forma oportuna, eficiente y al menor costo posible.

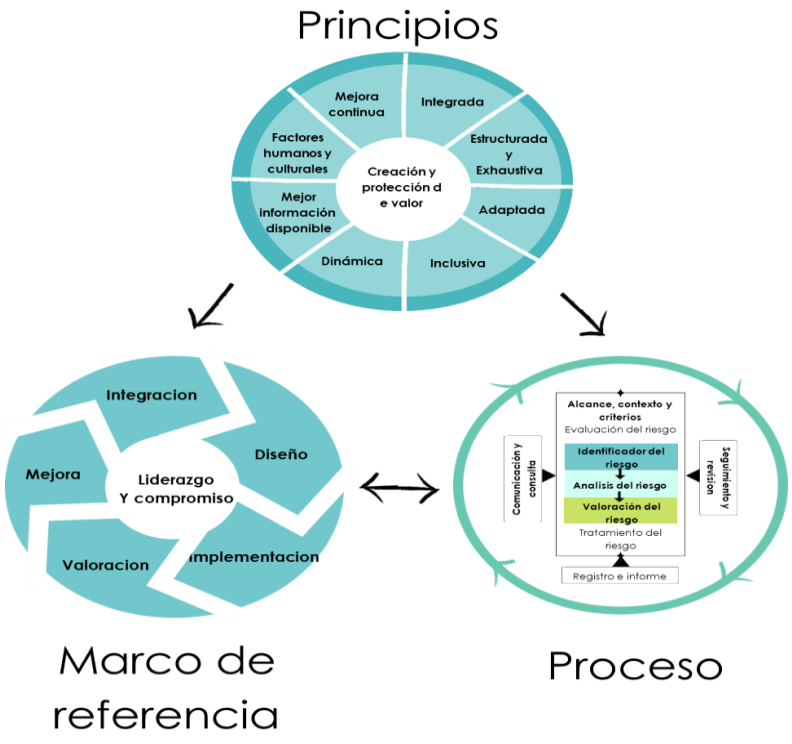
1.4. Marco de referencia

La Universidad para la implementación del SGR reconoce y aplica marcos de referencia y normativas internacionales, tales como:

1.4.1. ISO 31000:2018

La cual recoge una serie de buenas prácticas internacionales que proporcionarán la eficiente gestión de los riesgos a todos los niveles, publicada por el International Organization for Standardization (ISO).

Esta norma establece principios y directrices que ayudan al diseño, la implementación, la operación, el mantenimiento y la revisión del SGR, encaminado a la mejora continua. La componen 8 principios, un marco de referencia y un proceso, relacionados entre sí, de la siguiente manera:



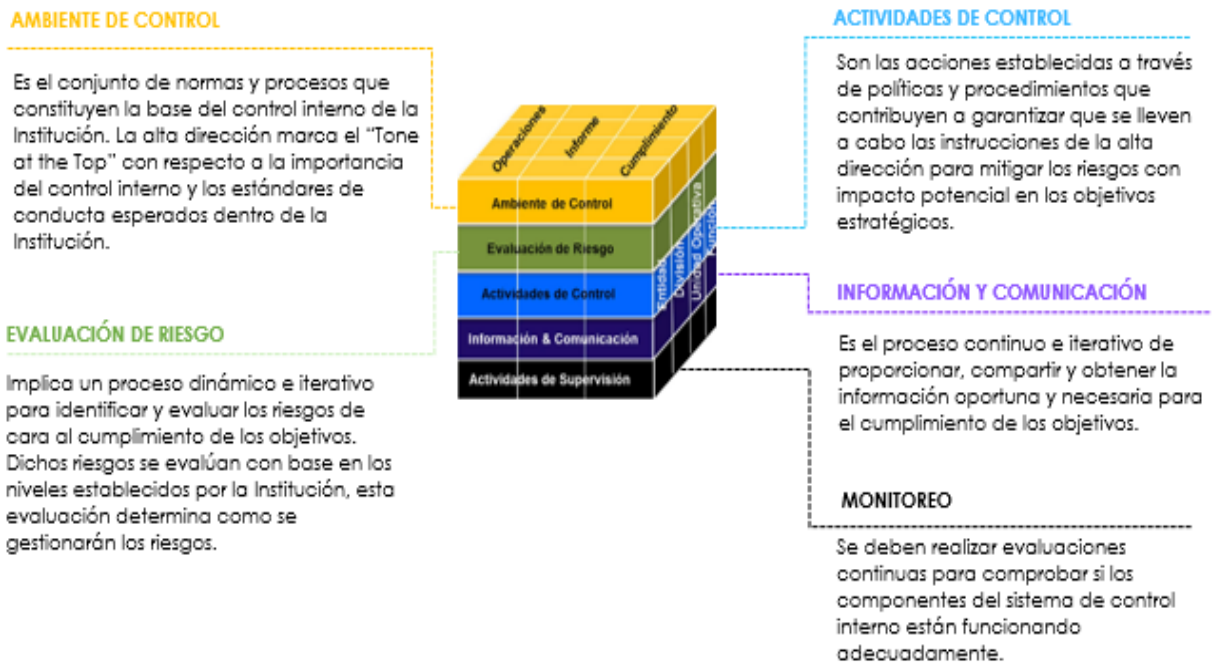
Gráfica 1. ISO 31000:2018 (International Organization for Standardization (ISO), 2018)

1.4.2. Marco COSO

The Committee of Sponsoring Organizations of the Treadway Comisión, por sus siglas en ingles COSO, fue constituido con el objetivo de proporcionar liderazgo frente a la gestión del riesgo empresarial (ERM), el control interno, y la disuasión del fraude.

