SANMARTÍN
Fundación Universitaria

FUNDACIÓN UNIVERSITARIA SAN MARTIN
CONSEJO SUPERIOR

ACUERDO N° 04
24 de abril de 2024

"Por el cual se aprueba la Política de Gestión de Riesgos de la Fundación Universitaria San Martín"

El Consejo Superior de la Fundación Universitaria San Martín en uso de sus facultades legales y estatutarias, en especial las consagradas en los artículos 18 numerales 5 y 7, y 56 de los Estatutos y

CONSIDERANDO

Que la Fundación Universitaria San Martín con domicilio en Bogotá D.C., es una Institución universitaria de carácter privado, con Personería Jurídica reconocida mediante Resolución No. 12387 del 18 de agosto de 1981, expedida por el Ministerio de Educación Nacional.

Que la Constitución Política en el artículo 69, garantiza la autonomía universitaria, y establece que las instituciones de educación superior podrán darse sus directrices y regirse por sus propios estatutos de acuerdo con la ley.

Que la Ley 30 de 1992 desarrolla los alcances de la autonomía universitaria y regula la educación superior en los aspectos generales de los programas académicos; así, en su artículo 29 dispone que en ejercicio de su autonomía, las instituciones universitarias podrán darse y modificar sus estatutos, designar sus autoridades académicas y administrativas, crear, desarrollar sus programas académicos, lo mismo que expedir los correspondientes títulos, definir y organizar sus labores formativas, académicas, docentes, científicas, culturales y de extensión, y arbitrar y aplicar sus recursos para el cumplimiento de su misión social y de su función institucional.

Que los Estatutos de la Fundación Universitaria San Martín en su artículo 9 establece como uno de los objetivos institucionales *"Ubicar a la Fundación Universitaria San Martín como una organización acorde con la modernidad, con amplia autonomía, con calidad académica, amplia cobertura y alto compromiso social".*

Que adicionalmente, el artículo 38 de los Estatutos, señala que *"El control de las actividades de la Fundación Universitaria San Martin será ejercido por la Revisoría Fiscal y la Auditoria Interna en consonancia con los presentes Estatutos, los reglamentos que para el efecto expida el Consejo Superior y la Ley".*

Que la gestión del riesgo para las entidades en todos sus órdenes cobra cada día mayor relevancia, dado el dinamismo y los constantes cambios en el mundo globalizado, enfrentando factores internos y externos que pueden crear incertidumbre sobre el logro de los objetivos.

SANMARTÍN
Fundación Universitaria

FUNDACIÓN UNIVERSITARIA SAN MARTIN
CONSEJO SUPERIOR

ACUERDO N° 04
24 de abril de 2024

"Por el cual se aprueba la Política de Gestión de Riesgos de la Fundación Universitaria San Martín"

Que la Fundación Universitaria San Martín, con el propósito de preservar la eficacia y eficiencia de su misión, así como salvaguardar los recursos que administra, ha evidenciado la necesidad de implementar un sistema de administración de riesgos con base en el análisis del contexto estratégico, así como la determinación de métodos para el tratamiento y monitoreo de sus riesgos, con el fin de prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de sus objetivos.

Que en la sesión del Consejo Superior celebrada el 24 de abril de 2024 se presentó la propuesta de la Política de Gestión de Riesgos de la Fundación Universitaria San Martín; una vez revisada y encontrándola ajustada, fue aprobada por el Consejo Superior, según consta en Acta No. 5 del 24 de abril de 2024.

Que en mérito de lo expuesto,

ACUERDA:

ARTÍCULO PRIMERO: Aprobar la Política de Gestión de Riesgos de la Fundación Universitaria San Martín según documento adjunto que forma parte integral del presente Acuerdo.

ARTÍCULO SEGUNDO: El presente Acuerdo rige a partir de la fecha de su aprobación y deroga todas las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dado en la ciudad de Bogotá D.C., a los veinticuatro (24) días del mes de abril de dos mil veinticuatro (2024)

ARLEY GÓMEZ LÓPEZ
Presidente Consejo Superior

ALEJANDRO SUAREZ PARADA
Secretario General

FUNDACIÓN UNIVERSITARIA SAN MARTÍN-Nit: 860.503.634-9
Personería Jurídica N° 12387 de Agosto 18 de 1981
VIGILADA MINEDUCACIÓN
www.sanmartin.edu.co

POLÍTICA DE ADMINISTRACIÓN DE RIESGO EN LA INSTITUCIÓN.

SAN MARTÍN
Fundación Universitaria

Rectoría

Abril de 2024.

Contenido

Introducción

La gestión del riesgo para las entidades en todos sus órdenes cobra cada día mayor relevancia, dado el dinamismo y los constantes cambios en el mundo globalizado, enfrentando factores internos y externos que pueden crear incertidumbre sobre el logro de los objetivos. Es por ello que la Institución con el propósito de preservar la eficacia y eficiencia de su misión, así como salvaguardar los recursos que administra, toma la decisión de implementar un sistema de administración de riesgos con base en el análisis del contexto estratégico, así como la determinación de métodos para el tratamiento y monitoreo de sus riesgos, con el fin de prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de sus objetivos. A través del Sistema de Control Interno establecido por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés), Marco Integrado de Control Interno[1] y los componentes que la conforman se proporciona una estructura de control a la gestión, la cual brinda elementos para construir y fortalecer el control interno en la Institución como es su componente de gestión de riesgos.

