GIR

MARCO INTEGRAL PARA LA GESTIÓN DEL RIESGO

UNAL - MIGR

Lineamientos y pautas metodológicas para el direccionamiento, la articulación y la Gestión Integral de las Tipologías de Riesgos aplicables a la UNAL

Vicerrectoría General
Sistema Integrado de Gestión Académica, Administrativa y Ambiental

siga

UNIVERSIDAD NACIONAL DE COLOMBIA

CONSIDERACIONES GENERALES

El presente documento se elaboró con base en la Guía para la administración de riesgos de procesos UNAL V9[1], la Guía para la gestión de riesgos en proyectos UNAL, referentes internacionales en la materia (Norma Técnica Colombiana ISO 31000:2018, COSO – Gestión del riesgo empresarial Integrando Estrategia y Desempeño 2017) y otras guías de entidades públicas Nacionales[2], con el fin de extender y articular la gestión de riesgos operativos, de corrupción y PAMEC a las demás tipologías de riesgos aplicables a la UNAL, a través de las disposiciones y pautas metodológicas definidas en este documento.

Partiendo de la información contenida en la primera versión de este documento, se procederá con su socialización, retroalimentación, adopción e implementación por parte de los procesos, las estrategias, los proyectos y los sistemas de gestión a cargo de las diferentes tipologías de riesgos aplicables a la UNAL, razón por la cual se encuentra información en construcción asociada, principalmente, a algunas tipologías de riesgos a las que todavía no se ha extendido la gestión de riesgos institucional.

Si bien la información contenida en este documento es de interés general para los procesos, las estrategias, los proyectos y los sistemas de gestión en todos sus niveles de aplicación, la Alta Dirección y, en general, todos los funcionarios de la Universidad Nacional de Colombia que apoyan y/o tienen responsabilidad frente a la gestión del riesgo, está diseñado para los responsables de la segunda línea de defensa de cada tipología de riesgos, quienes deberán facilitar e instruir en el uso de herramientas, métodos, documentos y formatos dirigidos a la implementación de las pautas metodológicas contenidas en este documento a los responsables de la primera línea de defensa a cargo de la identificación y gestión de riesgos.

La Política Integral de Gestión del Riesgo, contenida en el numeral 2.1 de este documento, fue socializada el 28 de abril de 2023 al Comité Nacional de Coordinación del Sistema de Control Interno, de manera que se recibieron las recomendaciones y retroalimentaciones pertinentes. La política será presentada para aprobación de este Comité en las sesiones programadas en el segundo semestre del 2023.

[1] Con la aprobación del presente Marco, la "Guía para la administración de riesgos de procesos UNAL V9" será derogada.

[2] Como la Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 – DAFP, el Manual Sistema Integral de Administración de Riesgos Colpensiones y otras guías o manuales de entidades públicas nacionales con base al Marco COSO ERM 2017 y a la NTC ISO 31000:2018.

CONTENIDO

1 GENERALIDADES

1.1 INTRODUCCIÓN

La Universidad Nacional de Colombia (UNAL), en el propósito de dar cumplimiento a sus funciones misionales y a la normatividad interna y externa aplicable, debe establecer las posibles situaciones adversas que la pueden afectar y pueden llevar a la materialización, el incumplimiento o la pérdida de sus objetivos, estrategias, proyectos de inversión o su reputación, así como a hechos de corrupción, al incumplimiento de reglamentaciones o de seguridad de la información, entre otros, en las diferentes sedes, proyectos, procesos y sistemas. En este sentido, la gestión del riesgo en la UNAL es una tarea que conlleva la gestión de la incertidumbre a la que está expuesta constantemente como organización, por lo que se requiere realizar acciones que seguramente no desaparecerán por completo esta incertidumbre, pero ayudarán a disminuir su probabilidad de ocurrencia y sus múltiples impactos, a fin de garantizar que los objetivos trazados se cumplan.

Esta serie de acciones, a través de las cuales y de forma sistémica se identifican los diferentes eventos adversos que pueden afectar la organización y las acciones para disminuir la probabilidad de ocurrencia o mitigar su impacto, se denomina “gestión del riesgo”. Para esto se requiere del compromiso de toda la comunidad universitaria, no solo en desarrollar esta tarea como una actividad que requieren los diferentes órganos de control y de certificación, sino como una actividad que agrega valor a la gestión y contribuye al cumplimiento de los procesos, los proyectos y las estrategias que se ejecutan en la Universidad, y, por ende, al cumplimiento de sus objetivos misionales y de la normatividad que la rige.

Si, de forma general, se entiende el riesgo como aquel evento que puede afectar el funcionamiento de la institución, se está ante la necesidad de formular acciones que permitan garantizar —hasta donde sea posible— su correcto funcionamiento. Esto, al gestionar los riesgos estratégicos de proyectos que afectan el cumplimiento de los objetivos estratégicos diseñados por la UNAL a través de sus Planes Globales de Desarrollo y el Plan Estratégico Institucional (PLEI); los riesgos de corrupción y fraude que afectan el compromiso legal, la transparencia y la imagen institucional y pueden materializarse en hechos de prevaricato, cohecho, peculado, abuso de autoridad o celebración indebida de contratos; los riesgos de seguridad informática y de la información que comprometen los activos tecnológicos y la confidencialidad, integridad y disponibilidad de la información; los riesgos de seguridad y salud en el trabajo que afectan a todos los miembros de la comunidad universitaria; los riesgos ambientales que repercuten en el ecosistema y las comunidades que los habitan; los riesgos financieros que ponen en riesgo la liquidez y los recursos económicos, así como cualquier otro tipo de riesgo contemplado en el presente Marco Integral para la Gestión del Riesgo UNAL que afecte a la institución.

En un mundo cada vez más incierto, complejo, ambiguo y volátil, donde los contextos de las organizaciones cambian de forma permanente, la gestión del riesgo es trascendental en las organizaciones para garantizar el cumplimiento de las estrategias y los objetivos, crear y proteger el valor, adaptarse con facilidad ante los cambios del entorno interno y externo, integrar y articular las tipologías de riesgos, adaptarse a las mejores prácticas de gestión del riesgo empresarial, fomentar la cultura de gestión del riesgo, disminuir el margen de error frente a la gestión del riesgo, cumplir

las necesidades de los grupos de interés y fortalecer la transparencia, la rendición de cuentas y la toma de decisiones.

Frente a este panorama, y con el fin de contar con una visión holística de la gestión del riesgo en sus diferentes dimensiones, obtener beneficios derivados de su gestión y en pro de integrar en la gestión del riesgo de la UNAL referentes y lineamientos existentes —sin perder de vista las singularidades que requiere gestionar las tipologías de riesgo al interior de la entidad—, se propone el documento MARCO INTEGRAL PARA LA GESTIÓN DEL RIESGO para la Universidad Nacional de Colombia, entendido como el marco de referencia con el cual ***se impartirán los lineamientos, las disposiciones y las pautas metodológicas generales para gestionar el riesgo en los diferentes procesos, sistemas de gestión y otras dependencias responsables de algún tipo de riesgo, lo cual, de acuerdo con lo establecido por la norma internacional ISO 31000, representa el conjunto de componentes que brindan las bases y las disposiciones de la UNAL para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de todas sus instancias.***

1.2 OBJETIVO MIGR UNAL

Establecer los lineamientos y las disposiciones para la articulación y gestión de riesgos a cargo de los procesos, las estrategias, los proyectos y los sistemas de gestión de la Universidad Nacional de Colombia, contribuyendo al cumplimiento de las estrategias y los objetivos misionales, a la reducción de eventos no deseados con sus impactos, a potenciar las oportunidades, la promoción de la cultura de la gestión del riesgo y a la creación y protección del valor. Lo anterior, adaptando al contexto institucional referentes nacionales e internacionales que permitan diseñar, implementar, evaluar, mejorar, integrar y liderar un Marco unificado de políticas, responsabilidades, pautas metodológicas y tipologías de riesgos con el fin de identificar, analizar, valorar, tratar, monitorear, comunicar e informar de manera efectiva los riesgos a los que se expone la UNAL en todos sus niveles de aplicación con base en el apetito, la tolerancia y la capacidad definida.

1.3 ALCANCE MIGR UNAL

El presente documento institucional tiene cobertura en la totalidad de procesos, estrategias, proyectos y sistemas de gestión vigentes, al igual que cobija a todos los miembros y dependencias de la UNAL con responsabilidades frente a la gestión de las tipologías de riesgo.

1.4 SIGLAS Y ABREVIATURAS

CNCSCI: Comité Nacional de Coordinación del Sistema de Control Interno

COSO: Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission)

CSU: Consejo Superior Universitario

DAFP: Departamento Administrativo de la Función Pública

DNEIPI: Dirección Nacional de Extensión, Innovación y Propiedad Intelectual

DNPAA: Dirección Nacional de Personal Académico y Administrativo

DNPE: Dirección Nacional de Planeación y Estadística

ETIR: Equipo Técnico Integral de Riesgos

GNFA: Gerencia Nacional Financiera y Administrativa

ISO: Organización Internacional para la Estandarización

KRI's: Indicadores clave de riesgo

MIGR: Marco Integral para la Gestión del Riesgo UNAL

N/A: No aplica

NTC: Norma Técnica Colombiana

ONCI: Oficina Nacional de Control Interno

QHSV: Quien haga sus veces

SI: Seguridad de la información

SIGA: Sistema Integrado de Gestión Académica, Administrativa y Ambiental

SST: Seguridad y Salud en el Trabajo

UNAL: Universidad Nacional de Colombia

VRA: Vicerrectoría Académica

VRG: Vicerrectoría General

VRI: Vicerrectoría de Investigación

1.5 DEFINICIONES[3]

Apetito de riesgo: nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección.

Capacidad de riesgo: máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

Causa: todos aquellos eventos o factores internos y externos que solos, o en combinación con otros, pueden producir la materialización de un riesgo.

Causa inmediata: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

[3] Definiciones tomadas y/o adaptadas de NTC ISO 31000: 2018, principios y directrices del Icontec; Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 del DAFP.

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

Consecuencia (impacto): 1. Resultado de las causas (eventos) que afectan a los objetivos. **2.** Efectos que puede ocasionar a la organización la materialización del riesgo. **Nota:** una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos. Las consecuencias se pueden expresar de forma cuantitativa o cualitativa.

Control: 1. Medida que mantiene y/o modifica un riesgo. **2.** Medida que permite reducir o mitigar un riesgo. **Nota:** los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo con una frecuencia determinada.

Gestión del riesgo: actividades coordinadas para dirigir y controlar la organización con relación al riesgo. **Nota:** las actividades son de carácter operativo y estratégico.

Marco de referencia o Marco Integral de Gestión del Riesgo: 1. Marco utilizado para asistir a la organización en integrar la gestión del riesgo en todas sus actividades, funciones, procesos y sistemas de gestión, considerándose clave el apoyo de la alta dirección. **2.** Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización.

Nivel de riesgo: valor numérico obtenido al calificar el riesgo por medio de la combinación (cruce o multiplicación) de la probabilidad de ocurrencia del evento con la magnitud de los impactos (consecuencias o efectos) que el evento traería en el cumplimiento de los objetivos y los procesos, las estrategias, los proyectos y los sistemas de gestión de la Universidad. **Nota**. el nivel de riesgo se obtiene en dos momentos: 1. Antes del uso de controles (llamado “nivel de riesgo inherente”); 2. después del uso de controles (llamado “nivel de riesgo residual”).

Niveles de aceptabilidad: nivel de gravedad obtenido al operar o ubicar en el mapa de calor el nivel de riesgo.

Mapa de calor: elemento que permite visualizar de forma gráfica la ubicación y distribución de los riesgos inherentes y residuales (perfil de riesgo), teniendo en cuenta su nivel de riesgo y el correspondiente nivel de aceptabilidad.

Perfil de riesgo: resultado consolidado de la medición permanente de los riesgos a los que se ven expuestos los procesos, las estrategias, los proyectos, los sistemas de gestión y, en general, la institución. Nota: el perfil de riesgo se determina con la evaluación del nivel de riesgo inherente y residual.

Política de gestión del riesgo: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Probabilidad: posibilidad de que algo suceda.

Riesgo: 1. Efecto de la incertidumbre sobre los objetivos. **Nota:** un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en

oportunidades y amenazas (abarcando eventos o causas). Los objetivos pueden tener diferentes aspectos y categorías y se pueden aplicar a diferentes niveles. Con frecuencia el riesgo se expresa en términos de sus causas, su probabilidad de ocurrencia y sus consecuencias.

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de proyectos: cualquier amenaza o conjunto de amenazas que se pueden llegar a materializar de forma que afectan el objetivo, las metas, las actividades, los entregables, los recursos o los activos asociados al proyecto. **Nota:** en los riesgos de proyectos las amenazas hacen referencia a las causas o los factores internos y externos que pueden ocurrir y afectar el proyecto.

Riesgo de seguridad de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o un daño en un activo de información. **Nota:** en los riesgos de seguridad de la información las causas conocidas como agentes generadores se dividen en amenazas y vulnerabilidades; las amenazas son propiamente las causas y las vulnerabilidades aquellas debilidades de la entidad que pueden ser explotadas para ocasionar dichas amenazas.