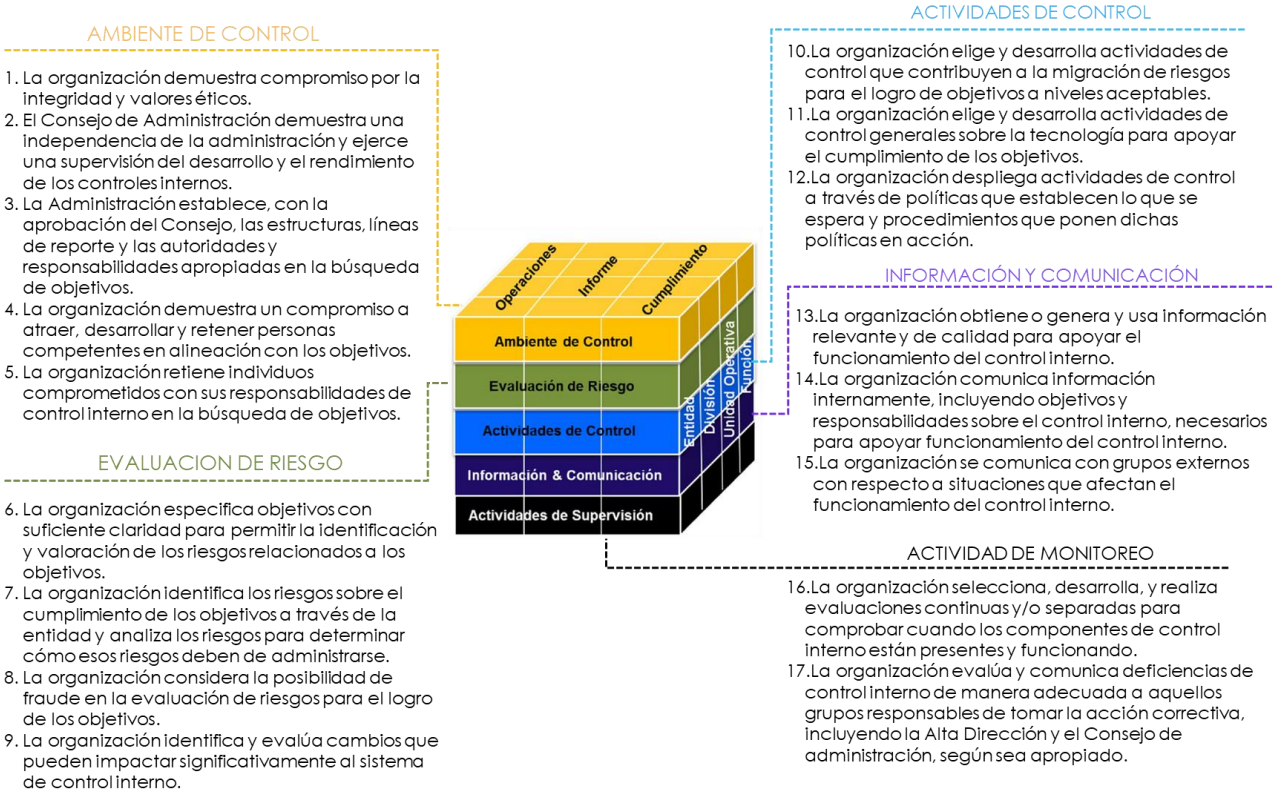
El marco COSO 2013, ofrece a la Institución las guías necesarias para la implementación y mantenimiento del control interno. Este Marco establece 5 componentes enmarcados en 17 principios, con una relación integral que debe estar presente en todos los niveles de la Institución, de la siguiente forma:

Componentes COSO



Gráfica 2. Componentes COSO (Committee of Sponsoring Organizations of the Treadway commission (COSO), 2013)

Relación de los principios - componente



Gráfica 3. Relación principio-componente COSO (Committee of Sponsoring Organizations of the Treadway commission (COSO), 2013)

La implementación y mantenimiento de los 5 componentes y los 17 principios proporcionan una seguridad razonable para el cumplimiento de los objetivos Institucionales, cubriendo aspectos fundamentales del ambiente de control, la evaluación del riesgo, las actividades de control, las actividades de monitoreo y lo relacionado con la información y la comunicación dentro de la Institución.

Teniendo en cuenta que el modelo COSO ERM 2004 fue actualizado en el año 2017 mediante el Modelo COSO ERM 2017, este último se fundamenta en la identificación y gestión de los riesgos estratégicos y la importancia de la generación de valor. La Universidad toma como referencia los dos modelos (COSO 2013 – COSO ERM 2017).

Este marco establece 5 componentes y 20 principios relacionados así:

Gráfica 4. Marco COSO 2017 (Committee of Sponsoring Organizations of the Treadway commission (COSO), 2017)

El Marco COSO ERM 2017 proporciona orientaciones generales para posicionar y establecer la gestión del riesgo en la planificación estratégica, logrando su integración en todos los niveles de la Institución, ya que los componentes y principios definidos cubren todos los aspectos, desde el gobierno hasta el monitoreo, recalcando siempre la influencia que tienen los riesgos en la estrategia, desempeño y sus funciones en todas las unidades académicas y administrativas de la Institución.

1.4.3. ISO 27001

La norma ISO 27001 es un marco normativo de seguridad tecnológica, la cual establece una serie de recomendaciones, lineamientos y controles que buscan el aseguramiento de los datos, así como contribuir con la confidencialidad, integridad y disponibilidad de la información. Dentro de esta norma se encuentra el Anexo A, el cual registra una serie de controles cuya implementación contribuye con la seguridad de la información, para lo cual la Universidad valida la pertinencia de la aplicación de estos

controles y los implementa según el nivel de riesgo al que este expuesto, la capacidad y recursos Institucionales.