Adicionalmente los principios que constituyen fuente para garantizan la efectividad del sistema de control interno de acuerdo con la naturaleza de las operaciones de la Institución, son:

i. Autocontrol: Capacidad de todos los empleados, independientemente de su nivel jerárquico para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos.

ii. Autorregulación: La Constitución Política de Colombia otorga a las Universidades autonomía para gobernarse y regularse, por ello tienen una responsabilidad social y debe rendir cuentas a la sociedad sobre el cumplimiento de su misión.

iii. Autogestión: Ejercicio proactivo de las responsabilidades individuales para sumar esfuerzos. Permite a las personas apropiarse de los procesos y procesos académico-administrativos, para orientarlos al logro de la misión institucional.

iv. Autoevaluación: Proceso de reflexión sobre lo que se hace para construir sobre la base de las mejores experiencias, identificar debilidades y prevenir riesgos en la gestión.

[1] Guía de COSO Integrado (Committe Sponsoring Organization of the Treadway Commission Committee of Sponsoring Organizations of the Treadway Commission and Enterprise Risk Management — Integrated Framework).

1. Objetivo

Implementar un sistema de administración de riesgos que permita la minimización de los costos y daños asociados, con el propósito de prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de los objetivos en la Institución.

1.1. Objetivos Específicos

a) Identificar en la Institución los riesgos estratégicos y operativos, y sus Fuentes.
b) Priorizar los riesgos a través de un ejercicio de valoración, teniendo en cuenta los factores propios de su entorno y sus impactos posibles sobre la Institución.
c) Medir la probabilidad de ocurrencia de los riesgos y su impacto sobre los recursos económicos, humanos, entre otros. Esta medición puede ser cualitativa y cuantitativa.
d) Evaluar los controles existentes y su efectividad, mediante un proceso de valoración.
e) Construir los mapas de riesgos que resulten pertinentes.
f) Definir los planes de mejoramiento según los resultados de la evaluación de riesgos.

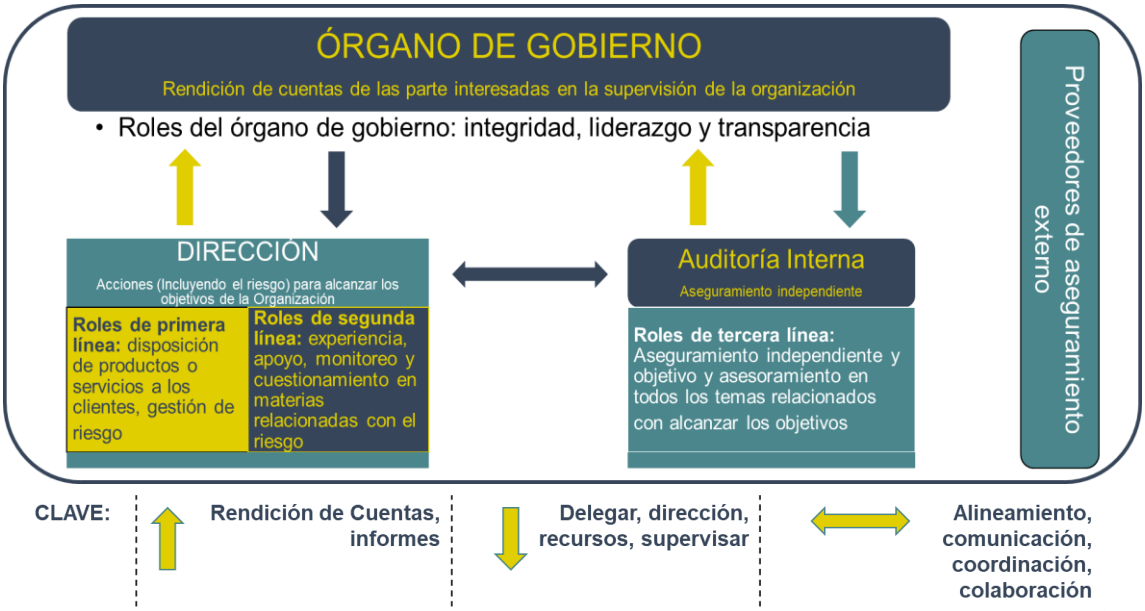
2. Alcance

La política de gestión de riesgos impacta a los procesos de la Institución tanto misionales, estratégicos y de apoyo, mediante la aplicación de la metodología de gestión de riesgos.

3. Roles y Responsabilidades de la Administración de Riesgo.

Para una efectiva gestión de riesgos y control, la Institución acogerá el modelo de las tres líneas de defensa emitido por el Instituto de Auditores Internos que se describe a continuación:

Figura 1: Modelo de las tres líneas del IIA 2020.



Nota. Adaptado del Modelo de las Tres líneas del IIA[2] 2020; Una Actualización de las tres líneas de defensa.

La Institución ha estructurado sus líneas de defensa de la siguiente manera:

Figura 2: Adaptación del modelo de las tres líneas.

Nota: Adaptado de la Guía para la Práctica: Auditoría Interna y la Segunda Línea de Defensa.

[2] The Institute of Internal Auditors

Asignando los roles y las responsabilidades de cada una de las líneas para el funcionamiento de la gestión del riesgo como se muestra a continuación:

Tabla 1: Responsabilidades según modelo tres líneas.