Riesgo inherente: 1. Evaluación preliminar en la que una organización busca conocer el comportamiento y el nivel de riesgo de los posibles eventos en ausencia de cualquier tipo de control. **2.** Nivel de riesgo propio resultante de combinar la probabilidad con el impacto en ausencia de mecanismos de control. **Nota:** el riesgo inherente constituye una parte del perfil de riesgo.

Riesgo residual: 1. Es el nivel de riesgo resultante de aplicar la efectividad de los controles al riesgo inherente. **Nota:** el riesgo residual constituye una parte del perfil de riesgo.

Tolerancia de riesgo: valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

1.6 DOCUMENTOS DE REFERENCIA

Para la construcción del MIGR se tomaron como base, primero, las guías elaboradas en años anteriores en la institución, y, segundo, los referentes y las metodologías nacionales e internacionales en gestión del riesgo que se enlistan a continuación.

- Universidad Nacional de Colombia. *Guía para la administración de riesgos de procesos UNAL V9*. 2021
- Universidad Nacional de Colombia. *Guía para la gestión de riesgos en proyectos UNAL V0*. 2022
- Instituto Colombiano de Normas Técnicas y Certificación – Icontec. *Norma Técnica Colombiana NTC-ISO 31000 Gestión del riesgo - principios y directrices.* 2018.
- Committee of Sponsoring Organizations of the Treadway Commission - COSO. *Enterprise Risk Management Integrating with Strategy and Performance - COSO ERM*. 2017.
- Comité de Organizaciones Patrocinadoras de la Comisión Treadway - Committe Of Sponsoring Organizations of the Treadway Commission - COSO. *Gestión del riesgo empresarial - Aplicación de la gestión del riesgo empresarial a los riesgos relacionados con factores medioambientales, sociales y de gobierno.* 2018.

- Comité de Organizaciones Patrocinadoras de la Comisión Treadway - Committe Of Sponsoring Organizations of the Treadway Commission - COSO. *Gestión del riesgo empresarial integrando estrategia y desempeño Resumen ejecutivo*.
- Departamento Administrativo de la Función Pública. *Guía para la administración del riesgo y el diseño de controles en entidades públicas V5.* 2020.
- Colpensiones. *Manual Sistema Integral de Administración de Riesgos.*

1.7 Marco Legal

La normatividad interna y externa que conforma el presente MIGR y regula de manera transversal la gestión de riesgos de la Universidad Nacional de Colombia es se expone en la tabla 1[4].

Tabla 1 Normograma interno y externo aplicable al MIGR UNAL

Normativa	Emitida por	Origen	Descripción Normativa
Ley 87 de 1993	Gobierno Nacional – Congreso de Colombia	Externa	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2, literal a) proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2, literal f) definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 489 de 1998	Gobierno Nacional – Congreso de Colombia	Externa	Por la cual se dictan normas sobre la organización y el funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones. Capítulo VI. Sistema Nacional de Control Interno.
Ley 1474 de 2011	Gobierno Nacional – Congreso de Colombia	Externa	Estatuto Anticorrupción. Art 73. Plan Anticorrupción y de Atención al Ciudadano: señala la obligatoriedad para cada entidad del orden nacional, departamental y municipal de elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano; entre sus componentes se encuentran el Mapa de Riesgos de Corrupción y las medidas para mitigar estos riesgos. Modificado por la Ley 2195 de 2022.
Decreto 1083 de 2015	Presidencia de la Republica - DAFP	Externa	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Artículo 2.2.21.5.4. Administración del riesgo como para integral del fortalecimiento de los sistemas de control interno en las entidades públicas. Modificado por el Decreto 1499 de 2022 y modificado transitoriamente por el Decreto 1507 de 2022.
Decreto 648 de 2017	Presidencia de la Republica – DAFP	Externa	Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública. Artículo 2.2.21.1.6 Funciones del Comité Institucional de Coordinación de Control Interno, literal g) someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
Decreto 1499 de 2017	Presidencia de la Republica	Externa	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Resolución 316 de 2018	Rectoría	Interna	Por la cual se actualiza el Sistema de Control Interno de la Universidad Nacional de Colombia y se derogan las Resoluciones de Rectoría 1428 de 2006 y 139 de 2018. Artículo 8, Comités de Coordinación del Sistema de Control Interno de la Universidad Nacional de Colombia. Numeral 8, un Comité Nacional de Coordinación del Sistema de Control Interno, el cual adoptará un reglamento

[4] La normatividad aplicable a la gestión del riesgo institucional es cambiante según las disposiciones de la UNAL y de entes gubernamentales.

Normativa	Emitida por	Origen	Descripción Normativa
			mediante acto administrativo de la Rectoría y tendrá las siguientes funciones: literal f) someter a aprobación del Señor Rector la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
Ley 2195 de 2022	Gobierno Nacional – Congreso de Colombia		Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. Modificado por el decreto 1463 de 2022.
Resolución 605 de 2022	Rectoría	Interna	Por la cual se define, se estructura y se establecen roles y responsabilidades del Sistema Integrado de Gestión Académica, Administrativa y Ambiental - SIGA, de la Universidad Nacional de Colombia y se derogan las disposiciones que le sean contrarias. Deroga la resolución de Rectoría 1528 de 2018.

Además, son aplicables los documentos elaborados por el DAFP relacionados con el Modelo Integral de Planeación y Gestión MIPG, principalmente los asociados a la Dimensión 7 – Control Interno.

Considerando las particularidades de la institución, cada tipología de riesgos puede contener, además de la normatividad descrita en la tabla anterior, una regulación complementaria aplicable a su gestión según su naturaleza[5].

1.8 BENEFICIOS MIGR

Gestionar el riesgo a través de un MIGR no solo permite integrar y articular los procesos, las estrategias, los proyectos y los sistemas de gestión de la UNAL bajo unos lineamientos y unas pautas metodológicas comunes y particulares para identificar y dar respuesta a los eventos adversos que pueden perjudicar a la institución, sino que también produce trece beneficios que contribuyen al mejoramiento y fortalecimiento de la institución:

- Crea y proteger el valor en la UNAL.
- Articula y optimiza la estrategia y el desempeño con la gestión del riesgo en los procesos, proyectos y sistemas de gestión de la UNAL en todos sus niveles de aplicación.
- Contribuye a acelerar el crecimiento, fomentar la cultura de gestión del riesgo, mejorar el desempeño y fomentar la innovación en el interior de la organización.
- Integra la gestión del riesgo en las actividades y funciones más importantes de la institución.
- Fomenta la participación de la Alta Dirección en la toma de decisiones estratégicas frente a la gestión del riesgo y el tratamiento de eventos con un impacto significativo.
- Facilita el diseño y la implementación de un enfoque estructurado para la gestión del riesgo.
- Gestiona la incertidumbre frente al apetito, la tolerancia y la capacidad definida por la Alta Dirección.

[5] Tal como es el caso de los riesgos, en proyectos de inversión donde aplica la normatividad relacionada con el Banco de proyectos de la UNAL (resoluciones de Rectoría 418 de 2000 ,165 de 2005, 309 de 2009, entre otras); los proyectos de extensión donde es requerida la normatividad del ente contratante y otra normativa interna como la Resolución del Manual de Convenios y Contratos de la UNAL y el Acuerdo 036 de 2009 del CSU que reglamenta la Extensión en la UNAL; los riesgos se seguridad social en salud - PAMEC - que también son regulados por el Decreto 780 de 2916 del Ministerio de Salud y Protección Social.

- Contribuye al logro de los objetivos, las estrategias, los proyectos, procesos y fines misionales.
- Aporta información de valor para los procesos, las estrategias, proyectos y sistemas de gestión.
- Aumenta la confianza de los grupos de interés y blinda a la Universidad ante sus requerimientos.
- Fomenta el autoconocimiento de la Universidad y el pensamiento basado en riesgos dentro de la institución.
- Permite a largo plazo mejorar la resiliencia de la institución y su capacidad de anticipar y responder ante el cambio al considerar cómo este podría afectar el desempeño, y exigir así ajustes en la estrategia[6].
- Aumenta los resultados positivos y las ventajas, a la vez que reduce las sorpresas negativas[7].

[6] Adaptado de COSO ERM Gestión del riesgo empresarial integrando estrategia y desempeño, resumen ejecutivo, pagina 3.

[7] La gestión del riesgo empresarial permite a las entidades mejorar su capacidad para identificar riesgos y establecer respuestas adecuadas, reduciendo las sorpresas y los costes o las pérdidas relacionados, al tiempo que se benefician de los nuevos desarrollos (tomado de COSO ERM Gestión del riesgo empresarial integrando estrategia y desempeño, resumen ejecutivo, página 3).

2 GESTIÓN INTEGRAL DEL RIESGO

La gestión integral del riesgo en la UNAL propuesta en el presente MIGR se alcanza por medio de un ciclo de mejora continua (PHVA) para el diseño (definición), implementación, verificación y mejora de: 1. La Política integral de gestión del riesgo; 2. Las tipologías de riesgos asignadas a procesos, estrategias, proyectos y sistemas de gestión pertinentes; 3. El modelo de las Tres Líneas de Defensa con los roles y responsabilidades; y 4. Las pautas metodológicas generales y particulares para su gestión.

2.1 POLÍTICA INTEGRAL DE GESTIÓN DEL RIESGO

La Política Integral de Gestión del Riesgo es un elemento clave del MIGR que contiene la declaración de la dirección y las intenciones generales de la UNAL con respecto a la gestión del riesgo. Se complementa con las pautas metodológicas para la gestión de las tipologías de riesgos que son aplicadas por los funcionarios de los procesos, las estrategias, los proyectos y los sistemas de gestión; esta política integral está compuesta por:

2.1.1 Declaración (objetivo general)

La Universidad Nacional de Colombia se compromete con la probidad institucional, la integridad académica y la previsión de los riesgos, mediante el monitoreo permanente para la mejora continua y el fortalecimiento del desempeño, el desarrollo de competencias en las personas, la creación y protección de valor y la transparencia en la gestión institucional, a través de pautas metodológicas para la administración colectiva e individual del riesgo, estableciendo acciones y controles dirigidos a la gestión priorizada, de acuerdo con la probabilidad y el impacto.

2.1.2 Pilares de la gestión del riesgo

En la redacción de la declaración de la Política integral de gestión del riesgo se aprecian tres pilares: compromiso, acciones y beneficios, tal como se aprecia en la ilustración 1.

Ilustración 1 - Pilares de la Política Integral de Gestión del Riesgo

2.1.3 Objetivos específicos

1. Direccionar la articulación de la gestión del riesgo institucional a través de la emisión de lineamientos y pautas metodológicas que permitan a encargados de los procesos, las estrategias, los proyectos y sistemas de gestión, e implementar un proceso ordenado y sistemático acorde a sus particularidades para la administración de sus tipologías de riesgo, controles y planes asociados.
2. Fortalecer y direccionar la gestión de riesgos de procesos por medio de estrategias de monitoreo y acompañamiento.
3. Contribuir con la cultura de transparencia, la cultura de gestión de riesgos y el reporte de eventos materializados en el interior de la UNAL.

2.1.4 Principios y disposiciones generales para la gestión integral del riesgo

2.1.4.1 Para la definición, la operación y el seguimiento de la Política Integral de Gestión del Riesgo

Buscando aumentar el valor de la gestión del riesgo realizada por funcionarios de los procesos, las estrategias, los proyectos y sistemas de gestión en los que recaen las tipologías de riesgos, e integrar a la Alta Dirección representada por el Comité SIGA en las actividades estratégicas, se han establecido las siguientes disposiciones para la definición, la operación y el seguimiento de la Política Integral de Gestión del Riesgo que se implementa a través del MIGR:

- Las máximas instancias frente a la gestión del riesgo institucional son el Comité Nacional de Coordinación del Sistema de Control Interno y el Comité SIGA; este último será apoyado técnicamente por el Equipo Técnico Integral de Riesgos - ETIR.
- La Política Integral de Gestión del Riesgo debe ser elaborada o actualizada cada trienio por parte del Equipo Técnico Integral de Riesgos, así como revisada y aprobada por el Comité Nacional de Coordinación del Sistema de Control Interno.
- La Coordinación SIGA, por medio de un instrumento previamente aprobado por el Comité SIGA, realizará seguimiento semestral al cumplimiento de los objetivos de la Política Integral de Gestión del Riesgo, reportando el informe o los resultados del seguimiento al ETIR.
- El Equipo Técnico Integral de Riesgos semestralmente revisará el informe de seguimiento al cumplimiento de la Política Integral de Gestión del Riesgo realizado por la Coordinación SIGA, en el cual plasmarán sus observaciones y acciones de mejora sugeridas para fortalecer la gestión del riesgo y garantizar el cumplimiento de los indicadores y las actividades asociadas a los objetivos de dicha política. Como cuerpo asesor del Comité SIGA reportará a este último, con el fin de mantenerlo informado sobre el cumplimiento de la política, eventos de riesgos materializados y comportamientos de riesgos significativos, de tal forma que la gestión de riesgos contribuya a la toma de decisiones.
- El ETIR deberá garantizar de manera razonable que la gestión integral de riesgos dispuesta en el MIGR esté alineada con la estrategia, la misión, la visión y los valores de la institución.
- El Comité SIGA deberá verificar que el apetito, la tolerancia y la capacidad del riesgo estén correctamente alineados con el contexto organizacional, las intenciones de la Alta Dirección, y la capacidad operativa y estratégica de la institución; para ello se apoyará del ETIR.