1.4.4. COBIT

La Asociación de Auditoría y Control de Sistemas de Información o ISACA por sus siglas en inglés, publica constantemente actualizaciones del marco COBIT, que tienen como objetivo principal el desarrollo de políticas y buenas prácticas para la seguridad y el control de Tecnología de Información (TI).

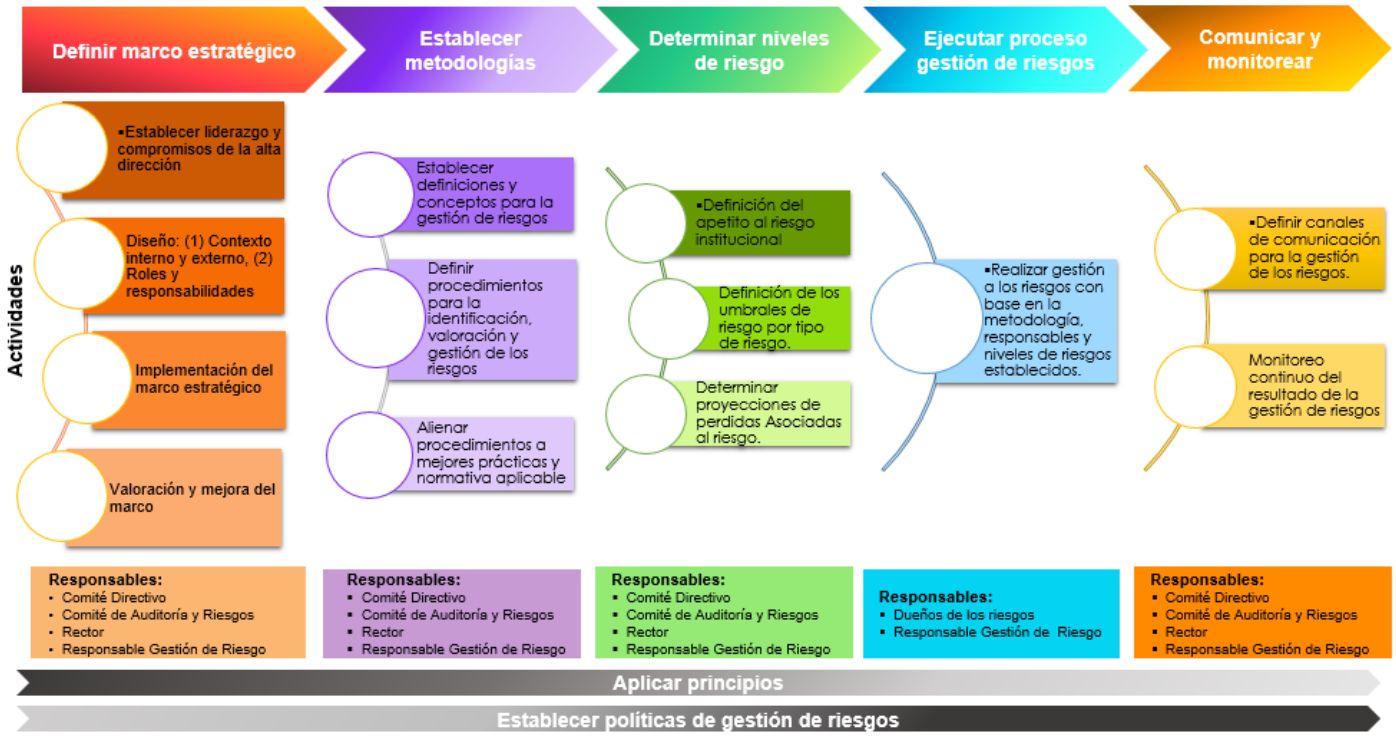
El marco COBIT está basado en 5 principios y 7 catalizadores/ habilitadores conforme con las áreas responsables de: evaluar, planear, construir, entregar y supervisar los recursos de TI. Como se muestra en la siguiente gráfica.

Gráfica 5. COBIT (Information Systems Audit and Control Association ISACA, 2019)

2. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE RIESGOS

Teniendo en cuenta la importancia de identificar, analizar, tratar y monitoreas los diferentes riesgos, la Institución aplica las determinaciones establecidas en los marcos mencionados anteriormente, destacando la norma ISO 31000:2018, aplicando sus principios, estableciendo un marco de referencia y proceso para la implementación del Sistema de Gestión de Riesgos.

La Universidad considera al momento de definir su Sistema de Gestión de Riesgos un marco estratégico, responsables de la gestión, metodologías a implementar, las cuales se articulan para lograr estructurar un sistema sólido y alineado a las necesidades de la Institución como se muestra a continuación:



Gráfica 6. Implementación Sistema de Gestión de Riesgos.

2.1. Definición del marco estratégico

Para la implementación de un Sistema de Gestión de Riesgos que se adecue a la estructura y tamaño de la Institución, es necesario definir un marco estratégico propio para la Universidad que se adapte a las necesidades y características de la misma, por lo que se debe considerar liderazgo y compromiso por parte de la alta dirección, integrar la gestión de riesgos en todos los procesos Institucionales, análisis al entorno interno y externo de la Universidad, asignación de roles, autoridades y responsabilidades, valoración y mejora del marco estratégico. Todo lo anterior debe estar alineado a los principios para la gestión de riesgos.

El propósito del marco estratégico de la gestión de riesgo es apoyar la integración de esta gestión en todas las actividades y funciones de la Universidad, incluyendo la gobernanza y toma de decisiones eficaces Institucionales.

2.1.1. Establecer liderazgo y compromisos de la alta dirección

La alta dirección debe asegurar que la gestión del riesgo esté integrada en todas las actividades de la Institución, demostrando liderazgo y compromiso que permita:

- Adaptar e implementar todos los componentes del marco estratégico.
- Publicar la política que establezca un enfoque, un plan o una línea de acción para la gestión del riesgo.
- Asegurar los recursos necesarios para gestionar los riesgos.
- Asignar autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la Institución.