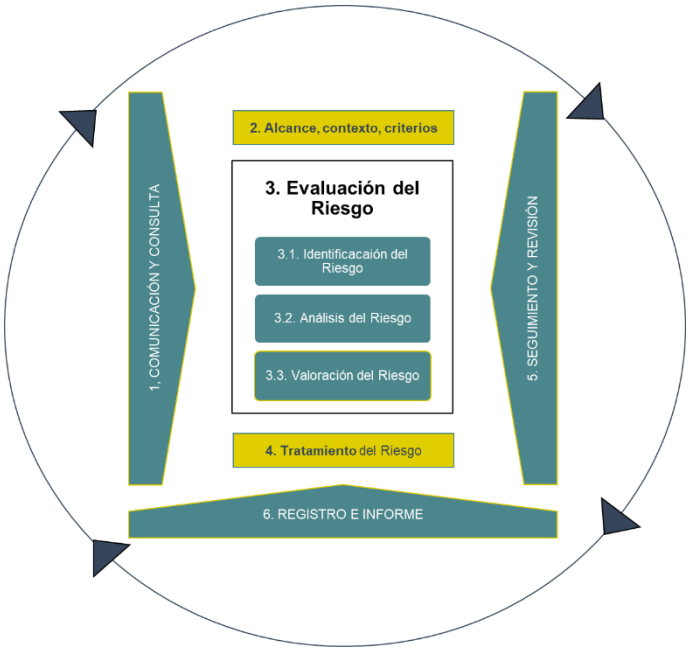
	Responsables	Responsabilidades
Línea Estratégica	Consejo Superior Comité de Auditoría	- Definir el marco de la gestión del riesgo en la Institución. - Determinar el grado de aceptación de riesgo y ejercer la supervisión de la gestión de riesgo.
1ra Línea de Defensa	Directores y Coordinadores Líderes de procesos.	- Identificar, evaluar y realizar seguimiento de los riesgos de la Institución. - Implementar controles para la mitigación de los riesgos. - Implementar acciones correctivas en caso de materialización del riesgo.
2da Línea de Defensa	Rectoría Gestión de Riesgos	- Realizar seguimiento y evaluar la efectividad de los controles de la primera línea acorde con sus responsabilidades. - Realizar la consolidación y análisis de la información de la gestión del riesgo para la toma de decisiones.
3ra Línea de Defensa	Auditoría Interna	- Realizar monitoreo del funcionamiento eficaz de la gestión de riesgos.

Nota. Adaptado de la Política de Gestión del Riesgo de la Agencia Presidencial de Cooperación Internacional – APC Colombia.

4. Metodología para la Administración del Riesgo

Para la implementación de la Gestión de Riesgos en la Institución, se adoptaría la Norma Técnica Colombiana NTC ISO 31000:2018 Gestión del Riesgo, la cual establece las directrices para gestionar el riesgo al que se enfrentan las organizaciones.

Figura 3: Proceso.



Nota. Adaptado de Norma Técnica Colombiana NTC-ISO 31000. Gestión del Riesgo, pág.10, 2018.

4.1. Comunicación y Consulta:

"*El Propósito es asistir a las personas interesadas pertinentes a comprender el riesgo, (…), La comunicación busca promover la toma de conciencia y la comprensión del riesgo, mientras que la consulta implica obtener retroalimentación en información para apoyar la toma de conciencia."(Normas ICONTEC-NTC 31000,2018, pag 11)*

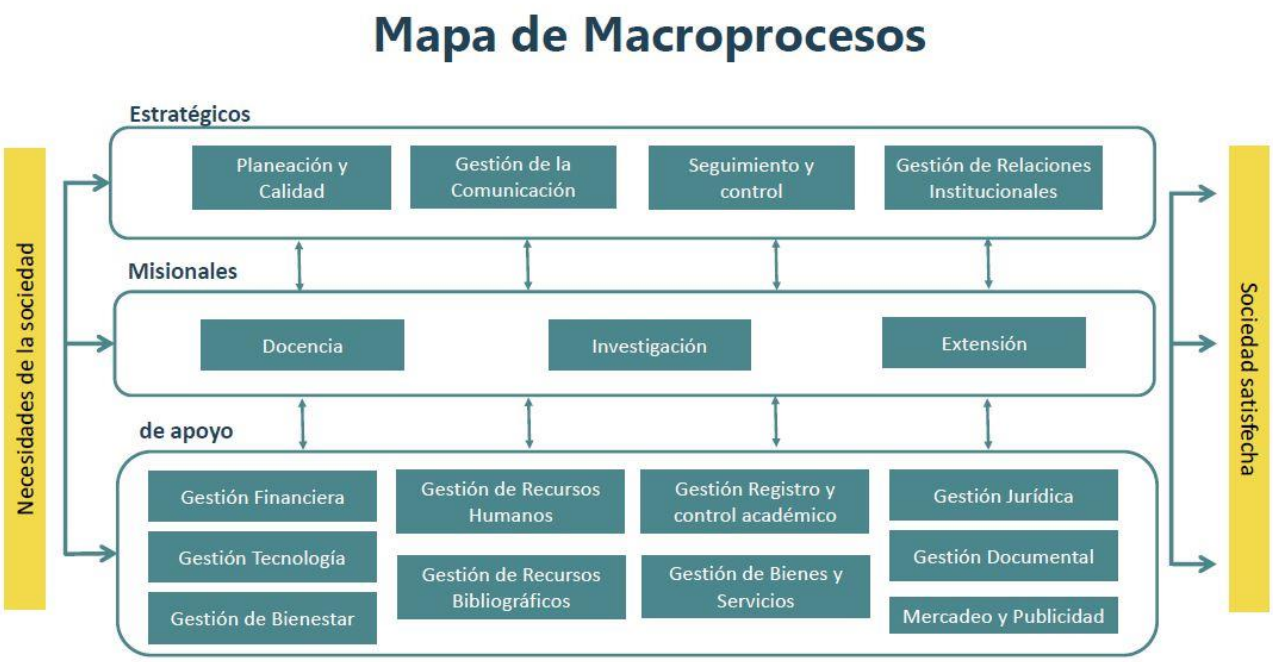
Este paso se desarrollará en todas las etapas de la gestión de riesgo.