2.1.4.2 Para la toma de decisiones frente a la gestión del riesgo por parte de la Alta Dirección

Si bien la elaboración, actualización y aprobación del MIGR con su Política Integral es fundamental para la integración, el diseño, la implementación, la valoración y mejora de la gestión del riesgo en la institución es crucial para la Universidad. De esta manera, a partir del MIGR y la gestión realizada desde los procesos, las estrategias, los proyectos y sistemas de gestión dirigidos a la identificación, el análisis, la valoración, la comunicación, el tratamiento, el monitoreo y el registro e informe de sus tipologías de riesgos, la Alta Dirección, representada por el Comité SIGA, tomará decisiones estratégicas y metodológicas que: 1. Aporten valor a la gestión del riesgo; 2. Den direccionamiento y lineamientos frente a dicha gestión; y 3. Dictaminen el curso de acción a seguir ante ciertos eventos posibles o materializados que puedan afectar de forma significativa a la institución, para lo cual se han establecido los siguientes mecanismos dirigidos al fortalecimiento de la toma de decisiones por parte de la Alta Dirección:

- EL Comité SIGA y el ETIR deben apropiarse y concientizarse del MIGR UNAL aplicable a todos los tipos de riesgos existentes, teniendo una forma de actuar coherente con las responsabilidades asignadas.
- Los informes de gestión de riesgos deben ser revisados por el ETIR y el Comité SIGA de manera anual, de modo que realicen observaciones y recomendaciones pertinentes que contribuyan al fortalecimiento de la gestión del riesgo y aporten a la protección - creación de valor institucional.

- El Equipo Técnico Integral de Riesgos debe analizar, tomar acciones y establecer el curso a seguir frente a los riesgos residuales significativos —posibles o materializados— que puedan ser o suponer un peligro extremo para la institución. Para aquellos riesgos residuales significativos que el ETIR no pueda tomar ninguna acción, se deben escalar y comunicar al Comité SIGA para su análisis y toma de decisiones correspondiente[8].

2.1.4.3 De alcance y cumplimiento frente al MIGR

- La Gestión integral del riesgo en la UNAL está inmersa en todos los procesos y sistemas de gestión de la institución, incluyendo el direccionamiento estratégico y la formulación y gerencia de proyectos.
- Los responsables de cada tipología de riesgos contenida en el MIGR deberán adoptar e integrar en su gestión los lineamientos establecidos en el presente MIGR; además, deberán desarrollar y actualizar en dicho MIGR, con la asesoría de la Coordinación SIGA Nivel Nacional, aquellos que sean necesarios para su revisión por parte del ETIR y con aprobación por parte del Comité SIGA.
- La metodología definida para la gestión integral del riesgo debe permitir priorizar aquellos eventos más significativos a los que se expone la UNAL, centrando los esfuerzos, primero, en los riesgos estratégicos, sin descuidar los de los procesos, proyectos y demás tipologías contenidas en el MIGR.
- Los líderes y funcionarios de los procesos, las estrategias, los proyectos y sistemas de gestión deben dar cumplimiento a los principios, a los lineamientos y las pautas metodológicas contenidos en el presente MIGR, e implementar los mecanismos definidos para resolver los conflictos de interés en la gestión de riesgos, principalmente los relacionados con riesgos materializados y riesgos residuales significativos[9]; de no hacerlo se expone a la UNAL a eventos adversos de impacto alto o catastrófico.

2.1.4.4 De competencia y capacitación en gestión del riesgo y en el MIGR

- La capacitación y el desarrollo de competencias frente a la gestión integral del riesgo es obligatoria para todos los servidores públicos de la UNAL.
- Los integrantes del Comité SIGA, por medio del ETIR y la Coordinación SIGA, deberán apropiarse y capacitarse en el MIGR, principalmente en lo que compete a sus responsabilidades frente a la gestión del riesgo y la toma de decisiones.
- El ETIR debe estar integrado por funcionarios con conocimientos, habilidades y experiencia en la gestión del riesgo, preferiblemente con experiencia en la materia en el interior de la institución o en otras entidades de educación superior. Los integrantes del ETIR serán delegados por el Comité SIGA con la participación de los responsables de las tipologías de riesgo.
- Cada vez que se presente un cambio en los integrantes que conforman el Comité SIGA o el ETIR, el ETIR —por el mecanismo que defina y/o con el apoyo de la Coordinación SIGA Nivel

[8] Para aquellos riesgos residuales significativos posibles o materializados que el Comité SIGA no pueda tomar ninguna acción, se podrán escalar y comunicar al CNCSCI para su análisis y toma de decisiones correspondiente.
[9] Es una omisión grave frente a la gestión del riesgo institucional no informar oportunamente la materialización de un riesgo, así como los riesgos residuales significativos.

Nacional— deberá dar inducción a los nuevos integrantes en un tiempo no mayor a tres meses a partir de su llegada, principalmente en sus responsabilidades frente al MIGR, la Política Integral de Gestión del Riesgo y las tipologías de riesgos aplicables a la UNAL.

- La Coordinación SIGA, de la Mano de la Dirección Nacional de Personal Académico y Administrativo, con la participación de los principales responsables de cada tipología de riesgos, deben planificar y ejecutar anualmente el plan de capacitación de gestión integral del riesgo, por el cual se brinde capacitación y entrenamiento en el MIGR y en cada una de las tipologías de riesgos que lo componen.
- La Alta Dirección de la institución, representada por el Comité SIGA, de la mano de la Dirección Nacional de Personal Académico y Administrativo y la Gerencia Nacional Financiera y Administrativa, deben promover y facilitar los medios necesarios para el desarrollo de competencias frente a la gestión del riesgo en los líderes y funcionarios de los procesos, las estrategias, los proyectos y sistemas de gestión de la institución.
- En la medida de las posibilidades, la Alta Dirección desde la DNPAA deberá desarrollar estrategias con el fin de atraer, formar y retener talento humano competente en materia de gestión del riesgo al interior de la UNAL.

2.1.4.5 De documentación y uso de sistemas de información para la administración de riesgos

- El MIGR es elaborado y actualizado por la Coordinación SIGA Nivel Nacional[10], revisado por el ETIR y aprobado por el Comité SIGA[11], y publicado en el módulo de documentos del sistema de información Institucional SoftExpert, según lo dispuesto para la gestión de documentos controlados por parte del proceso Gestión Documental.
- Se debe registrar, almacenar y mantener disponible para consulta de partes internas y externas[12] la información de la gestión de los diferentes tipos de riesgos, en la medida de lo posible, en el sistema de información institucional SoftExpert o en otros sistemas de información institucionales parametrizados para ello[13]. Cuando no sea posible, se debe mantener en documentos electrónicos que permitan su modificación e interpretación, garantizando el respaldo (*backup*) de dicha información y su divulgación en la comunidad UNAL.
- Los responsables de la segunda línea de defensa de cada tipología contenida en el MIGR deben facilitar e instruir en el uso de herramientas, métodos, documentos y formatos para la gestión de sus riesgos, así como la implementación de las pautas metodológicas contenidas en cada una de las etapas del numeral 2.4,"Metodología integral para la gestión de riesgos", brindando asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su gestión.

[10] Es elaborado y actualizado con aportes de los líderes e integrantes de los procesos, estrategias, proyectos y sistemas de gestión.
[11] Las actualizaciones al MIGR deben acompañarse de una estrategia de capacitación e implementación para garantizar en la media de lo posible la adopción de los cambios en la gestión de riesgos realizada por los líderes y funcionarios de los procesos, estrategias, proyectos y sistemas de gestión.
[12] La divulgación de información a partes internas y externas estará regulada y limitada por la Ley 1712 del 2014.
[13] Previo al cargue de la información en los sistemas de gestión de riesgos, los líderes y responsables de los procesos, estrategias, proyectos y sistemas de gestión podrán utilizar diferentes herramientas para recopilar la información.

- Las herramientas, los documentos y los formatos elaborados por los responsables de la segunda línea de defensa de las tipologías de riesgos para facilitar la implementación y recolección de información del proceso con miras a la gestión del riesgo contenido en el numeral 2.4, "Metodología para la gestión integral de riesgos", deben ser revisados y retroalimentados —según su nivel de importancia— por la Coordinación SIGA, Nivel Nacional o el ETIR, con el fin de que estén articulados con la política, los principios y las pautas metodológicas contenidas en el presente MIGR.

2.1.4.6 *De comunicación y administración/intercambio de información resultante de la gestión del riesgo*

- Es indispensable el uso de los canales y medios de comunicación institucionales durante el proceso permanente de obtención y el intercambio de información de la gestión del riesgo realizada desde los procesos, las estrategias, los proyectos y sistemas de gestión, así como que fluya de manera ascendente y descendente por todos los niveles de aplicación de la UNAL[14].
- Los responsables de cada tipología de riesgos deberán enviar un informe anual/semestral de la gestión de riesgos realizada a la Coordinación SIGA Nivel Nacional, la cual elaborará el informe consolidado que será revisado y analizado por el ETIR para la aprobación y presentación de resultados al Comité SIGA.
- El MIGR y los resultados de la gestión integral del riesgo deben ser difundidos a los diferentes actores involucrados para su análisis y toma de decisiones, a través de los canales y medios de comunicación institucionales establecidos para ello.

2.1.4.7 *De gobierno y cultura en la gestión integral del riesgo*

- La alta dirección, representada por el Comité SIGA, apoyada por el ETIR, deberán dar lineamientos para administrar los recursos disponibles en la gestión integral del riesgo, centrándose en promover la cultura de la gestión del riesgo e implementar el MIGR, con base en los principios de autogestión, autocontrol y autorregulación.
- La Alta Dirección y el Comité SIGA, en apoyo del ETIR, deberán promover e incentivar estrategias dirigidas a fortalecer la cultura de la gestión integral del riesgo en el interior de la UNAL y en las terceras partes que tengan alto impacto o influencia en las actividades y los objetivos de la institución.
- La cultura de gestión integral del riesgo debe incorporar la evaluación del riesgo en la toma de decisiones estratégicas y otras significativas del ETIR y el Comité SIGA, analizando las causas, las consecuencias, los controles, los planes de acción y los indicadores de los eventos posibles o materializados más significativos, con relación a las afectaciones en las estrategias y los objetivos institucionales definidos.
- La cultura de gestión integral del riesgo debe articularse con el compromiso y los valores éticos definidos por la UNAL.

[14] Los niveles de aplicación van desde el nivel nacional y sedes hasta llegar a las facultades, centros e institutos.

2.2 TIPOLOGÍAS DE RIESGOS CONTENIDAS EN EL MIGR UNAL

Considerando que el MIGR UNAL se concibe como una estructura de alto nivel en la que se integran las tipologías de riesgos y las pautas metodológicas para su administración, con sus respectivos procesos, estrategias, proyectos y sistemas de gestión responsables, es elemental definir las tipologías de riesgos vigentes y aplicables a la gestión del riesgo institucional, las cuales se muestran en la tabla 2.

Tabla 2 - Tipologías de riesgos contenidas en el MIGR UNAL

Tipo de riesgo	**Sistemas/instancias responsables[15]**
Riesgos estratégicos	Dirección Nacional de Planeación y Estadística, Vicerrectoría General, Vicerrectoría Académica, Vicerrectoría de Investigación, Secretaría General, Rectoría, Consejo Superior Universitario, Gerencia Nacional Financiera y Administrativa, Vicerrectorías de sede y Direcciones de sedes de presencia Nacional, líderes de los procesos estratégicos.
Riesgos de proyectos	Dirección Nacional de Planeación y Estadística, Vicerrectoría de Investigación, Dirección Nacional de Extensión, Dirección Nacional de Investigación y Laboratorios, directores, supervisores e interventores de los proyectos. Comités y otros[16].
Riesgos de seguridad de la información (SI)	Dirección Nacional de Estrategia Digital, Sistema de Gestión de Seguridad de la Información, dueños o propietarios de los activos de información y de procesamiento de información.
Riesgos de fraude, lavado de activos (LA), financiación del terrorismo (FT) y financiamiento de la proliferación de armas de destrucción masiva (FPADM).	Gerencia Nacional Financiera y Administrativa[17]
Riesgos de procesos (operativos y de corrupción, de atención al paciente PAMEC)	Líder SGC Nivel Nacional, Sistemas de Gestión de Calidad (Coordinaciones del SGC en sede), líderes y funcionarios de los procesos, Unisalud.
Riesgos de seguridad y salud en el trabajo (SST)	Sistema de Gestión y Seguridad y Salud en el Trabajo, divisiones o secciones de SST nivel nacional y sedes, direcciones de personal nivel nacional y sedes, unidades de gestión integral de las sedes de presencia nacional.