Esto ayudará a la Institución a:

- Alinear la gestión del riesgo con su estrategia, objetivos y cultura.
- Reconocer y abordar todas las obligaciones y compromisos adquiridos.

- Establecer la magnitud y el tipo de riesgo que puede o no ser tomado para guiar el desarrollo de los criterios de riesgo, asegurando su comunicación al interior de la Institución y partes interesadas.
- Promover seguimiento sistemático de los riesgos.
- Asegurar que el marco estratégico de la gestión del riesgo sea apropiado al contexto de la Institución.

La Alta Dirección para asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización, ha delegado la responsabilidad del Sistema de Gestión Integral de Riesgos al Comité de Auditoria y Riesgos.

2.1.2. Diseño del marco estratégico

Para el desarrollo del marco estratégico se debe comprender la Institución en su contexto externo e interno.

2.1.2.1. Análisis entorno interno y externo

Para la definición del contexto interno y externo se realizará un análisis teniendo en cuenta los aspectos mencionados a continuación:

Aspectos Internos

- Misión, visión y valores Institucionales,
- Estrategia y objetivos (Plan de Desarrollo Institucional "PDI"),
- Gobernanza, estructura, roles y responsabilidades,
- Políticas, directrices y procedimientos adoptados,
- Cultura Institucional,
- Las capacidades entendidas en términos de recursos y conocimiento, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías, entre otros,
- Los datos, los sistemas de información y los flujos de información,
- Las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores,
- Las relaciones contractuales y los compromisos, las interdependencias e interconexiones.

Aspectos Externos

- Los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales que afectan el entorno externo de la Universidad,
- Las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas,
- Las relaciones contractuales y los compromisos,
- La complejidad de las redes y dependencias,
- Comparación con otras instituciones pares tanto nacionales como internacionales,

2.1.2.2. Compromiso de la gestión del riesgo

La alta dirección de la Institución demuestra su compromiso continuo con la gestión de riesgos mediante la implementación de la Política de Gestión de Riesgos, que expresa los objetivos y los compromisos de la Universidad con la gestión de riesgos. El compromiso debe incluir, pero no se limita a:

- Propósito de la gestión de riesgos y los vínculos con sus objetivos y otras políticas, si aplica.
- Liderazgo en la integración de la gestión del riesgo.
- Fortalecimiento de la cultura del riesgo Institucional.
- Toma de decisiones, frente a la gestión de riesgos
- Roles y responsabilidades frente a la gestión de riesgos.
- Disponibilidad de los recursos necesarios.
- Manejo de conflicto en los objetivos.
- Medición e informe como parte de los indicadores de desempeño.
- Revisión y comunicación de la política.

2.1.2.3. Roles y responsabilidades

La alta dirección establece en su política de gestión de riesgos los roles y responsabilidades frente al Sistema de Gestión de Riesgos Institucional, asegurando: autoridad, responsabilidad, rendición de cuentas, recursos y la comunicación a todos los niveles de la Institución.

Por otra parte, la alta dirección debe establecer las determinaciones con relación a la comunicación y consulta del marco estratégico para que estas sean oportunas y aseguren que la información sea recopilada, consolidada, se sintetice y se compare de manera apropiada y pertinente, y se proporcione una retroalimentación alienada a la mejora continua.

2.1.3. Implementación del marco estratégico

La institución implementa el marco estratégico de la gestión del riesgo mediante:

- El desarrollo de un plan apropiado que incluya plazos y recursos.
- La identificación de los responsables de toma de decisiones en toda la Institución.
- La modificación de los procesos aplicables para la toma de decisiones, cuando sea necesario.
- El aseguramiento de que las disposiciones de la Institución para gestionar el riesgo son claramente comprendidas y puestas en práctica.

La implementación con éxito del marco estratégico requiere el compromiso y la toma de conciencia de todas las partes interesadas en la Institución. Esto permite abordar explícitamente la incertidumbre en la toma de decisiones, al tiempo que asegura que cualquier incertidumbre nueva o subsiguiente se pueda tener en cuenta cuando surja.

Si se diseña e implementa correctamente, el marco estratégico de la gestión de riesgos asegurará que el proceso de la gestión del riesgo sea parte de todas actividades en toda la Institución, incluyendo la toma de decisiones, y que los cambios en los contextos externo e interno se captarán de manera adecuada.

2.1.4. Valoración y mejora

Para una valoración eficaz del marco estratégico de la gestión del riesgo, la Universidad debe:

- Medir periódicamente el desempeño del marco estratégico con relación a su propósito, sus planes para la implementación, sus indicadores y el comportamiento esperado.
- Determinar si permanece idóneo para apoyar el logro de los objetivos de la Institución.

Además, se realizará el seguimiento continuo para realizar adaptaciones del marco estratégico en función de los cambios externos e internos.

2.2. Metodología establecida para la gestión de riesgos

La Universidad establece y determina los elementos centrales necesarios, para que el Sistema de Gestión de Riesgos se desarrolle de la manera esperada, cumpliendo con la normatividad en conjunto con la aplicación de mejores prácticas en gestión de riesgos, como se muestra en el **Anexo N°1 Metodología para la valoración de riesgos y controles,** donde se podrá observar el detalle de los componentes relacionados con:

- Definición del riesgo
- Análisis y evaluación del riesgo
- Actividades de control

2.3. Establecimiento de responsabilidades frente a la gestión de riesgos

La Universidad siendo consciente de la importancia de involucrar la gestión de riesgos en todas sus actividades y funciones, debe articularla por medio de canales de comunicación adecuados, que permitan la mejora continua y creación de valor.

Por lo cual, la Universidad adopta el modelo de las tres líneas de defensa, ya que proporciona una manera simple y efectiva para la mejora continua de la gestión de riesgos y el control interno.