4.2. Alcance, Contexto y Criterios:

"*El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican definir el alcance del proceso y comprender los contextos internos.*" (NTC-ISO 31000,2018, pag 11).

Por lo anterior, la definición del contexto es el punto de partida para una correcta identificación de factores tanto internos como externos que pueden desencadenar riesgos y afectar el cumplimiento de los objetivos institucionales, porque permite tener una comprensión de la entidad cimentada en hechos y datos reales.
Basados en el mapa de procesos de la Institución:

Figura 4: Mapa de Macroprocesos Institución Universitaria San Martín.



Nota. Institución Universitaria San Martín. Recuperado de

https://macroprocesos.sanmartin.edu.co/mapa_macroprocesos.

El contexto de gestión de riesgos se define en dos niveles:

- **Institucional:** Contexto global en el que la Institución se desenvuelve y dentro del cual busca cumplir sus objetivos misionales.

- **Operacional:** Contexto en el cual opera la Institución con 17 Macroprocesos y 60 procesos, detallando sus procedimientos con el fin de cumplir con los objetivos institucionales.

Bajo este contexto se desarrollarán dos matrices de riesgos:

- **Estratégicos:** Asociados a la forma en que se administra la Institución, su manejo se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, cumplimiento del PEI[3], la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Operacionales:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, y de la articulación entre las dependencias.

Se establece una clasificación de los siguientes riesgos:

- **Riesgos Académicos:** Se relacionan con el cumplimiento de la prestación de los servicios educativos asociados a los procesos misionales.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la Institución que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la Institución para cumplir con los requisitos legales, contractuales, y de ética pública.

- **Riesgos Tecnológicos:** Están relacionados con la capacidad tecnológica de la Institución para satisfacer sus necesidades actuales y futuras, en el cumplimiento de la misión.

- **Riesgos de Fraude:** Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte del conglomerado social a hacia la Institución.

- **Riesgo de Activos:** Están relacionados con la pérdida, daño, destrucción, indisponibilidad de edificios, instalaciones, equipos e inventarios propios o de terceros.

[3] Proyecto Educativo Institucional.

- **Riesgo de Personas**: Están relacionados con temas laborales y seguridad de las personas que conforman la comunidad Sanmartiniana.

- **Riesgos Operativos:** Están relacionados con el cumplimiento de las actividades de los procesos de apoyo y estratégicos.

4.3. Evaluación del Riesgo

4.3.1. Identificación del Riesgo

"El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que puedan ayudar o impedir a una organización lograr sus objetivos." (NTC-ISO 31000, 2018, pág. 13).

Para identificar los riesgos, se parte de las debilidades y amenazas detectadas y se hace una priorización atendiendo los siguientes criterios:

- Los de mayor impacto en el incumplimiento del objetivo y servicios educativos.
- Los que han desencadenado un hallazgo recurrente a partir de una evaluación interna o externa (incumplimiento de requisitos normativos, fallas, oportunidades de mejora de auditorías internas o externas, críticas o recurrentes).
- Los que se han materializado.

Los riesgos se definirán con la alta dirección y los líderes de los macroprocesos y procesos de la Institución, por medio de talleres liderados por Auditoría Interna.

Asignación de causas y consecuencias: cuando ya se tienen redactados los riesgos se procede a asociar sus causas y consecuencias, bajo las siguientes definiciones y clasificaciones.

- **Causas**: se consideran los agentes generadores del riesgo, medios, circunstancias, sujetos u objetos que pueden desencadenar la amenaza, clasificadas en externas e internas:

Tabla 2: Clasificación de Causas.

CLASIFICACIÓN DE CAUSAS					
EXTERNAS			**INTERNAS**		
E1	**Políticas**	Cambios de gobierno, cambios en la legislación, políticas públicas.	**I1**	**Personas**	Capacidad y cantidad del personal, salud, seguridad, baja productividad, estabilidad laboral, niveles de estrés laboral.
E2	**Medio Ambientales**	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**I2**	**Infraestructura**	Disponibilidad de activos, capacidad de los activos.
E3	**Sociales**	Demografía, responsabilidad social, terrorismo, seguridad ciudadana, valores sociales, calidad de vida.	**I3**	**Procesos**	Capacidad, diseño, ejecución, proveedores, entradas, salidas, interacción con otros procesos.
E4	**Culturales**	Actitud de los ciudadanos.	**I4**	**Procedimientos**	Claridad en emisión de lineamientos, adecuada difusión, formalización.
E5	**Legales**	Regulación.			
EXTERNAS E INTERNAS					
CEI1	**Económicas**	Mercados financieros, niveles de desempleo, competencia, demanda y oferta, inflación, niveles de deuda pública, disponibilidad de recursos.			
CEI2	**Tecnológicas**	Desarrollo, producción, mantenimiento electrónico, datos externos, tecnología emergente, integridad de datos, disponibilidad de datos y sistemas, desarrollo de sistemas de información, mantenimiento, niveles de automatización.			

Nota. Adaptado de la Guía Administración del Riesgo, Universidad Nacional, pág. 28, 2019.

- **Consecuencias:** Son los efectos concretos de la materialización del riesgo que recaen sobre el activo amenazado y finalmente sobre la Institución, se definen en términos de los resultados, el desenlace y la magnitud del daño:

Tabla 3: Consecuencias del Riesgo.