[15] Los responsables para cada tipo de riesgos son aproximados y pueden cambiar de acuerdo con la normatividad interna y la regulación externa aplicable a la UNAL; solo se mencionan las principales instancias y los principales sistemas de gestión. Se puede consultar con detalle todas las instancias implicadas en la gestión integral del riesgo en el numeral 2.3 Modelo de las tres líneas de defensa – Roles y responsabilidades.
[16] Los otros actores involucrados en la gestión de riesgos en proyectos se pueden consultar en el numeral 2.3 Modelo de las tres líneas de defensa – Roles y responsabilidades.
[17] Responsable sugerido según la naturaleza de los riesgos; se encuentra pendiente por validar los actores involucrados en la gestión de esta tipología de riesgos.

Tipo de riesgo	Sistemas/instancias responsables[15]
Riesgos ambientales	Sistema de Gestión ambiental, comité técnico nacional de gestión ambiental, jefes de oficinas de gestión ambiental y/o responsables de gestión ambiental de las sedes, al igual que líderes de los procesos.

Es posible que, dada la naturaleza, las características y el alcance particular de cada riesgo, existan algunos que se relacionen a más de una tipología; por ejemplo, un riesgo estratégico podría ser también un riesgo de seguridad de la información o un riesgo ambiental; un riesgo de proyecto podría ser un riesgo estratégico si este consiste en invertir un alto monto de recursos en desarrollar/adquirir un sistema de información, y a la vez un riesgo de seguridad de la información teniendo en cuenta los diferentes eventos que podrían ocurrir a la hora de adquirir o desarrollar dicho sistema. En la ilustración 2 se muestra una matriz relacional entre las tipologías de riesgos vigentes contenidas en el MIGR UNAL.

Ilustración 2 - Matriz relacional entre las tipologías de riesgos contenidas en el MIGR UNAL

	Estratégicos	Proyectos	Operativos (Procesos)	Corrupción (Procesos)	Fraude LA y FT	Seguridad y salud trabajo	Seguridad información	Ambientales
Estratégicos	-							
Proyectos		-						
Operativos (procesos)			-					
Corrupción (procesos)				-				
Fraude, LA y FT					-			
SST						-		
SI							-	
Ambientales								-

2.3 Modelo de las Tres Líneas de Defensa - Roles y responsabilidades

Los roles y las responsabilidades para una gestión integral del riesgo en la UNAL han sido definidos con base en el modelo de las tres líneas de defensa, en pro de articular y orientar a los líderes y

gestores de los procesos, las estrategias, los proyectos y sistemas de gestión en la administración y el escalamiento de sus riesgos, fundamentado en el autocontrol, la autoevaluación y la evaluación independiente.

A continuación, se muestran para cada línea de defensa los actores involucrados con sus responsabilidades, partiendo de aquellos trasversales a todas las tipologías de riesgos, hasta los encargados de la identificación y el autocontrol de riesgos de cada categoría.

2.3.1 Línea estratégica

Es la encargada del direccionamiento y la definición de la estrategia institucional para la gestión integral del riesgo. Está conformada por el Comité Nacional de Coordinación del Sistema de Control Interno y el Comité SIGA, y tiene como responsabilidad principal "definir el Marco Integral para la Gestión del Riesgo y el Control".

Tabla 3 - Línea estratégica – responsables y responsabilidades aplicables a la UNAL

Responsables	Responsabilidades
Comité SIGA	***Definir el MIGR y control y supervisar su cumplimiento*** - Revisar y aprobar el Marco Integral para la Gestión del Riesgo. - Tomar decisiones frente a los resultados del seguimiento de la Política Integral de Gestión del Riesgo. - Analizar y tomar acciones frente a los riesgos residuales significativos que hayan sido escalados del ETIR. - Analizar y tomar acciones frente a la gestión de riesgos materializados de alto impacto a nivel de procesos, estrategias, proyectos o de alcance institucional que hayan sido escalados del ETIR.
Comité Nacional de Coordinación del Sistema de Control Interno - CNCSCI	- Presentar ante aprobación del representante legal la Política Integral de Gestión del Riesgo. - Tomar acciones frente a la gestión de riesgos materializados de alto impacto en el nivel de procesos, estrategias, proyectos o de envergadura institucional que hayan sido escalados por el Comité SIGA.

2.3.2 Tercera línea de defensa - Evaluación independiente a la gestión de riesgos

Conformada por la Oficina Nacional de Control Interno, esta línea de defensa, a través de la evaluación, la auditoría, el seguimiento y acompañamiento independiente, busca evaluar la efectividad del sistema de control interno con un enfoque basando en riesgos, generando alertas y recomendaciones para evitar posibles incumplimientos o la gestión incorrecta de eventos significativos —posibles o materializados— en los diferentes procesos, estrategias, proyectos y sistemas de gestión que componen la Universidad.

Tabla 4 - Tercera línea de defensa: responsables y responsabilidades aplicables a la UNAL

Responsables	Responsabilidades

Oficina Nacional de Control Interno - ONCI	***Evaluación de la efectividad del sistema de control interno con un enfoque basado en riesgos*** - Funciones propias de evaluación independiente a los procesos, las estrategias, los proyectos y sistemas de gestión realizadas a través de: - Auditorías - Seguimiento independiente - Acompañamiento independiente - Dar recomendaciones a los procesos, las estrategias, los proyectos y sistemas de gestión para evitar incumplimientos y/o gestionar riesgos significativos posibles o materializados.

2.3.3 Segunda línea de defensa - Autoevaluación, acompañamiento y seguimiento a la gestión de riesgos

Conformada de manera transversal por el Equipo Técnico Integral de Riesgos y la Coordinación SIGA Nivel Nacional, y de manera particular por los principales responsables de cada una de las tipologías de riesgos que integran el MIGR, es la encargada de realizar la autoevaluación, el acompañamiento, la asesoría y el seguimiento a la primera línea de defensa en la implementación de las pautas metodológicas, las herramientas y los lineamientos para la gestión integral y particular de riesgos; en esta línea recae la responsabilidad de asesorar al Comité SIGA, desarrollar herramientas y documentos para facilitar la gestión de riesgos y elaborar informes con los resultados de la gestión del riesgo realizada por los procesos, las partes estratégicas, los proyectos y sistemas de gestión a la Alta dirección para su toma de decisiones.

Tabla 5 - Segunda línea de defensa: responsables y responsabilidades aplicables a la UNAL[18]

Tipología riesgo	Responsables	Responsabilidades
Institucional - transversal	Equipo Técnico Integral de Riesgos -	**Servir de ente asesor especializado en gestión integral del riesgo a la Alta Dirección y los actores principales de la 2LD.** - Definir, realizar seguimiento, control e implementación de las políticas y los lineamientos de la administración integral de los riesgos, entre ellos la Política integral de Gestión del Riesgo. - Asesorar al Comité SIGA, la Coordinación SIGA y los principales responsables (segunda línea de defensa) de las tipologías de riesgos contenidas en el MIGR como equipo técnico especializado en gestión integral del riesgo. - Analizar, tomar acciones y establecer el curso a seguir frente a los riesgos residuales significativos —posibles o materializados— que puedan ser o suponer un peligro alto o extremo para la institución, que hayan sido escalados

[18] La tabla contiene los responsables de las tipologías de riesgos de procesos (operativos y de corrupción), proyectos, estratégicos y ambientales, que conforman la segunda línea de defensa. Se encuentran pendientes por definir los responsables y las funciones de los riesgos de seguridad en información, seguridad y salud en el trabajo, de fraude, lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

Tipología riesgo	Responsables	Responsabilidades
		desde la Coordinación SIGA Nivel Nacional o los principales responsables de cada tipología de riesgos[19].
Institucional – transversal	Coordinación SIGA Nivel Nacional	**Generar lineamientos, asesoría y seguimiento transversal a la gestión integral del riesgo realizada por los principales responsables de las tipologías del MIGR y la primera línea de defensa.** - Establecer lineamientos, capacitación, orientación y alertas para la gestión integral del riesgo. - Establecer mecanismos transversales para el seguimiento y/o la autoevaluación de los riesgos. - Brindar asesoría a los principales responsables de las tipologías de riesgos presentes en los procesos, las estrategias, los proyectos y los sistemas de gestión cuando estos lo requieran. - Realizar seguimiento a la Política Integral de Gestión del riesgo. - Monitorear la gestión de riesgos y los controles dirigidos por los principales responsables de las tipologías de riesgos y ejecutados por la primera línea de defensa. - Apoyar la gestión y mitigación de riesgos residuales significativos posibles o materializados, escalando aquellos eventos importantes al ETIR. - Consolidar los resultados de la gestión del riesgo de las diferentes tipologías de riesgos que conforma el MIGR presentes en los procesos, las estrategias, los proyectos y sistemas de gestión de la UNAL.
Riesgos de procesos (operativos, Corrupción, PAMEC)	Líder SIGA Nivel Nacional. Coordinadores del SGC en sede o QHSV[20]	**Acompañamiento, seguimiento y definición de lineamientos, herramientas y documentos particulares para la gestión de las tipologías de riesgos del MIGR ejecutadas por la primera línea de defensa[21]** - Dar lineamientos, herramientas, capacitación, orientación y alertas para la gestión particular de las tipologías de riesgos contenidas en el MIGR. - Establecer mecanismos particulares para el seguimiento y la autoevaluación de riesgos y controles. - Brindar asesoría y acompañamiento a los líderes y funcionarios de la primera línea de defensa encargados de
Riesgos estratégicos	Comité Nacional de Planeación Estratégica. DNPE. Oficinas de planeación y estadística en las sedes	
Riesgos de proyectos	DNPE. VRI. Supervisores e interventores de proyectos. Otros[22]	

[19] Para aquellos riesgos residuales significativos que el ETIR no pueda tomar ninguna acción, se deben escalar y comunicar al Comité SIGA para su análisis y tratamiento correspondiente.
[20] Abreviatura de "quien haga sus veces".
[21] El responsable de cada tipología de riesgos se encargará de ejecutar de manera particular las funciones de la segunda línea de defensa que le competan.
[22] La casilla de la tabla contiene un resumen de los actores de la segunda línea de defensa para la tipología de riesgos en proyectos. Para este tipo en concreto, existen actores puntuales para los diferentes proyectos gestionados en la institución:

Tipología riesgo	Responsables	Responsabilidades
Riesgos ambientales	Comité Técnico Nacional de Gestión Ambiental. Coordinación Nacional de Gestión Ambiental	los procesos, las estrategias, los proyectos y sistemas de gestión. - Coordinar y consolidar los resultados del monitoreo de la gestión de riesgos y los controles ejecutado por la primera línea de defensa, reportando los resultados a la Coordinación SIGA Nivel Nacional, según los lineamientos dispuestos para ello. - Apoyar la gestión y mitigación de riesgos residuales significativos —posibles o materializados— identificados por la pimera línea de defensa, escalando aquellos eventos importantes a la Coordinación SIGA Nivel Nacional o al ETIR.
Riesgos de seguridad en la información	***Por definir***	
Riesgos de Seguridad-Salud en el Trabajo	División Nacional de SST, DNPAA	
Riesgos de fraude, LA, FT y FPADM	***Por definir***	

2.3.4 Primera línea de defensa – Autocontrol y gestión de riesgos

Está conformada por los integrantes de los procesos, las estrategias, los proyectos y sistemas de gestión en los que se desarrollan e implementan los procesos de control y la gestión de riesgos de las tipologías contenidas en el MIGR a través de su identificación, análisis, valoración, tratamiento, comunicación y seguimiento.

Tabla 6 - Primera línea de defensa: responsables y responsabilidades aplicables a la UNAL[23]

Tipología riesgo	Responsables	Responsabilidades
Riesgos de procesos (Operativos, Corrupción, PAMEC)	Líderes e integrantes de los procesos en el nivel nacional, sedes, facultades, centros e institutos.	**Desarrollo e implementación de la gestión de riesgos y controles en los procesos, estrategias, proyectos o sistemas de gestión** - Establecer el contexto del proceso, la estrategia, el proyecto o sistema de gestión para la identificación de causas y riesgos.
Riesgos estratégicos	DNPE. VRG. VRA. VRI. Secretaría General. Rectoría. CSU. GNFA. Vicerrectorías de sede y direcciones de sedes de presencia	

- Inversión: DNPE, Oficinas de Planeación y Estadística o QHSV, supervisores e interventores, comités de contratación nivel nacional y sedes.
- Extensión: consejos de facultad, comité de investigación y extensión de facultad o QHSV, supervisores e interventores, direcciones de investigación y extensión en sede o QHSV. DNEIPi, Comité Nacional de Extensión.
- Investigación: Consejos de facultad, Comité de Investigación y Extensión de Facultad o QHSV, vicedecanaturas de Investigación y Extensión, Direcciones de Investigación y Extensión en sede o QHSV, Dirección Nacional de Investigación y Laboratorios, Comité Nacional de Investigación.
- Regalías: supervisores e interventores, delegados del seguimiento de un proyecto (cuerpos colegiados, académicos o administrativos), direcciones de sede, vicerrectorías de sede (líderes de sede donde recaen los proyectos del SGR).