2.3.1. Modelo de las tres líneas

El modelo de las tres líneas proporciona una manera simple y efectiva para mejorar la comunicación en la gestión de riesgos y control interno, mediante la aclaración de las funciones y deberes esenciales relacionadas. El modelo clasifica las áreas funcionales y de responsabilidad de la Universidad y brinda una visión de las operaciones, garantizando una adecuada supervisión y gestión del riesgo, además de ser apropiado para cualquier organización independientemente de su tamaño o complejidad.

Este modelo contempla seis principios y tres líneas que se relacionan así:

Principio 1: Gobierno

El gobierno de la Institución requiere una estructura y procesos apropiados para:

- Aceptar la rendición de cuentas a las partes interesadas por la supervisión de la Institución.
- Se compromete con las partes interesadas para vigilar sus intereses y comunicarse de forma transparente sobre el logro de los objetivos.
- Nutre una cultura que promueve el comportamiento ético y la rendición de cuentas.
- Establece estructuras y procesos de gobierno, incluyendo los comités asesores, según sea necesario.
- Delega la responsabilidad y proporciona recursos a la dirección para lograr los objetivos de la Institución.
- Determina el grado de aceptación del riesgo de la Institución y ejerce supervisión de la gestión del riesgo (incluyendo el control interno).
- Supervisa el cumplimiento de las expectativas legales, reglamentarias y éticas.
- Establece y supervisa la independencia, objetividad y competencia del rol de auditoría interna.

Principio 2: Roles del órgano de gobierno

El órgano de gobierno asegura que:

- Se han establecido estructuras y procesos adecuados para un gobierno eficaz.
- Los objetivos y actividades de la Institución están alineados con los intereses prioritarios de las partes interesadas.

El órgano de gobierno:

- Delega la responsabilidad y proporciona recursos a la dirección para alcanzar los objetivos de la institución mientras que asegura que se cumplan las expectativas legales, regulatorias y éticas.
- Establece y supervisa el rol de auditoría interna, para proporcionar claridad y confianza en el progreso hacia el logro de los objetivos.

Principio 3: Dirección y roles de primera y segunda línea

La responsabilidad de la dirección de alcanzar los objetivos Institucionales comprende tanto los roles de primera como las de segunda línea. Los roles de la primera línea establecen y mantienen estructuras y procesos adecuados para la gestión de operaciones y riesgos. Los roles de segunda línea proporcionan asistencia en la gestión del riesgo. Los roles de primera y segunda línea pueden mezclarse o separarse.

Algunos roles de segunda línea pueden ser asignadas a especialistas para proporcionar experiencia adicional, apoyo, monitoreo y cuestionar a aquellos con roles de primera línea. Los roles de segunda línea pueden centrarse en objetivos específicos de la gestión de riesgos. Como alternativa, los roles de segunda línea pueden abarcar una responsabilidad más amplia en la gestión de riesgos, como la gestión de riesgos empresariales (ERM). Sin embargo, la responsabilidad de la gestión del riesgo sigue siendo parte de los roles de primera línea y dentro del ámbito de la gestión.

Roles de primera línea

- Dirige y orienta las acciones (incluyendo la gestión del riesgo) y la aplicación de recursos para lograr los objetivos de la Institución.
- Mantiene un diálogo continuo con el órgano de gobierno e informa sobre: los resultados previstos, reales y esperados, vinculados a los objetivos de la Institución y el riesgo.

- Establece y mantiene estructuras y procesos adecuados para la gestión de operaciones y riesgos (incluyendo el control interno).
- Garantiza el cumplimiento de las expectativas legales, reglamentarias y éticas.

Roles de segunda línea

- Proporciona conocimientos especializados, complementarios, apoyo, vigilancia y cuestionamientos relacionados con la gestión del riesgo, entre otros:

    - El desarrollo, la implementación y la mejora continua de las prácticas de gestión de riesgos (incluyendo el control interno) a nivel de procesos, sistemas e Institución.
    - El logro de objetivos de gestión de riesgos, tales como: cumplimiento de leyes, reglamentos y comportamiento ético aceptable, control interno, seguridad de la información y la tecnología, sostenibilidad y aseguramiento de calidad.

- Proporciona análisis e informes sobre la adecuación y eficacia de la gestión de riesgos (incluyendo el control interno).

Principio 4: Roles de tercera línea

La Auditoría Interna proporciona aseguramiento y asesoramiento independientes y objetivos sobre la adecuación y eficacia del gobierno y la gestión de riesgos. Esto se logra mediante la aplicación competente de procesos sistemáticos y disciplinados, experiencia y percepciones. Informa de sus conclusiones, e inclusive puede considerar el aseguramiento de otros proveedores internos y externos.

Auditoría Interna

- Mantiene la rendición de cuentas ante el Comité de Auditoría y Riesgos, como órgano de gobierno y con independencia de las responsabilidades de la dirección.
- Comunica el aseguramiento y asesoramiento independientes y objetivos al Comité de Auditoría y Riesgos, a la dirección y al órgano

de gobierno, sobre la adecuación y eficacia de la gobernanza y la gestión de riesgos (incluyendo el control interno) para apoyar el logro de los objetivos de la Institución y promover y facilitar la mejora continua.