CONSECUENCIAS	
C1	Pérdidas Económicas
C2	Pérdidas de imagen
C3	Insostenibilidad Financiera
C4	Incumplimientos legales
C5	Daños a la integridad física
C6	Llamados de atención
C7	Sanciones
C8	Reprocesos
C9	Insatisfacción de la comunidad
C10	Pérdida de información

Nota. Adaptado de la Guía Administración del Riesgo, Universidad Nacional, pág. 30, 2019.

4.3.2. Análisis del Riesgo

"*El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos."* (Norma ICONTEC-NTC 31000, 2018, pág.14).

El análisis del riesgo busca establecer su probabilidad de ocurrencia y las consecuencias (impacto) de su materialización, calificándolos y evaluándolos para determinar el nivel de riesgo de la información obtenida en la identificación de riesgos.

Los criterios para la calificación del riesgo son subjetivos y dependen de su particularidad, y de los antecedentes del proceso, así como del conocimiento y experiencia de las personas que participan en su análisis.

Por probabilidad se entiende incertidumbre frente a de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad. Bajo el criterio de frecuencia se analiza el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o

eventos ocurridos asociados al riesgo. Bajo el criterio de Factibilidad se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Los siguientes son los niveles de probabilidad a manejar:

Tabla 4: Parámetros de probabilidad.

VALOR	NIVEL	DESCRIPCIÓN	FRECUENCIA
1	**Muy Baja**	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	**Baja**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
3	**Media**	El evento podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
4	**Alta**	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
5	**Muy Alta**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Nota. Adaptado Guia Externa Administración del Riesgo, Función Pública, pág. 39, 2020.

Parámetros de impacto: El impacto se mide según el grado en el que las consecuencias o efectos pueden perjudicar a la Institución si se materializa el riesgo. Las variables pueden describirse en forma cualitativa, cuantitativa o mixta.

Por impacto se entienden las consecuencias que puede ocasionar a la Institución la materialización del riesgo.

Tabla 5: Parámetros de impacto.

VALOR IMPACTO	NIVEL DE IMPACTO	DESCRIPCIÓN					
		PERSONAS / LESIONES	OPERACIÓN	IMAGEN	SANCIONES	PÉRDIDAS ECONÓMICAS	AMBIENTAL
1	**Leve**	● No se ven afectadas las personas ● Lesiones sin incapacidad y/o requieren atención de primeros auxilios o tratamiento médico.	No hay interrupción de las operaciones de la Institución	No se ve afectada la imagen o credibilidad de la Institución	● No hay intervenciones de entes de control. ● No se generan sanciones económicas o administrativas	Pérdidas económicas mínimas, menor a 20 SMMLV.	● Contaminación puntual sin consecuencias para el ambiente ● Alerta interna sobre incumplimiento de estándares ambientales.
2	**Menor**	● Baja afectación en las personas ● Lesiones con incapacidad parcial temporal (trabajo restringido)	Interrupción de las operaciones de la Institución por algunas horas, menor a un (1) día	Imagen o credibilidad institucional afectada internamente.	Comentarios adversos de los entes de control internos o externos, pero no hay intervención, reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	Pérdidas económicas menores, entre 21 y 30 SMMLV.	Daño ambiental leve recuperable en el corto plazo
5	**Moderado**	● Afectación a un grupo reducido de personas ● Lesiones con incapacidad total temporal	Interrupción de las operaciones de la Institución por un (1) día	Imagen o credibilidad institucional afectada localmente	Acciones por parte de los entes de control internos o externos que pueden incluir sanciones menores, reclamaciones o quejas de los usuarios que podrían implicar una denuncia antes los entes reguladores o una demanda de largo alcance para la entidad.	Pérdidas económicas moderadas, entre 31 y 50 SMMLV	Daño ambiental significativo recuperable a mediano plazo

VALOR IMPACTO	NIVEL DE IMPACTO	DESCRIPCIÓN					
		PERSONAS / LESIONES	OPERACIÓN	IMAGEN	SANCIONES	PÉRDIDAS ECONÓMICAS	AMBIENTAL
10	**Mayor**	● Afectación en la ejecución del proceso que repercute en las personas ● Lesiones con incapacidad parcial permanente.	Interrupción de las operaciones de la Institución por más de dos (2) días.	Imagen o credibilidad de la Institución afectada en la región.	Acciones por parte de los entes de control internos o externos que incluyen sanciones medianas.	Pérdidas económicas mayores, entre 51 y 100 SMMLV	Daño ambiental grave recuperable a largo plazo.
20	**Catastrófico**	● Afectación en la ejecución del proceso que repercute en la mayoría de las personas ● Lesiones fatales o con incapacidad total permanente.	Interrupción de las operaciones de la Institución por más de cinco (5) días.	Imagen o credibilidad de la Institución afectada a gran escala.	● Acciones por parte de los entes de control internos o externos que incluyen sanciones significativas ● Intervención por parte de un ente de control u otro ente regulador.	Pérdidas económicas significativas, mayor a 100 SMMLV	Daño ambiental irrecuperable.

Nota. Adaptado de la Guia Externa Admnistración del Riesgo,Función Pública, pág. 40, 2020.

Teniendo en cuenta los parámetros previamente descritos de Probabilidad e Impacto, se identificarán los niveles que apliquen al tipo de riesgo sujeto de análisis y se realizará su calificación a partir del cruce de estas dos variables en la matriz.

Como resultado se ubicarán en los rangos que se fijan en los niveles de severidad y que se les asocia un código de color “tipo” semáforo con el que se establece la severidad del riesgo, donde se tendrían los siguientes rangos:

Tabla 6: Severidad del Riesgo.