[23] La tabla contiene los responsables de las tipologías de riesgos de procesos (operativos y de corrupción), proyectos, estratégicos y ambientales que conforman la segunda línea de defensa. Se encuentran pendientes por definir los responsables y las funciones de los riesgos de seguridad en la información, la seguridad y la salud en el trabajo, de fraude, lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

Tipología riesgo	Responsables	Responsabilidades
	nacional, líderes de procesos estratégicos.	- Identificar y analizar los riesgos. - Evaluación y tratamiento de los riesgos. - Diseño y ejecución de mecanismos de control. - Ejecución del seguimiento y revisión de riesgos. - Gestión de riesgos materializados y riesgos residuales significativos (acciones preventivas y correctivas). - Prevenir, detectar y mitigar la materialización de riesgos (acciones de mejora).
Riesgos de proyectos	Directores de proyectos y su equipo de trabajo. Coordinadores funcionales.	
Riesgos ambientales	Jefes de Oficina y Responsables de Gestión Ambiental en las sedes. Líderes de procesos	
Riesgos de seguridad en la información	***Por definir***	
Riesgos de Seguridad y Salud en el Trabajo	Responsables del SGSST Nivel Nacional y Sedes, Contratistas del SST de las SPN, Líderes de procesos Nivel Nacional y Sedes	
Riesgos de fraude, LA, FT y FPADM	***Por definir***	

2.4 METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS

En este apartado se definen las ***pautas metodológicas*** para la ***gestión integral del riesgo*** en la UNAL, tomando como referente y estructura las etapas del proceso de gestión de riesgos definidas en la Norma Técnica Colombiana ISO 31000:2018, junto con otros elementos de estándares de gestión de riesgos[24], alineadas con el Sistema de Control Interno de la UNAL a cargo de la CNCSSCI y el Sistema Integrado de Gestión Académica, Administrativa y Ambiental – SIGA.

[24] Algunos de los estándares en los que se adaptaron elementos son:
- Para riesgos de proyectos los lineamientos del Project Management Institute – PMI.
- Para riesgos de corrupción los elementos definidos en la guía para la administración de riesgos y el diseño de controles en entidades públicas V5 del DAFP.
- Para riesgos ambientales la NTC ISO 14001:2015 y la NTC ISO 14004:2016.

Ilustración 3 - Etapas del proceso de gestión del riesgo aplicable a la UNAL[25]

La aplicación de las pautas metodológicas contenidas en cada etapa de la gestión del riesgo conlleva al establecimiento y la implementación de acciones estructuradas e integradas, orientadas a ***definir el contexto, identificar, analizar, valorar, comunicar, tratar, monitorear, registrar e informar los riesgos*** de las tipologías contempladas en el MIGR que pueden presentarse en los procesos, las estrategias, los proyectos y sistemas de gestión, en la que participan activamente los responsables definidos en el modelo de las tres líneas de defensa del numeral 2.3.

Es importante mencionar que las etapas del proceso para la gestión del riesgo están sustentadas en el ciclo de mejora continua "PHVA" y, por ende, su aplicación en la institución no debe ser secuencial sino iterativa[1]. La recolección de información de las etapas para la gestión del riesgo estará a criterio de los responsables de cada tipología de riesgos, cumpliendo siempre con lo estipulado en los principios ***De documentación y uso de sistemas de información para la administración de riesgos*** *del numeral* ***2.1.4.5****.*

A continuación, se aprecian las pautas metodológicas y los criterios de cada una de las etapas para la gestión integral del riesgo en la UNAL.

2.4.1 Establecimiento del contexto

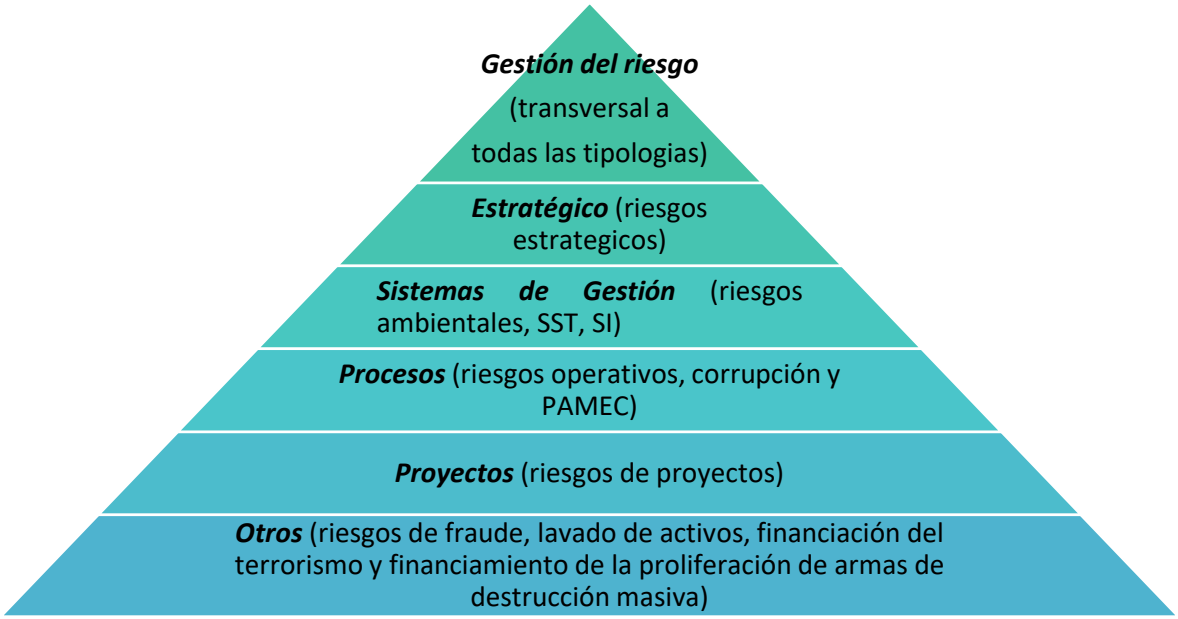
La implementación del MIGR implica un profundo conocimiento de la UNAL, en cuanto a su razón de ser, estructura, visión, valores, objetivos a corto medio y largo plazo, proyección a futuro, cultura organizacional, asignación presupuestal y estados financieros, activos y recursos tangibles e intangibles, procesos, estrategias, proyectos y sistemas de gestión, entre otros; también implica conocer el entorno en el que se desenvuelve desde lo social, político, cultural, tecnológico,

[25] Tomado de NTC ISO 31000:2018, página 10.

económico y ambiental, por mencionar algunos. Por ello, esta primera etapa es clave para el ***establecimiento del contexto*** de la gestión integral del riesgo, en la que se ***identifican los factores internos y externos*** que puedan desencadenar riesgos, afectando el cumplimiento de los objetivos, así como la creación y protección de valor en la institución; estos factores internos y externos se entienden como las causas, las amenazas, las debilidades o los agentes generadores que al presentarse generan riesgos.

El establecimiento del contexto en la Universidad Nacional de Colombia se realiza desde diferentes niveles, tal como se expone en la ilustración 4.

Ilustración 4 - Niveles de establecimiento de contexto aplicables a la UNAL



2.4.1.1 Contexto de la gestión integral del riesgo

Contexto bajo el cual opera la gestión integral del riesgo, en el que se definen las políticas, los roles, las responsabilidades, el alcance y otros elementos para el marco de operación integral que se van a considerar para su administración, así como los criterios y las pautas metodológicas que se deben tener en cuenta a lo largo de las etapas del proceso para la gestión del riesgo. Este contexto se expone en los numerales anteriores y a lo largo de las etapas del proceso para la gestión del riesgo contenidas en este apartado.

2.4.1.2 Contexto estratégico:

Es el contexto global en el que la Universidad se desenvuelve y dentro del cual busca cumplir sus objetivos misionales y sus estrategias. Está contenido en el Plan Global de Desarrollo formulado cada trienio, y al igual que el Plan Estratégico Institucional es el resultado de una serie de esfuerzos, recursos, de trabajo colaborativo y organizado en cada una de las dependencias y sedes de la institución. Este debe complementarse con un análisis de factores internos y externos de parte de la alta dirección de la Universidad y los procesos estratégicos entre los que se encuentran: DNPE

(con el proceso Direccionamiento Estratégico Institucional), VRG (con el proceso Mejoramiento de la Gestión), VRA, VRI, Secretaría General, Rectoría, CSU y GNFA, entre otros.

2.4.1.3 Contexto de los Sistemas de Gestión

Es el contexto en el que opera cada uno de los sistemas de gestión integrados en el modelo SIGA. Lo elaboran y actualizan periódicamente las coordinaciones de cada sistema, entre las que se encuentran el Sistema de Gestión de Calidad, el Sistema de Gestión Ambiental y el Sistema de Gestión y Seguridad y Salud en el Trabajo, entre otros. Se sugiere el uso de la Matriz DOFA, combinada con el análisis Pestal, para la identificación de los factores internos y externos.

2.4.1.4 Contexto de los procesos

Es el contexto en el que opera cada proceso. Su elaboración es liderada por el líder o coordinador del proceso y debe construirse de forma conjunta con las diferentes sedes y socializarse con sus integrantes. Debe de revisarse y actualizarse cada cierto periodo de tiempo, o en casos en los que pueda ser necesario incluir o excluir nuevas condiciones internas o externas. Se sugiere el uso de la matriz DOFA.

2.4.1.5 Contexto de los proyectos

Contexto en el que operan los proyectos de inversión, extensión, investigación y regalías. Lo elabora el director y coordinador funcional del proyecto desde la etapa de formulación, identificando las amenazas internas y externas que pueden presentarse durante el ciclo de vida del proyecto. Se sugiere el uso de los catálogos definidos para los tipos de proyectos, complementado con la identificación de factores internos y externos propios del objetivo del proyecto[26].

2.4.1.6 Otros contextos

Hace alusión a los contextos de otras tipologías de riesgos que no se encuentran inmersos en los niveles anteriores, de modo que es necesario identificar aquellos factores internos y externos que pueden desencadenar riesgos; queda a criterio del responsable de la tipología la selección de la herramienta y metodología más idónea para definirlo.

Para el desarrollo de esta etapa se pueden utilizar diferentes metodologías y herramientas, entre las que se encuentran el análisis DOFA, el análisis PESTAL (político, económico, sociocultural, tecnológico, ambiental y legal), entrevistas con expertos en el área, reuniones con directivos y con funcionarios de todos los niveles en la Universidad, sesiones de lluvias de ideas con los funcionarios de las áreas y los equipos de gestión, diagramas de flujo, herramientas de estudio “causa y efecto” y análisis por escenarios, entre otras.

[26] Los catálogos están en poder de los gestores de la segunda línea de defensa que conforman cada tipo de proyecto, siendo estos los encargados de su elaboración y puesta a disposición para los directores de proyectos.

Los responsables de la segunda línea de defensa de cada tipología deben facilitar e instruir en el uso de herramientas y métodos para el Establecimiento del Contexto, al brindar asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su levantamiento. Además, se debe llevar un registro y soporte de los factores internos y externos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios ***De documentación y uso de sistemas de información para la administración de riesgos*** *del numeral* ***2.1.4.5.***

2.4.2 Evaluación del riesgo - Identificación del riesgo

La identificación del riesgo implica conocer las fuentes de riesgos, las áreas de impacto, las causas y consecuencias potenciales; ***su fin es generar un listado de riesgos priorizados*** partiendo de aquellos que podrían en mayor medida perjudicar el cumplimiento de los procesos, las estrategias, los proyectos y sistemas de gestión de la UNAL; para ello, toma los factores internos y externos definidos en cada uno de los niveles del ***Establecimiento del Contexto.***

Para una adecuada identificación de riesgos se debe cumplir con lo siguiente.

2.4.2.1 Identificación y priorización de riesgos a partir del establecimiento del contexto

Es obligatorio para los responsables de la primera línea de defensa, en el momento de identificar sus riesgos, ***partir de los factores internos y externos*** —también conocidos como causas, amenazas, debilidades o agentes generadores— detectados en el establecimiento del contexto aplicable a la tipología de riesgos a la que se espera realizar la identificación. Es importante que los responsables de identificar los riesgos en cada tipología revisen vigencia tras vigencia estas causas, estableciendo aquellas que se han convertido en riesgos posibles o materializados, las que se han gestionado, aquellas que han pasado de ser debilidades o amenazas a fortalezas u oportunidades, las que han escalado y aumentado su criticidad, aquellas que se han unificado y las que se han excluido o perdido validez, de manera que se evidencie la articulación del establecimiento del contexto con la identificación de riesgos.

Considerando que el ***listado de riesgos identificados*** *a partir de las causas puede llegar a* ***ser muy extenso,*** *que* ***no todos los factores internos y externos tienen la misma importancia*** *o repercusión en los procesos, las estrategias, los proyectos y sistemas de gestión, y que los* ***recursos*** *humanos, tecnológicos, financieros y de otra índole con los que cuenta la UNAL son* ***limitados, se debe priorizar el listado de riesgos atendiendo los criterios que se exponen en la tabla 7.***

Tabla 7 - Criterios para la priorización de riesgos[27]

Criterio
Cuáles tienen mayor impacto y repercusión en el cumplimiento de los objetivos de los procesos, las estrategias, los proyectos y/o sistemas de gestión.
Cuáles tienen impacto en el cumplimiento de la misión y/o visión de la UNAL.