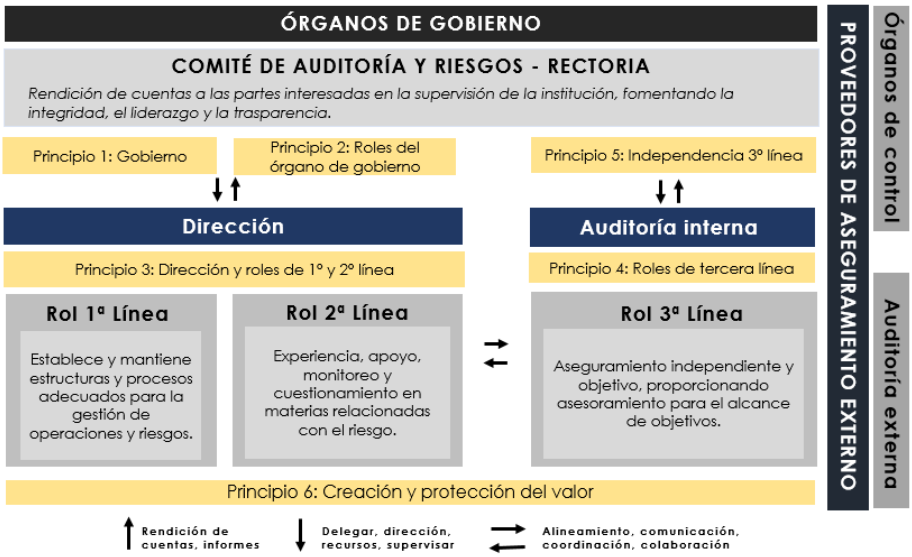
- Informa al órgano de gobierno las deficiencias en la independencia y la objetividad y aplica las salvaguardas necesarias.

Principio 5: Independencia de tercera línea

La independencia de la Auditoría Interna de las responsabilidades de la gerencia es fundamental para su objetividad, autoridad y credibilidad. Se establece mediante: la rendición de cuentas ante el órgano de gobierno; el acceso sin restricciones a las personas, los recursos y los datos necesarios para completar su trabajo; y la ausencia de prejuicios o interferencias en la planificación y prestación de servicios de auditoría.

Principio 6: Creación y protección del valor

Todos los roles que trabajan juntos contribuyen colectivamente a la creación y protección de valor cuando están alineadas entre sí y con los intereses prioritarios de las partes interesadas. La alineación de las actividades se logra mediante la comunicación, la cooperación y la colaboración. Esto asegura la fiabilidad, coherencia y transparencia de la información necesaria para la toma de decisiones basada en el riesgo.



Gráfica 8. Modelo de las 3 líneas (The Institute of internal Auditors, 2020)

2.3.2. Responsabilidades frente a la gestión de riesgos

La Alta Dirección (Comité Directivo, Comité de Auditoría y Riesgos, Rectoría), Directivos, Profesores, Administrativos y demás vinculados, deben ser conscientes de la importancia del papel que desempeñan dentro del Sistema de Gestión de Riesgos de la Institución; conocer como a través del cumplimiento de las funciones que le fueron asignadas, contribuyen al desarrollo y mejoramiento de los procesos, procedimientos, actividades, metas, planes, programas que ejecuta la Institución para cumplir con los objetivos que le han sido encomendados.

Es importante que todos los miembros involucrados en cada uno de los procesos, conozcan los riesgos a los que están expuestos, así como los controles establecidos para su gestión. Dentro de la mejora continua, se hace necesaria la revisión permanente del Sistema de Gestión de Riesgos, de tal forma que permita a los responsables una toma de decisiones oportuna mediante acciones preventivas o correctivas.

2.4. Definición niveles de riesgos

2.4.1. Definición apetito al riesgo

El objetivo de realizar la definición de los niveles de apetito al riesgo, es ayudar a la Institución en la toma de decisiones sobre los riesgos asociados al cumplimiento de objetivos y estrategia Institucional, proporcionando orientación en términos de:

- Definir la cantidad o nivel de riesgo que la Universidad está dispuesta a evitar, perseguir, tolerar o aceptar para lograr los objetivos estratégicos y operativos.
- Fortalecer el gobierno corporativo y la supervisión de riesgos por parte de la alta dirección con el apoyo del Comité de Auditoría y Riesgos.
- Proveer criterios guía para la toma de decisiones en todos los niveles.
- Asegurar que se aplique un nivel adecuado de toma de riesgos (bajo, moderado, alto y extremo) en los trabajos y proyectos ejecutados en la Institución.

- Contribuir en la asignación efectiva de recursos.
- Identificar cómo se adecuan las decisiones para lograr los objetivos de acuerdo con el perfil de riesgos establecido, y en caso de existir desviaciones, gestionarlas de forma eficiente y oportuna.
- Estimular una cultura de conciencia de riesgo

Definición

El apetito al riesgo se refiere a la cantidad y el tipo de riesgo que la Universidad se siente cómoda de aceptar para lograr los objetivos. Equilibra los beneficios del cambio o la innovación con las amenazas que el cambio puede traer.

Establece los límites de los riesgos que la Universidad puede tolerar en las actividades realizadas y ayuda a encontrar el equilibrio entre la toma de riesgos y evitación de riesgos.

Principios y enfoque

En general, la Universidad tiene un enfoque equilibrado del riesgo. El apetito al riesgo está alineado con los objetivos estratégicos definidos.

Es importante recordar que la gestión de riesgos no se trata únicamente de evitar riesgos, la visión y estrategia de la Universidad requiere que se gestione el riesgo en función del valor. Se acepta que el riesgo es proporcional a la potencial recompensa como el crecimiento, la transformación y la innovación.

Los aspectos clave para lograr el equilibrio son:

- Garantizar prácticas de gobernanza éticas y eficaces, incluida la gestión responsable de los recursos.
- Aprovechar las oportunidades que promueven el crecimiento, la transformación y la innovación, evitando impactos negativos innecesarios.
- Prevenir una cultura que es reacia al riesgo y ahoga el crecimiento, la transformación y la innovación.
- Fomentar una cultura que respalde la evaluación y la gestión de riesgos basada en valores.