Valor	Severidad	Acción
Entre 1 y 5	**Bajo**	Los riesgos en esta zona se encuentran en un nivel que puede reducirse fácilmente con los controles establecidos en la entidad. ***Riesgos aceptables.***
Entre 6 y 15	**Moderado**	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de riesgo baja. ***Riesgos moderados.***
Entre 20 y 50	**Alto**	Deben tomarse las medidas necesarias para llevar los riesgos a la zona de riesgo moderada o baja. ***Riesgos importantes.***
Entre 60 y 100	**Extremo**	Los riesgos en 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. ***Riesgos inaceptables.***

Nota. Adaptado Guia Externa Adminsitracion de Riesgo**,** Función Pública, pág.42, 2020.

Este primer análisis del riesgo se denomina **Riesgo Inherente**, es considerado como una evaluación preliminar en la que la institución busca conocer el comportamiento de los posibles eventos en ausencia de cualquier tipo de control.

Figura 5: Mapa de Calor Riesgo Inherente.

Probabilidad						
	5	5	10	25	50	100
	4	4	8	20	40	80
	3	3	6	15	30	60
	2	2	4	10	20	40
	1	1	2	5	10	20
		1	2	5	10	20
		Impacto				

Fuente: Elaboración propia

Para su calificación, se parte del supuesto que la Institución no cuenta con mecanismos que permitan evitar la probabilidad de ocurrencia de la amenaza o mitigar el impacto de su materialización.

En este caso se asume que no se tienen controles para modificar el riesgo, es por esto que se denomina “riesgo puro”.

Su importancia radica en que permite tener una línea base para evidenciar la evolución del riesgo a través de su proceso de gestión.

4.3.3. Valoración del Riesgo

“*El propósito de la valoración del riesgo es apoyar la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.”* (Norma ICONTEC-NTC 31000, pág.14).

La valoración del riesgo es el producto de confrontar los Riesgos Inherentes con los resultados del análisis de los controles identificados, a fin de determinar la zona de riesgo final llamado **Riesgo Residual**, con el objetivo de acordar prioridades para su manejo.

Identificación de controles: Los controles corresponden a las medidas de tratamiento que permiten modificar el riesgo, debido a que actúan sobre alguna de las dos variables de su medición (probabilidad o impacto), bien sea para detectarlo a tiempo (evitar que se materialice) o reducirlo (minimizar las consecuencias).

Análisis de Controles:

Se tendrá la siguiente tipología de los controles: preventivo, detectivo o correctivo:

Control Preventivo: Evita que un evento suceda. Por ejemplo, el requerimiento de un login y password en un sistema de información es un control preventivo. Éste previene (teóricamente) de que personas no autorizadas puedan ingresar al sistema.

Control Detectivo: Permite registrar un evento después de que ha sucedido, por ejemplo, registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros.

Control Correctivo: Este no prevé que un evento suceda, pero permiten enfrentar la situación una vez se haya presentado. Por ejemplo, en caso de un desastre natural u otra emergencia mediante las pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo, es posible volver a recuperar las operaciones.

Igualmente determinar si son controles:

Controles Automáticos: Utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o con controles de seguimiento para aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos dada su complejidad.

Controles Manuales: Operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

Evaluación del Control:

Se detalla la escala de parámetros para la evaluación del control:

Tabla 7: Parámetros de la evaluación del control.

CARACTERÍSTICAS		DESCRIPCIÓN
Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.
	Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.
	Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.
Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.
	Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.
Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
	Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran en ningún documento propio del proceso.
Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.
	Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo

Nota. Adaptada de la Guía para la Administración del Riesgo, Función Pública, pág. 45,46. 2020.

Como resultado de la evaluación del control se clasifica la eficiencia del control, con esta escala:

Tabla 8: Evaluación del Control.

CALIFICACIÓN DE LA EFICIENCIA DEL CONTROL	RANGO DE EFICIENCIA	DESCRIPCIÓN	DISMINUCIÓN DE LA PROBABILIDAD O EL IMPACTO
Fuerte	**>= 80%**	El control presenta un diseño eficiente y se está ejecutando correctamente.	2
Moderado	**Entre 60% y el 79%**	El control presenta un buen diseño y ejecución, susceptible de ser mejorado, en cualquiera de los dos aspectos.	1
Débil	**<= 59%**	El control presenta deficiencias en su diseño o ejecución.	0

Para establecer la eficiencia del control se debe tener en cuenta los siguientes criterios:

Tabla 9: Criterios de evaluación de controles para la mitigación de riesgos.

Eficiencia del Control	Diseño del control (Documentación + Implementación)	Solidez del Control (Frecuencia)	Resultado (Diseño +Solidez)	Son necesarias acciones
Fuerte **Rango de Eficiencia >=80%**	Fuerte (Siempre se ejecuta)	Fuerte	Fuerte	No
	Moderado (Se ejecuta algunas veces)	Fuerte	Moderado	Sí
	Débil (No se ejecuta)	Fuerte	Moderado	Sí
Moderado **Rango de Eficiencia entre 60% y 79%**	Fuerte (Siempre se ejecuta)	Moderado	Moderado	Sí
	Moderado (Se ejecuta algunas veces)	Moderado	Moderado	Sí
	Débil (No se ejecuta)	Moderado	Débil	Sí
Débil **Rango de Eficiencia <= 59%**	Fuerte (Siempre se ejecuta)	Débil	Débil	Sí
	Moderado	Débil	Débil	Sí
	Débil (No se ejecuta)	Débil	Débil	Sí

Nota. Adaptada de la Política Institucional de Administración de Riesgos en la Universidad del Pacífico, pág. 27.

Los controles diseñados se aplican para disminuir la probabilidad de ocurrencia de un evento que pueda llevar a la materialización de un riesgo.