[27] Los responsables de la segunda línea de defensa de cada tipología pueden establecer otros criterios y definir herramientas para priorizar sus riesgos, siempre y cuando no entren en contravía con lo dispuesto en el presente MIGR.

Criterio
Cuáles ya se han materializado en los procesos, las estrategias, los proyectos y/o sistemas de gestión.
Cuáles tienen mayor afectación en la conformidad o prestación de los productos, servicios, entregables y otros que son parte del quehacer de los procesos, proyectos y sistemas de gestión.
Cuáles tienen mayor impacto en el cumplimiento de las metas y los indicadores establecidos (por ejemplo, indicadores de proceso, del Plan Global de Desarrollo y el Plan Estratégico Institucional, de planes de acción, entre otros).
Cuáles han desencadenado un hallazgo recurrente a partir de una evaluación interna o externa (incumplimiento de requisitos normativos, fallas, hallazgos de auditorías internas o externas críticos o recurrentes).
Cuáles son de gobierno del proceso, estrategia, proyecto o sistema de gestión, dónde recae la autoridad y responsabilidad para su gestión.
Cuáles tienen mayor complejidad según su alcance y naturaleza en relación con el éxito de la UNAL.
Cuáles tienen mayor rapidez de afectación y propagación en la UNAL.
Cuáles tienen mayor persistencia, es decir, el tiempo durante el que el riesgo impacta la UNAL.
Cuáles tienen mayor repercusión en la capacidad de recuperación de la UNAL para retornar a los niveles de tolerancia definidos o a la normalidad en la operación.

En el momento de **identificar y priorizar los riesgos a partir del contexto,** es importante hacer un análisis de los riesgos reportados en vigencias anteriores estableciendo si son pertinentes, si están incorporados en las amenazas y debilidades detectadas en el análisis de su contexto, si están bien definidos o son susceptibles de ser mejorados en su redacción. Como resultado de esta revisión se deben dejar soportes en los que se expliquen las modificaciones y eliminaciones que se generen, con su debida justificación.

2.4.2.2 Redacción de riesgos

Después de identificar y priorizar los riesgos, estos deben ser redactados de una forma que sea fácil de entender y en la que confluyan los diferentes elementos para su definición. Dadas las particularidades de las diferentes tipologías de riesgo, se cuenta con unos ***elementos obligatorios para definir un riesgo aplicable a cualquier tipología*** y ***una forma de redacción sugerida***; también se cuenta con ***elementos y formas de redacción complementarios de algunas tipologías*** de riesgos contenidas en el presente MIGR, los cuales se describen a continuación.

2.4.2.2.1 Elementos obligatorios para la definición de riesgos de cualquier tipología

En el momento de definir un riesgo de cualquier tipología, a fin de que este sea comprensible para los integrantes de los procesos, de las estrategias, los proyectos y sistemas de gestión, y para que sea entendible para actores ajenos a la UNAL, se debe incluir en su redacción o mencionar los siguientes elementos.

Ilustración 5 - Elementos obligatorios para la definición de un riesgo[28]

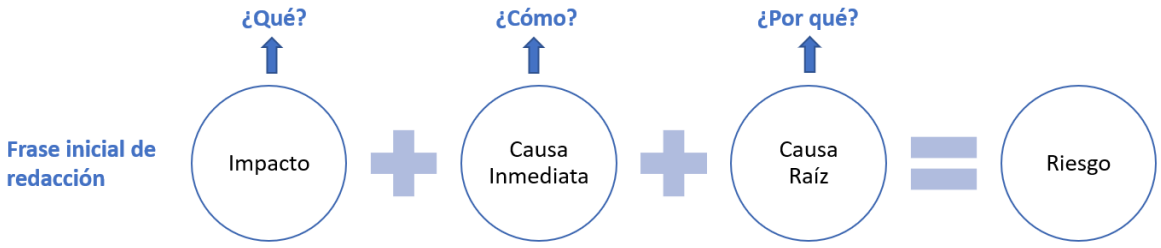
Impacto	Causa inmediata	Causa raiz
• Hace referencia a lo **que** podría pasar si se materializa el riesgo, es decir, a las consecuencias que puede ocasionar a la UNAL la materialización del riesgo.	• Hace alusión a **cómo** podría llegar a darse el riesgo por una causa inminente, es decir, a los factores, las circunstancias o las situaciones más inmediatas o evidentes sobre las cuales se presenta el riesgo, sin constituir la causa principal o la base para que se presente el riesgo.	• Conocida como causa principal o básica, hace mención del **por qué** más importante y no tan evidente o superficial por el cual podría llegar a presentarse el riesgo, es decir, corresponde a las razones, circunstancias o situaciones por las cuales se puede presentar el riesgo, siendo el punto de partida para la definición de controles.

*Es obligatorio definir para cada riesgo identificado y priorizado 1. El "**Impacto**" y 2. la "**Causa raíz**" y/o "**Inmediata**".*

2.4.2.2.2 Forma de redacción sugerida para un riesgo de cualquier tipología

Para que un riesgo sea redactado de una manera que sea fácil de entender por cualquier servidor público, se sugiere la siguiente forma de redacción, que inicia con frases como "posibilidad de" o "posible", y luego confluyen los tres elementos obligatorios para la definición de cualquier riesgo, tal como se aprecia en la ilustración 6.

Ilustración 6 - Estructura de redacción sugerida para cualquier riesgo



De los tres elementos requeridos para redactar un riesgo, se puede ver cómo el ***impacto*** hace referencia a la consecuencia o el efecto, en este caso negativo, que genera el riesgo sobre el objetivo, los productos, los servicios, los activos, los recursos, los usuarios, los procedimientos y las actividades del proceso, la estrategia, el proyecto o el sistema de gestión. Por otro lado, la ***causa inmediata*** y la ***causa raíz*** son aquellos factores internos o externos que pueden llegar a materializar el riesgo y originar su impacto.

[28] Las definiciones de impacto, causa inmediata y causa raíz fueron adaptas con base en lo dispuesto en la página 33 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5" del DAFP.

Es importante, en la medida que sea posible para cada tipología de riesgos, ***identificar y gestionar riesgos que garanticen de forma razonable el cumplimiento del objetivo*** de los procesos, las estrategias, los proyectos y sistemas de gestión donde tenga alcance, para lo cual se deben formular riesgos que abarquen los atributos definidos en su objetivo[29].

2.4.2.2.3 Redacción de riesgos operativos de procesos y riesgos estratégicos

Los riesgos operativos y estratégicos asociados a los procesos y las estrategias institucionales serán redactados con base en la forma de redacción sugerida del numeral anterior, en el que confluyen los tres elementos obligatorios para la definición de cualquier riesgo. Las tablas 8 y 9 contienen ejemplos de estos riesgos redactados a partir de la estructura sugerida y que pueden ser aplicables en algunos procesos de la Universidad.

Tabla 8 - Ejemplos de riesgos operativos de procesos redactados con base a la estructura sugerida

Proceso	**Frase inicial redacción**	**Impacto (¿Qué?)**	**Causa inmediata (¿Cómo?)**	**Causa raíz (¿Por qué?)**
Gestión administrativa de bienes y servicios	Posibilidad de	Afectación económica	Por multa y sanción del ente regulador	Debido a adquisición de bienes y servicios fuera de los requerimientos normativos
Mejoramiento de la gestión	Posible	Pérdida de la certificación institucional del Sistema de Gestión de Calidad.	Por retrasos o la inejecución de las actividades de los planes de acción derivados de la auditoría de certificación.	Provocados por limitaciones y alta rotación en el personal que apoya los procedimientos y actividades del SGC.
Gestión tecnológica	Posibilidad de	Afectación a la integridad y disponibilidad de la información académica y financiera.	Por ingreso a las aplicaciones y modificaciones de datos no autorizadas en los sistemas de información institucionales.	Generados por vulnerabilidades y debilidades en el control de acceso y gestión de permisos de los usuarios.
Servicios generales y de apoyo administrativo	Posibles	Pérdidas económicas.	Por daños o deterioro en los bienes (muebles) y otros equipos de oficina.	Debido a carencia de recursos monetarios, de personal y de tiempo para los mantenimientos preventivos, detectivos y correctivos requeridos.
Direccionamiento estratégico institucional	Posibles	Afectaciones a la imagen y a la gestión institucional.	Ocasionada por proyectos de inversión desarticulados de los objetivos, ejes estratégicos, misión y visión institucionales.	Debido a falta de capacitación, apropiación e interiorización de parte los directores de proyectos y sus equipos de trabajo.

[29] Lo anterior, teniendo en cuenta que pueden existir atributos del objetivo del proceso, de la estrategia, el proyecto o sistema de gestión que no tengan causas inmediatas, causas raíz o impactos, por lo cual no tendrían que identificarse riesgos para estos atributos.

Tabla 9 - Ejemplos de riesgos estratégicos redactados con base a la estructura sugerida

Frase inicial redacción	Impacto (¿Qué?)	Causa inmediata (¿Cómo?)	Causa raíz (¿Por qué?)
Posibilidad de	Desfinanciación debido a…	Recursos insuficientes por…	Cambios en la legislación
Posible	Incumplimiento de las metas y estrategias institucionales.	Ocasionado por ausencia de articulación entre el PLEI y el PGD.	Debido a cambios en el gobierno universitario de turno.
	Afectación de los procesos adaptativos de direccionamiento estratégico.	Debido a una tasa insuficiente de apropiación y maduración del modelo inter – sedes.	Por resiliencia de los funcionarios en los diferentes niveles de aplicación.

2.4.2.2.4 Elementos para la definición y redacción de riesgos de corrupción de procesos

A la hora de redactar o describir un riesgo de corrupción se deben incluir los elementos de su definición mencionados en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5" del DAFP, que se aprecian en la ilustración 7.

Ilustración 7 - Estructura de redacción para riesgos de corrupción del DAFP

La tabla 10 contiene ejemplos de riesgos de corrupción —redactados con base en la estructura sugerida en la guía del DAFP— que pueden ser aplicables en algunos procesos de la Universidad.

Tabla 10 - Ejemplos de riesgos de corrupción redactados con base a la estructura sugerida del DAFP

Proceso	Acción u omisión	Uso del poder	Desviación de la gestión de lo público	Beneficio privado
Gestión administrativa de bienes y servicios	Posibilidad de recibir o solicitar	Cualquier dádiva o beneficio	A nombre propio o de terceros	Con el fin de celebrar un contrato
Divulgación de la producción académica	Selección de evaluadores académicos	Que emitan concepto favorable a una obra	Sin el cumplimiento de los lineamientos establecidos por el proceso	En beneficio de un funcionario o tercero.
Servicios generales y de apoyo administrativo	Recibir	Dádiva	A nombre propio o de terceros	Para favorecer a un proveedor de servicios generales

Proceso	Acción u omisión	Uso del poder	Desviación de la gestión de lo público	Beneficio privado
Gestión de la investigación y creación artística	Apropiación y/o utilización	De los recursos financieros asignados	Para los proyectos de investigación de forma indebida o intencional	En pro de un beneficio particular.
Mejoramiento de la gestión	Manipulación	De la información del sistema de gestión	Para presentar resultados que favorezcan o desfavorezcan	La gestión de un sistema o de un proceso particular
Divulgación de la información Oficial	Aceptar	Algún tipo de regalo o dádiva para	Permitir el uso inadecuado de información institucional, ocultando, modificando o extraviando documentos generados o archivados por la institución, en favor o en contra	de un funcionario o proceso en particular.

*Adicional a los cuatro elementos para la correcta redacción de un riesgo de corrupción, con el fin de **facilitar** la identificación de la causa generadora del riesgo, se debe definir en algún campo, con claridad y sin ambigüedades, al igual que en cualquier otra tipología, el **impacto**, la **causa raíz** y/o la **causa inmediata**, las cuales serán clave para la definición de los controles del riesgo de corrupción asociado.*

2.4.2.2.5 Elementos para la definición y redacción de riesgos en proyectos.

Para definir un riesgo de proyecto en forma clara y comprensible, es necesario identificar y redactar correctamente los siguientes dos elementos:

- **Amenaza:** es cualquier unidad o conjunto de circunstancias o eventos adversos que pueden ocurrir en cualquier etapa del proyecto, de manera que acarreen consecuencias para este. En el momento de determinar la amenaza tenga en cuenta las siguientes recomendaciones:
  - Las amenazas se originan de circunstancias o eventos adversos.
  - Comprenda cuál es la variable más afectada en el proyecto por la amenaza (costo, tiempo, alcance, calidad).
  - No se deben confundir las amenazas (causas) y consecuencias (las consecuencias son lo que puede pasar en el proyecto si la amenaza se presenta).
  - En lo posible, redáctelas de una forma simple y concisa, evitando entrar en un alto nivel de detalle.
  - No importa si la amenaza es controlable o no por el proyecto, por las dependencias o la institución.
- **Componente amenazado:** hace referencia a el(los) componente(s) del proyecto que más se vería(n) afectado(s) en caso de ocurrir la amenaza; los componentes del proyecto se dividen en objetivos, metas, entregables (productos), actividades, recursos y activos.