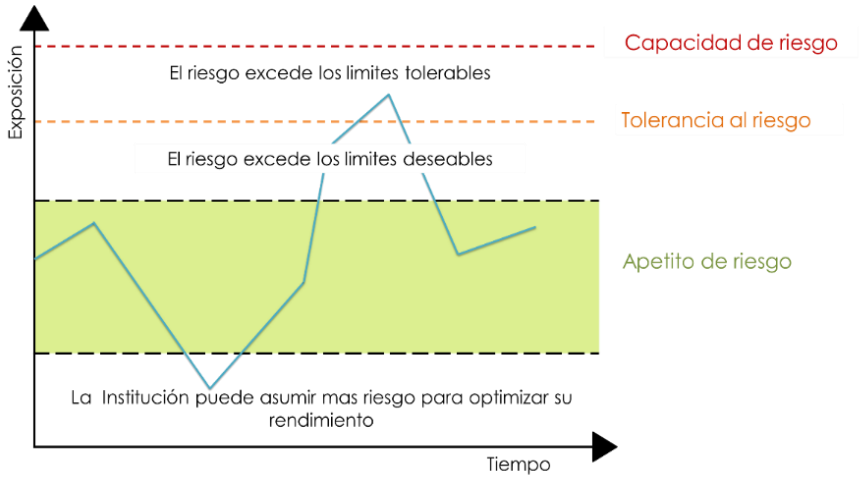
Los siguientes principios básicos proporcionan un contexto en la definición de los niveles de riesgo en la Institución.

- Las categorías de riesgo definidas para la institución, no es una lista exhaustiva que aborde todas las situaciones de riesgo, pero proporciona pautas generales.
- Todos los responsables de la toma de decisiones en las diferentes categorías de riesgos, deben buscar el mejor interés y beneficio para la Universidad y sus grupos de interés.
- Los niveles de riesgo son una expresión prospectiva y reflejan la tolerancia para aceptar nuevos riesgos (además de los riesgos actuales) en la consecución de los objetivos estratégicos de la Universidad.
- Nuestra capacidad, tolerancia y apetito al riesgo son dinámicos y cambiarán con el tiempo en respuesta a diferentes factores.
- Todas las decisiones se alinean con la misión, visión, valores y estrategia de la Universidad.

Niveles de riesgo

Los niveles de riesgo de la Institución se definen bajo la siguiente escala:

- Capacidad de riesgo: Nivel máximo de riesgo que la Universidad puede soportar en la persecución de sus objetivos.
- Tolerancia al riesgo: Será la desviación respecto al apetito.
- Apetito al riesgo: Nivel de riesgo que la Universidad quiere aceptar.



Gráfica 9. Niveles de apetito al Riesgo *(La fabrica de pensamiento, 2013)*

Responsables del apetito al riesgo

La definición de las categorías de riesgos estratégicos, se determinan en talleres desarrollados con miembros del Comité Directivo, Rector, Vicerrectores, Secretaria General y algunos Directores clave de la Institución. Estos talleres se realizan con el objetivo de:

- Conocer la percepción y alinear a la alta dirección en la identificación de riesgos estratégicos.
- Establecer y utilizar métricas cuantitativas y cualitativas para la determinación del apetito al riesgo en las diferentes categorías de riesgos.
- Realizar una evaluación detallada de todos los factores de riesgo que pueden afectar el cumplimiento de la estrategia institucional (sector al que pertenece, cultura organizacional, liquidez y sostenibilidad financiera, medio ambiente y político, regulación, ciberseguridad, entre otros).
- Determinar el apetito al riesgo deseable en el momento actual y a mediano plazo, considerando tanto las circunstancias más probables como escenarios de estrés.
- Integrar el apetito de riesgo a la planificación estratégica, a través de políticas, directrices y límites de gestión, así como a través de la participación de todas las líneas de defensa en los procesos clave del apetito.

Resultado del análisis anterior, se describe a continuación las escalas de apetito al riesgo o postura frente al riesgo, así como, algunas de las diferentes categorías de riesgos definidos por la alta dirección de la Institución, a modo de ejemplo:

Postura frente al riesgo	Descripción
Tolerancia 0	La Institucion no está preparada para aceptar ningún riesgo.
Aversión	Preparado para aceptar solo los niveles bajos de riesgo, con preferencia segura para la toma de decisiones y la implementación de la estrategia, aunque reconociendo que puede haber poca oportunidad de innovación o explotación de nuevas oportunidades.
Cautela	Dispuesto a aceptar algunos riesgos bajos, manteniendo una preferencia general por decisiones seguras en la elaboración e implementación de la estrategia, a pesar de la probabilidad de que exista un potencial restringido para la innovación y el aumento de resultados y beneficios.
Moderado	Inclinando predominantemente hacia la exposición a niveles modestos de riesgo para lograr resultados o beneficios aceptables, pero poco ambiciosos.
Flexible	Preparado para considerar decisiones innovadoras e implementación estratégica con la más alto probabilidad de resultados y beneficios productivos, incluso cuando hay niveles elevados de riesgo asociado.
Abierto	Tomar de manera proactiva decisiones innovadoras / creativas / pioneras y adoptar formas de implementación de la estrategia, aceptando los niveles de riesgo sustancial asociados con el fin de asegurar resultados y beneficios de gran éxito.

Gráfica 10. Postura frente al riesgo.

Categoría de riesgo	Descripción	Apetito al riesgo / Postura frente al riesgo					
		Tolerancia 0	Aversión	Cautela	Moderado	Abierto	Flexible
Riesgos estratégicos	Reputación						
	Gestión de la estrategia						
	Deserción de estudiantes						
	Competencia y mercado						
	Innovación y crecimiento						
Riesgos operativos	Daño a bienes Físicos						
	Fraude						
	Salud, seguridad y bienestar						
Riesgos financieros	Liquidez y sostenibilidad financiera						
Riesgos legales	Cumplimiento legal y regulatorio.						