Para establecer el desplazamiento de la probabilidad y el impacto frente a la evaluación de los controles, se utilizarán los siguientes criterios:

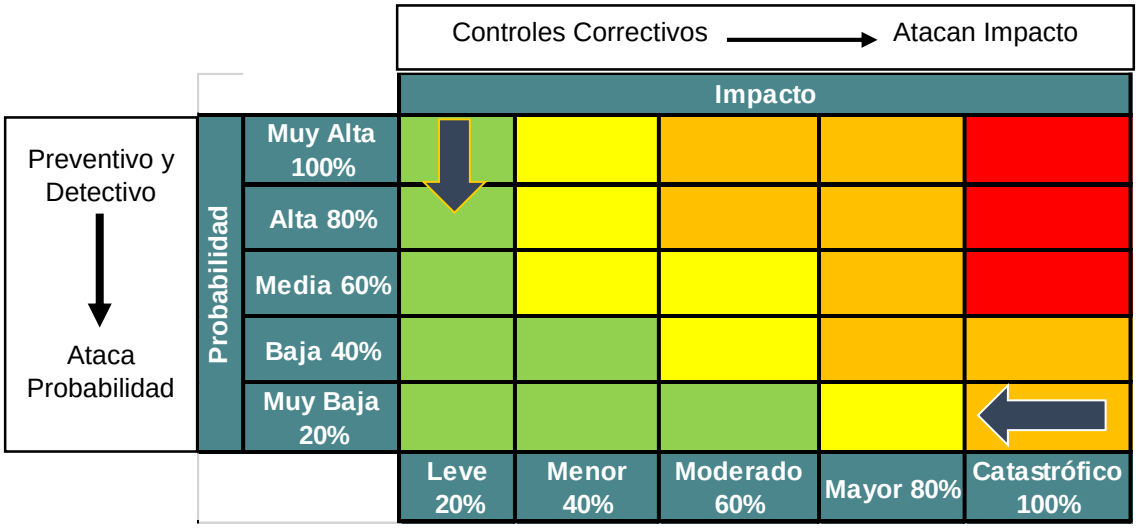
Tabla 10: Criterios para el desplazamiento de la probabilidad o impacto del riesgo después de aplicado el control.

Solidez del Control	Disminuye Probabilidad	Disminuye Impacto	# Columnas de desplazamiento en el Eje de Probabilidad	# Columnas de desplazamiento en el Eje de Impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No Disminuye	2	0
Fuerte	No Disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No Disminuye	1	0
Moderado	No Disminuye	Directamente	0	1

Nota. Adaptada de la Política Institucional de Administración de Riesgos en la Universidad del Pacífico, pág. 29.

Se debe tener en cuenta que, si la solidez del control es débil, no se presenta disminución alguna en el cuadrante de probabilidad o impacto asociado al riesgo analizado.

Figura 7: Movimiento del Mapa de Calor acorde a los controles



Nota. Adaptado de la Guia Externa Admnistración de Riesgos, Función Pública, pág.47, 2020.

Riesgo residual: El riesgo residual es aquel que persiste aún después de haberse aplicado los controles que corresponden con el evento identificado.

5. Nivel aceptable del Riesgos

Los niveles de aceptación del riesgo se determinan como resultado de su valoración, con el fin de generar un grado de confianza razonable en el cumplimiento de los objetivos de la Institución, partiendo de la premisa que el riesgo nunca podrá ser nulo a menos que desaparezca el activo amenazado.

La Institución considera que para los riesgos residuales que queden en la escala de severidad alto o extremo, se realizará una evaluación de riesgos por método cuantitativo con el fin de determinar su impacto. Para ello se utilizarán métodos de evaluación matemática, utilizando factores que detallen el costo estimado del riesgo en su materialización y un análisis del costo beneficio de las medidas que habría que tomar para reducir el impacto del riesgo.

Los factores para tener en cuenta en la magnitud del riesgo estarían enfocados en métodos cuantitativos como por ejemplo el método William T. Fine, que contempla tres factores:

*"**1. Exposición**= Situación del riesgo/Tiempo.*

***2. Probabilidad**= Accidentes esperados/Situaciones de riesgo.*

***3. Consecuencias**= Daño esperado/Tiempo"*.

(Manual para la Formación de Nivel Superior en Prevención de Riesgos Laborales, Métodos de Evaluación de Riesgos Pág. 47, Rubio Juan; 2005).

6. Tratamiento del Riesgo

"El propósito, es seleccionar e implementar opciones para abordar el riesgo". (Norma ICONTEC-ISO 31000, 2018, pag.15).

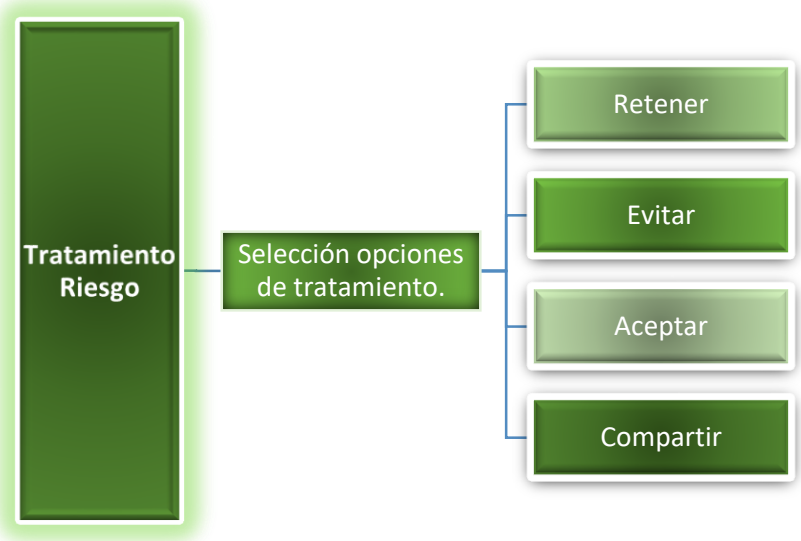
6.1. Selección de opciones de tratamiento del riesgo

"Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para el tratamiento del riesgo pueden implicar una o más de las siguientes:

- *Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo;*
- *Aceptar o aumentar el riesgo en busca de una oportunidad;*
- *Eliminar la fuente del riesgo;*
- *Modificar la probabilidad;*
- *Modificar las consecuencias;*
- *Compartir el riesgo (por ejemplo: a través de contratos, compras de seguros);*

- *Retener el riesgo con base en una desición informada."* (Norma ICONTEC-NTC 31000, 2018, pag.15).

Figura 8. Tratamiento del riesgo.



Fuente: Elaboración Propia.

Como resultado del método cuantitativo aplicado a los riesgos residuales con severidad alto o extremo, se realizará un análisis del costo que implica la adopción de nuevas medidas que permitan modificar los riesgos en contraste con las pérdidas derivadas de su materialización para tomar la decisión de implementarlas o no.

Una vez se defina cuáles son los riesgos que deben recibir tratamiento, se deberá seleccionar la opción de manejo que mejor se adapte a cada riesgo en particular, teniendo en cuenta los siguientes conceptos:

- **Evitar**: Para tomar esta opción de manejo, se debe eliminar la actividad que genera riesgo o sustituirla por otra menos riesgosa.

- **Retener**: Con base en una decisión tomada se espera disminuir el impacto de la materialización del riesgo, debilitando los efectos negativos que repercuten en el activo amenazado.

- **Compartir**: Trasladar a un tercero ajeno al proceso la gestión del riesgo, en este caso lo más común es recurrir a la adquisición de pólizas o seguros.

- **Aceptar**: El riesgo y las consecuencias que conlleve en caso de que se llegue a materializar. Generalmente esta opción se toma cuando la probabilidad es rara y el impacto es insignificante y no se arriesga la estabilidad de la institución, o bien porque el tratamiento es demasiado costoso y no representa un mayor beneficio.

6.2. Preparación e implementación de los planes de tratamiento del riesgo

> "E*l propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado. El plan de tratamiento debería identificar claramente el orden en e cual el tratamiento del riesgo se debería implementar."* (Norma ICONTEC-NTC 31000, 2018, pag.16).

Para los riesgos definidos en zonas de calificación moderado, alto y extremo requieren tratamiento con el objetivo de llevarlos a zona de calificación baja, mientras que los que se encuentran en zona baja deben ser monitoreados y controlados para evitar que se materialicen en el futuro.

Los riesgos que concluyan en el tratamiento de "Retener" se realizaran los planes de acción para cada riesgo, el cual debe contemplar la definición de las actividades para desarrollar en aras de mitigar los riesgos. La estimación y asignación del presupuesto para el plan de tratamiento de riesgos identificados en la institución, corresponderá al líder del macroproceso donde se identificó el riesgo, teniendo presente los recursos: Humanos, Tecnológicos, Logísticos, Financieros.

Las actividades del plan serán medidas y controladas mediante un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación del plan que lleve el riesgo a un nivel aceptable.

7. Seguimiento y Revisión

"*El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficiencia del diseño e implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso de la gestión del riesgo, con responsabilidades claramente definidas."* (Norma ICONTEC-NTC 31000, 2018, pag.17).

Seguimiento a la matriz de riesgos estratégicos liderado por Auditoría Interna con el apoyo de Rectoría a los planes de acción establecidos para la mitigación de los riesgos con una periodicidad semestral, donde se supervise los avances de las actividades por medio de los indicadores establecidos.

Monitoreo de la matriz de riesgos operacionales y efectividad de los controles por medio de auditoría internas, según el plan de auditoria anual, donde el propósito es evaluar su aplicación de los mismos. Dependiendo de los resultados se realizarán

compromisos donde se implementarían actividades con la dinámica de los planes de acción antes mencionados para mantener el nivel de riesgo aceptable.

8. Registro e Informe

Pretende comunicar las actividades de gestión de riesgo y sus resultados a la Institución.

Informe con los resultados de la gestión de riesgo al Consejo Superior por lo menos una vez al año.

Avances de la implementación de la gestión de riesgo al Comité de Auditoría con el fin de tener el concepto y asesoría.

9. Referencias

The Institute Internal of Auditors, 2016, Auditoría Interna y la Segunda Línea de Defensa.

The Institute Internal of Auditors, 2020, El Modelo de las Tres Líneas de Defensa, Una actualización de las tres líneas de defensa.

Comité de Organizaciones Patrocinadoras de la comisión Treadway (COSO), 2013, Marco Integral de Control Interno.

Departamento de la Función pública, Guía Externa para la Administración del Riesgo y el Diseño de Controles en entidades Públicas, 2020.

ICONTEC, Norma Técnica Colombiana NTC-ISO 31000, 2018, Gestión del Riesgo Directrices.

Universidad Nacional de Colombia, Guía para la Administración del Riesgo UN, 2019.

Universidad del Pacífico, Política Institucional de Administración de Riesgos en la Universidad del Pacífico Vr.05, 2020.

Manual para la Formación de Nivel Superior en Prevención de Riesgos Laborales, Rubio Romero Juan Carlos, 2005.