Ilustración 8 - Estructura de redacción para riesgos de proyectos

Otros elementos para la correcta definición de riesgos que facilitan su comprensión e interpretación en el interior de los proyectos son:

- **Variable amenazada según metodología PMBOK[30]:** hace referencia a la variable o par de variables contenidas en el estándar de gestión de proyectos PMBOK que más se pueden ver afectadas por la amenaza. Estas variables son: costo, tiempo, alcance, calidad y cualquiera de sus combinaciones (costo-calidad, costo-tiempo, entre otras).
    - **Costo:** conocido como presupuesto del proyecto. Representa la cantidad de dinero que va a ser requerida para ejecutar las actividades del proyecto.
    - **Tiempo:** conocido como cronograma. Representa el plazo en el que está previsto llevar a cabo las actividades del proyecto.
    - **Alcance:** representa lo que está previsto que se entrega al final del proyecto, por ejemplo, la suma de productos, servicios y resultados. También puede entenderse como las tareas/actividades requeridas para cumplir los objetivos del proyecto.
    - **Calidad:** comprende la calidad tanto de la gestión del proyecto como la de sus entregables. Se aplica a todos los proyectos, independientemente de la naturaleza de sus entregables. Sobre los entregables, su calidad está dada por dos factores:
        - La conformidad con lo requerido: se refiere al conjunto de características medibles establecidas para satisfacer al cliente, lo que implica un concepto técnico de calidad. Significa preguntarnos si estamos generando lo que nos solicitaron.
        - Lo adecuado para el uso: podemos haber construido los entregables de acuerdo con lo requerido, pero quizá no sean adecuados para el uso. Implica aspectos de comodidad y facilidad de uso.
- **Subtipologías de riesgos aplicables a proyectos:** subclasificación particular de riesgos aplicable a los proyectos, que pueden ser los que se exponen en la tabla 11.

Tabla 11 - Subtipos de riesgos aplicables a los proyectos de inversión, extensión, investigación y regalías

Subtipologías de riesgos	Descripción
Administrativos o de gestión	Surgen del proceso administrativo que se debe llevar a cabo para formular, revisar, aprobar y ejecutar el proyecto. Están asociados a aquellas actividades de tipo administrativo que están establecidas en procesos,

[30] Abreviatura de Project Management Body of Knowledge (“fundamentos para la dirección de proyectos”).

Subtipologías de riesgos	Descripción
	procedimientos y en la normatividad institucional. Algunos riesgos administrativos pueden encontrarse en la: - dirección de proyectos - gestión de las operaciones - estructura organizacional - comunicación - normatividad interna - gestión contractual y financiera
Técnicos o de operaciones	Son aquellos que afectan el costo, el tiempo, el alcance o la calidad de un entregable, una actividad, una meta, un objetivo o al proyecto en general. Están asociadas a aspectos técnicos del proyecto y se basan en sus objetivos, metas, entregables y la naturaleza propia del proyecto. Algunos riesgos técnicos u operacionales pueden encontrarse en: - la definición del alcance - la definición de los requisitos y condiciones del proyecto - las estimaciones, supuestos y restricciones del proyecto - los procesos y recursos técnicos - la tecnología
Externos (naturales, socioculturales)	Son los riesgos que provienen de una fuente (amenaza) externa al proyecto y a la institución, pero que en caso de presentarse pueden afectar el correcto desarrollo del proyecto. Se incluyen fuentes externas de tipo ambiental, social, cultural y económico, entre otros. Algunos riesgos de tipo externo pueden encontrase en la: - legislación y política externa - sitios/instalaciones - desastre natural/ambiental/climático/biológico - competencia - sociedad

La tabla 12 contiene ejemplos de riesgos de proyectos redactados con base en la estructura sugerida en la ilustración 8 y que pueden ser aplicables en todos los tipos de proyectos de la UNAL (inversión, extensión, investigación y regalías).

Tabla 12 - Ejemplos de riesgos de proyectos redactados con base a la estructura sugerida

Subtipologías de riesgos	Componente amenazado	Amenaza
Administrativo o de gestión	Entregables y/o actividades	afectados por retrasos en la transferencia de recursos financieros.
Administrativo o de gestión	Metas y actividades	atrasadas o incumplidas por insuficiencia y/o rotación en el personal para la ejecución de los proyectos.
Administrativo o de gestión	Actividades y productos	afectados por el escaso uso y apropiación de las herramientas tecnológicas para la gestión del proyecto.
Técnico u operacional	Metas y productos	afectados por debilidades en el uso de las herramientas tecnológicas requeridas para el desarrollo del proyecto.

Subtipologías de riesgos	Componente amenazado	Amenaza
Técnico u operacional	Entregables (productos) y activos	incumplidos por retrasos o deficiencias de calidad por parte del contratista o proveedor.
Externo	Activos y recursos	afectados por hurto de equipos, herramientas, materiales y demás bienes necesarios para la ejecución del proyecto, por parte de terceros.
Externo	Metas y entregables	afectados o incumplidos por fenómenos de origen natural de tipo atmosféricos, hidrológicos y geológicos, entre otros.
Externo	Actividades y entregables	atrasados por fallas en el servicio de energía e internet de parte del proveedor.

*Adicional a los elementos "**Amenaza**" y "**Componente Amenazado**" requeridos para la correcta redacción de un riesgo de proyecto, se debe definir en algún campo con claridad y sin ambigüedades, al igual que en cualquier otra tipología, el **"impacto"**; si la **"amenaza"** se encuentra bien definida, esta puede entenderse como la **"causa raíz"** y/o la **"causa inmediata"**; estos elementos serán claves para el establecimiento de los controles asociados.*

*Existen **Catálogos** **de riesgos para proyectos** que están en poder de los gestores de la segunda línea de defensa que conforman cada tipo de proyecto, siendo estos los encargados de su elaboración, retroalimentación y puesta a disposición de los directores de proyectos, quienes podrán usarlos como guía para la identificación de los riesgos propios de su proyecto.*

2.4.2.2.6 TIPS para la correcta redacción de riesgos de cualquier tipología contenida en el MIGR

Para redactar adecuadamente los riesgos de cualquier tipología es importante tener en cuenta las siguientes premisas[31]:

I. No describir como riesgos omisiones, desviaciones o negaciones (ausencia) de controles. **Ejemplos**:
   - Errores en la liquidación de la nómina por fallas en los procedimientos existentes.
   - Retrasos en la prestación del servicio por no contar con digiturno para la atención.
   - Afectaciones a la movilidad entrante y saliente por debilidades en los procedimientos y actividades asociados.
   - Ausencia de controles de acceso y perfiles (permisos) de usuarios que garanticen la confidencialidad e integridad de la información que reposa en los SIA.

II. No describir causas como riesgos. **Ejemplos**:
   - Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

[31] Premisas adaptadas de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5" del DAFP, pagina 34.

- Debilidades en la integración y articulación de los procedimientos y dependencias académico - administrativos relacionadas con los trámites y servicios de formación brindados a los estudiantes.

III. No existen riesgos transversales, lo que puede existir son causas transversales. **Ejemplos**:
- Pérdida de expedientes, registros e información en general en medios físicos o digitales.
- Ausencia o limitaciones de personal de planta u contratista, alta rotación de personal contratista.
- Omisión, limitación o ausencia de normatividad y políticas (regulaciones) internas o externas para la gestión de los procedimientos y actividades de los procesos y proyectos.

IV. No confundir los riesgos con problemas y en lo posible no redactarlos como una no conformidad o incumplimiento.

2.4.2.3 Recomendaciones y ejemplos para la identificación de causas e impactos

Sin importar cual sea el tipo de riesgo, es ***clave en su redacción identificar el impacto, la causa inmediata y la causa raíz***. Es importante, en la medida que sea posible para cada tipología, ***identificar y gestionar riesgos que garanticen de forma razonable el cumplimiento del objetivo***, para lo cual se deben formular riesgos relacionados con los atributos del objetivo del proceso, la estrategia, el proyecto o sistema de gestión.

Para facilitar la identificación y redacción de riesgos de cualquier tipología se puede usar como referente los siguientes ejemplos de "causas" (conocidas como factores internos y externos, o debilidades y amenazas) e "impactos" (también llamados “efectos” o “consecuencias”), y así establecer aquellas que puedan afectar los objetivos, los productos, los servicios, los usuarios, los procedimientos, las actividades y otros que están inmersos en el quehacer de los procesos, las estrategias, proyectos y sistemas de gestión (véase la tabla 13).

Tabla 13 - Ejemplos de causas que pueden generar riesgos en los procesos, las estrategias, proyectos y sistemas de gestión.

Interna/ externa	Tipo de causa	Definición	Ejemplos
Interna	Personal	Eventos relacionados con las condiciones, acciones y resultados de los funcionarios de la institución.	Capacidad y cantidad de personal, salud, seguridad, baja productividad, hurto/pérdida de activos o recursos, posibles comportamientos no éticos, fraude interno (corrupción, soborno).
	Infraestructura y activos	Eventos relacionados con la infraestructura física de la institución.	Disponibilidad o estado/daño de los activos y la infraestructura, capacidad de los activos, acceso a nueva infraestructura o activos, incendios, inundaciones.
	Procesos	Eventos relacionados con los procedimientos y actividades que deben realizar los funcionarios de la institución	Capacidad, debilidades en el diseño y ejecución de las actividades y procedimientos, relaciones con proveedores y *stakeholders*, entradas y salidas del proceso, interacciones con otros procesos, estrategias, proyectos y/o sistemas de gestión, falta de procedimientos, errores de grabación o autorización, errores en cálculos para pagos

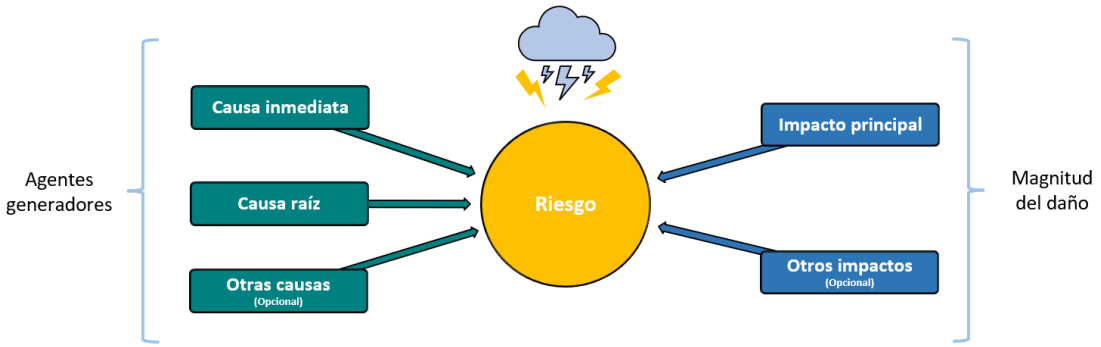
Interna/ externa	Tipo de causa	Definición	Ejemplos
			internos y externos, falta de capacitación a los funcionarios.
	Tecnología	Eventos relacionados con la infraestructura tecnológica, de red y de comunicaciones de la institución.	Daño de equipos, caída o indisponibilidad de aplicaciones y servicios, caída o deterioro de las redes y cableado, errores en programas/servidores/aplicaciones, integridad y disponibilidad de la información, mantenimiento de la infraestructura tecnológica y redes, niveles de automatización de los trámites y servicios.
	Estructura organizacional	Eventos relacionados con el organigrama y estructura de la institución.	Ausencia o limitaciones para el trabajo interdependencias, tamaño y complejidad de la institución.
	Cultura organizacional	Eventos relacionados con la manera propia de ser y hacer las cosas en la institución, sus sedes y funcionarios.	Débil estabilidad laboral, altos niveles de estrés laboral, deficientes estilos de liderazgo, debilidades en la apropiación de valores éticos y principios institucionales, fallas en la comunicación formal e informal.
	Económicos	Eventos asociados con la disponibilidad y el uso de los recursos monetarios	Poca disponibilidad de recursos, bajo o escaso flujo de caja, mal uso de los recursos económicos.
	Normas y directrices	Eventos relacionados con las normas y directrices propias de la institución.	Fallas en la emisión, formalización y difusión de las normas y directrices, baja interiorización o aplicación de los lineamientos y políticas internas.
Externa	Políticas y legales	Eventos relacionados con las políticas y regulaciones de entes gubernamentales y otros con influencia sobre la institución.	Cambios recurrentes o significativos en las legislaciones, regulaciones y políticas de entes gubernamentales de obligatorio cumplimiento para la institución, cambios de gobierno, limitada o nula voluntad política para el fortalecimiento de la educación superior.
	Económicas	Eventos relacionados con aspectos macroeconómicos en los niveles regional, país o internacional.	Fluctuaciones importantes negativas para la institución en los mercados financieros, altos niveles de desempleo, fuerte competencia en servicios de educación superior, limitaciones en la oferta y demanda de servicios y bienes para el correcto desempeño del proceso, altos niveles de inflación o niveles de deuda pública.
	Medio ambientales	Eventos relacionados con los ecosistemas, fenómenos naturales y las comunidades	Catástrofes naturales, niveles de emisiones y residuos por fuera de los valores establecidos, afectaciones a los ecosistemas o comunidades que los habitan.
	Sociales, culturales y de orden público	Eventos relacionados con la calidad de vida, cultura y condiciones sociales de los territorios donde se extienden las actividades de la institución	Demografía, condiciones sociales, débil compromiso con la responsabilidad social, nivel de calidad de vida, actitud de los ciudadanos.
	Tecnológicas	Eventos relacionados con la infraestructura tecnológica externa a la institución y las tecnologías emergentes	Interrupciones en los servicios de energía e internet, requerimientos de datos externos, nuevas tecnologías emergentes, mantenimientos de infraestructura y servicios tecnológicos externos.