Gráfica 11. Relación categorías de riesgos y apetito al riesgo.

Es importante que el equipo de la alta dirección responsable de definir y evaluar las categorías de riesgo, lo realicen continuamente, ya que los mismos cambian con el tiempo; por lo cual se deben abordar oportunamente.

2.5. Proceso de gestión de riesgos

El proceso de gestión de riesgos implica la aplicación sistemática de políticas y procedimientos que permiten la identificación, evaluación, tratamiento, seguimiento, comunicación y consulta de los riesgos. El proceso de la gestión del riesgo debe ser una parte integral de la gestión y toma de decisiones, la cual se debe integrar en la estructura, las operaciones y los procesos de la Institución. Puede aplicarse a nivel estratégico, operacional, de programa o de proyecto.

El flujo del proceso para la administración del riesgo se encuentra en el **Anexo N°2 Detalle proceso de gestión de riesgos**, compuesto por cada una de las actividades que comprende la ejecución del proceso, hasta el monitoreo y comunicación, así:

- Ejecución del proceso gestión de riesgo
- Planificación y evaluación del contexto
- Identificación y evaluación del riesgo
- Monitoreo y comunicación

2.6. Comunicación y monitoreo del Sistema de Gestión de Riesgos

La Universidad para asegurar una mejora continua debe implementar acciones para el seguimiento y revisión continuo de Sistema de Gestión de Riesgos Institucional el cual incluye: marco de referencia para la gestión de riesgos, política de gestión de riesgos, metodologías y el proceso de gestión de riesgos, este seguimiento permitirá cumplir con los objetivos Institucionales y una administración eficaz de los riesgos.

La comunicación y el monitoreo son actividades presentes en todas las etapas de la gestión de riesgos, con el objetivo de proporcionar retroalimentación, identificando brechas u oportunidades, manteniendo una comunicación permanente con todos los niveles de la Institución.

2.6.1. Canales de comunicación para la gestión de los riesgos

Los canales de comunicación se encuentran alineados a la metodología adoptada del modelo de las tres líneas, ver capítulo 2.3.1 Modelo de las tres líneas, ya que esta proporciona una comunicación clara, con emisores y receptores determinados, asegurando su idoneidad para generar un tránsito de información adecuado y pertinente.

2.6.2. Monitoreo continuo del resultado de la gestión de riesgos

Es responsabilidad de la Universidad, realizar de manera constante un análisis y seguimiento de los resultados de los diferentes procesos de gestión de riesgos realizados, para poder determinar su efectividad, además de identificar las oportunidades de mejora que agreguen valor a la institución.

2.7. Principios para la gestión del riesgo

Para realizar una adecuada implementación del Sistema de Gestión de Riesgos, se debe aplicar los principios establecidos en la ISO 31000:2018, los cuales proporcionan fundamento y orientación para el desarrollo eficaz y eficiente del mismo, comunicando su valor, intención y propósito en toda la Institución, mediante la adopción de los siguientes principios:

- Integrada: la gestión del riesgo es parte integral de todas las actividades de la Institución.
- Estructurada y exhaustiva: este enfoque contribuye a resultados coherentes y comparables.
- Adaptada: el marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales al contexto interno y externo de la Institución relacionado con sus objetivos.
- Inclusiva: la participación apropiada y oportuna de las partes interesadas permite que se consideren sus conocimientos, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- Dinámica: los riesgos pueden aparecer, cambiar o desaparecer con los cambios de contextos externos e internos de la Institución. La

gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

- Mejor información disponible: las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- Factores humanos y culturales: el comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
- Mejora continua: la gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

2.8. Política de gestión de riesgos

El desarrollo de cualquier actividad puede estar expuesta a situaciones que generen un impacto negativo afectando los objetivos establecidos en la Institución. Como consecuencia de la diversidad de riesgos, se requiere un acercamiento profundo, metodológico y sistemático a la administración de los mismos.

El Sistema de Gestión de Riesgos de la Institución, se basa en los principios de eficiencia, transparencia, responsabilidad, adaptabilidad, participación activa, información fiable y oportuna.

El presente documento se enmarca dentro de la Política de Gestión de Riesgos aprobada por el Comité Directivo.

Es responsabilidad del Comité de Auditoría y Riesgos elaborar la Política de Gestión de Riesgos para ser aprobaba por el Comité Directivo.

3. REFERENCIAS YANEXOS

3.1. Bibliografía

Committee of Sponsoring Organizations of the Treadway commission (COSO). (2013). *Marco Integrado de Control Interno.*

Committee of Sponsoring Organizations of the Treadway commission (COSO). (2017). *Marco COSO ERM 2017.*

Deloitte. (2017). *COSO ERM 2017 y la Generación de valor.*

Information Systems Audit and Control Association ISACA. (2019). *Objetivos de Control para las Tecnologías de la Informacion y Relacionadas (COBIT).*

International Organization for Standardization (ISO). (2018). *Norma ISO 31000:2018-Gestion de riesgos. Principios y directrices.*

La fabrica de pensamiento, I. E. (2013). *Escalas de apetito al riesgo, creación propia.*

Rodiguez, I. (18 de NOV de 2014). *Auditool*. Obtenido de ¿Qué es el riesgo, riesgo inherente y riesgo residual?: https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

The American Institute of Certified Public Accountants "AICPA". (s.f.). *Circular A-133.*

The Institute of internal Auditors. (2020). *THE IIA's THREE LINES MODEL.*

The Institute of Internal Auditors. (s.f.). *Marco Internacional para la Páctica Profesional.*

Universidad de los Andes. (2020). *Manual de auditoria interna 2020.*

3.2. Anexos

1. Metodología establecida para la valoración de riesgos y controles.
2. Proceso de gestión de riesgos.