Tabla 14 - Ejemplos de consecuencias asociadas a los riesgos que pueden afectar los procesos, las estrategias, proyectos y sistemas de gestión

Ejemplos de consecuencia
Pérdidas económicas
Afectaciones a la reputación y/o imagen institucional a nivel interno o externo
Insostenibilidad financiera, sobrecostos
Sanciones, llamados de atención, procesos judiciales
Incumplimientos normativos (internos) y legales (externos)
Reprocesos
Insatisfacción de los ***stakeholders***
Incremento de quejas y reclamos
Daños a la integridad física de las personas, infraestructura, tecnología y/o otros activos
Afectaciones o pérdidas de confidencialidad, integridad y disponibilidad de la información
Repercusiones al liderazgo organizacional
Impacto académico, científico, social y/o territorial
Afectaciones operacionales
Disminución de la competitividad
Impactos sobre la gobernabilidad y/o gobernanza
Incumplimientos en el cronograma o ajustes al alcance de los proyectos
Bienestar general
Pérdida de información
Insatisfacción de los grupos de interés

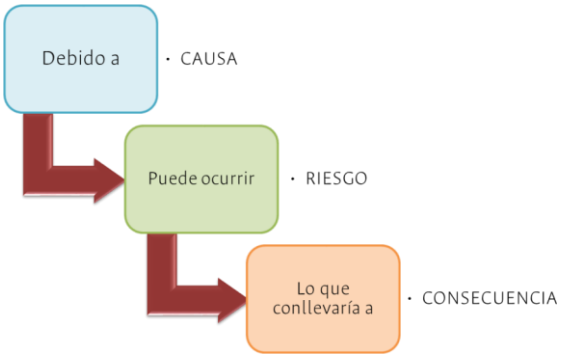
Un método usado para la correcta identificación de causas y consecuencias (impactos) es el ***análisis en esquema de corbatín*****,** en el que, de manera sencilla, se puede analizar la trayectoria del riesgo desde las causas a las consecuencias, donde el riesgo se representa en el centro, en la izquierda los agentes generadores(causas) y en la derecha los impactos.

Ilustración 9 - Esquema de corbatín para la Identificación de causas e impacto de los riesgos



Para subsanar cualquier duda en la asociación de causas e impacto a los riesgos de cualquier tipología, se puede utilizar la frase que se muestra en la ilustración 10.

Ilustración 10 - Frase de referencia para asociar causas e impactos a los riesgos de cualquier tipología



Los responsables de la segunda línea de defensa de cada tipología deben facilitar e instruir en el uso de herramientas y métodos para la identificación y priorización de riesgos, redacción de riesgos y definición correcta de causas e impactos, al brindar asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su gestión. Además, se debe llevar un registro y soporte de estos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios ***De documentación y uso de sistemas de información para la administración de riesgos*** *del numeral* ***2.1.4.5*** *del presente documento.*

2.4.3 Evaluación del riesgo – análisis del riesgo

En esta etapa se obtienen para el listado de riesgos priorizados y redactados, con sus respectivos impactos y causas, los ***parámetros de probabilidad e impacto*** para obtener el ***nivel de riesgo y el perfil de riesgo inherente***, así como su ubicación respectiva en el ***mapa de calor*** y el ***nivel de aceptabilidad***, con el ***análisis*** (sin el uso de controles) de su magnitud según el ***apetito***, la ***tolerancia*** y la ***capacidad de riesgo*** definidos por la UNAL. El ***análisis*** dependerá de la información obtenida en la etapa anterior de ***identificación de riesgos*** y los aportes de las diferentes partes involucradas.

Los criterios para la calificación del riesgo pueden ser subjetivos y dependen de su particularidad, así como de los antecedentes del proceso, la estrategia, proyecto y/o sistema de gestión, al igual que del conocimiento y la experiencia de los servidores públicos que participan en su análisis. Para fines prácticos, la UNAL calificará sus diferentes tipologías de riesgo utilizando los siguientes parámetros.

2.4.3.1 Parámetros de probabilidad

La ***probabilidad*** puede ser medida con ***criterios de frecuencia*** si se ha ***materializado el riesgo en el pasado,*** al contar el número de veces que se ha presentado la situación adversa en un espacio de tiempo determinado, en caso de contar con información documentada del evento. También se puede obtener con el ***número de veces que se ejecuta la actividad que conlleva al riesgo,*** si se tiene conocimiento de esta información. De lo contrario, este parámetro podrá medirse en términos de ***factibilidad,*** teniendo en cuenta la presencia de la causa que pueden propiciar el riesgo, aunque este no se haya materializado, lo cual implica un grado de creencia en la ocurrencia del hecho y puede variar dependiendo del conocimiento y la percepción que tenga el evaluador.

Sin importar cuál sea la tipología de riesgos, a fin de ***determinar la probabilidad*** se debe tener una tabla con los siguientes ***cinco niveles: 1- raro, 2 - improbable, 3 - posible, 4 – probable y 5 - casi seguro;*** por otro lado, los criterios para obtener la probabilidad pueden cambiar de una tipología a otra. Considerando las particularidades de las tipologías de riesgos contenidas en el MIGR, se cuenta con diferentes tablas para obtener el nivel de probabilidad (véanse las tablas 15-18)[32].

2.4.3.1.1 Parámetros de probabilidad para riesgos de procesos (operativos, corrupción y PAMEC)

En estos riesgos, la probabilidad deberá estimarse: 1. Por la **Frecuencia de Materialización** del riesgo; 2. Si no se cuenta con esta información deberá obtenerse por medio de la **Frecuencia de ejecución de la actividad,** que conlleva al riesgo; 3. En caso de no ser posible por las dos opciones anteriores, por **Factibilidad**.

Tabla 15 - Parámetros de probabilidad para riesgos de procesos

Valor	Nivel	Frecuencia de materialización	Frecuencia de actividad[33]	Factibilidad
1	Raro	No se ha presentado en los últimos cinco años.	La actividad que conlleva al riesgo se ejecuta como máximo dos veces por año.	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja.
2	Improbable	Al menos una vez en los últimos cinco años.	La actividad que conlleva al riesgo se ejecuta de tres a veinticuatro veces por año.	El evento puede ocurrir en algún momento. Probabilidad baja.
3	Posible	Al menos una vez en los últimos dos años.	La actividad que conlleva al riesgo se ejecuta de veinticinco a 499 veces por año.	El evento podría ocurrir en algún momento. Probabilidad media.
4	Probable	Al menos una vez en el último año.	La actividad que conlleva al riesgo se ejecuta de quinientas a 5000 veces por año.	El evento probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.
5	Casi seguro	Más de una vez al año.	La actividad que conlleva al riesgo se ejecuta más de 5000 veces por año.	Se espera que el evento ocurra en la mayoría de las circunstancias. Probabilidad muy alta.

[32] A la fecha de la elaboración del presente MIGR, se cuenta con las tablas de probabilidad para las tipologías de riesgos de procesos y proyectos (estratégicos y ambientales). Se encuentra pendiente por definir las tablas de probabilidad de los riesgos de seguridad en la información, la seguridad y la salud en el trabajo, de fraude, lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva; este ejercicio deberá llevarse a cabo con los responsables que conforman la segunda línea de defensa de estas tipologías. La tabla de probabilidad de riesgos de procesos puede ser usada y adaptada para determinar la probabilidad de cualquier otra tipología de riesgos que no cuente con parámetros propios de probabilidad.

[33] Criterios de frecuencia de actividad adaptados de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5", página 39.

2.4.3.1.2 Parámetros de probabilidad para riesgos estratégicos

El plazo establecido para el análisis de la probabilidad de los riesgos estratégicos será de seis años, teniendo en cuenta que el periodo rectoral es de tres años y que el cargo no puede ser ocupado por más de dos periodos consecutivos.

Tabla 16 - Parámetros de probabilidad para riesgos estratégicos

Valor	Nivel	Factibilidad	Frecuencia materialización[34]
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja.	No se ha presentado en los últimos seis años.
2	Improbable	El evento puede ocurrir en algún momento. Probabilidad baja.	Al menos una vez en los últimos seis años.
3	Posible	El evento podría ocurrir en algún momento. Probabilidad media.	Al menos una vez en los últimos tres años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.	Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. Probabilidad muy alta.	Más de una vez al año.

2.4.3.1.3 Parámetros de probabilidad para riesgos de proyectos

El periodo de tiempo establecido para estimar el nivel de probabilidad de los riesgos de proyectos estará limitado a un Intervalo no mayor a la duración de su ciclo de vida, considerando el ***número de veces que este pueda ocurrir*** durante el proyecto o el ***porcentaje de posibilidad que este ocurra***, en su defecto se estimará por ***factibilidad***.

Tabla 17 - Parámetros de probabilidad para riesgos de proyectos

Valor	Nivel	Factibilidad	Frecuencia[35]
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja. Ocurre en proyectos puntuales, excepcionales o algunos de un tipo específico.	Es raro que ocurra durante el proyecto. Existe una posibilidad inferior o igual al 5 % de que ocurra durante el proyecto.
2	Improbable	El evento puede ocurrir en algún momento. Probabilidad baja.	Puede ocurrir máximo una vez durante el proyecto.

[34] En caso de que se haya materializado el riesgo en los últimos seis años, la medición se obtiene por frecuencia al contar el número de veces que se ha presentado en este periodo de tiempo; se debe documentar la situación, de lo contrario se obtiene por factibilidad.
[35] Hace referencia al uso de información de acontecimientos asociados que indiquen la presencia de amenazas o la materialización del riesgo, que permita estimarla en un intervalo de tiempo no mayor a la duración del proyecto.

Valor	Nivel	Factibilidad	Frecuencia[35]
		Ocurre en pocos proyectos.	Existe una posibilidad entre el 6 % y 20 % de que ocurra durante el proyecto.
3	Posible	El evento podría ocurrir en algún momento. Probabilidad media. Ocurre en algunos proyectos.	Puede ocurrir máximo dos veces durante el proyecto. Existe una posibilidad entre el 21 % y el 50 % de que ocurra durante el proyecto.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta. Ocurre en alta proporción de los proyectos.	Puede ocurrir máximo tres veces durante el proyecto. Existe una posibilidad entre el 51 % y 80 % de que ocurra durante el proyecto.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. Probabilidad muy alta. Ocurre en casi todos los proyectos.	Puede ocurrir cuatro o más veces durante el proyecto. Existe una posibilidad mayor o igual al 81 % de que ocurra durante el proyecto.

2.4.3.1.4 Parámetros de probabilidad para riesgos ambientales:

Tabla 18 - Parámetros de probabilidad para riesgos ambientales

Valor	Nivel	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales o Probabilidad de ocurrencia muy baja o No se ha presentado en los últimos cinco años.
2	Improbable	El evento puede ocurrir en algún momento o Probabilidad de ocurrencia baja o Al menos una vez en los últimos cinco años.
3	Posible	El evento podría ocurrir en algún momento o Probabilidad de ocurrencia media o Al menos una vez en los últimos dos años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias o Probabilidad de ocurrencia alta o Al menos una vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias o Probabilidad de ocurrencia muy alta o Más de una vez al año.

*El **nivel de probabilidad** se puede obtener por frecuencia de ejecución de la actividad que conlleva al riesgo, frecuencia de materialización de las causas o del riesgo, y por factibilidad (subjetividad del evaluador). Las **descripciones de los niveles pueden cambiar según las particularidades de la tipología a la que pertenezca el riesgo.***

2.4.3.2 Parámetros de impacto

El ***Impacto*** se mide según el ***grado en que las consecuencias o los efectos pueden perjudicar*** a los procesos, las estrategias, los proyectos, los sistemas de gestión y, en general, a la institución, si se materializa el riesgo, teniendo en cuenta unas variables definidas que permiten determinar el grado de afectación, variables que son diferentes para cada tipología de riesgos.

Sin importar cuál sea la tipología de riesgos, a fin de determinar el impacto se debe tener una tabla con los siguientes ***cinco niveles: 1 - insignificante, 2 - menor, 5 - moderado, 10 - mayor y 20 – catastrófico***, excepto para los riesgos de corrupción en los que solo se usan los tres niveles superiores. Considerando las particularidades de las tipologías de riesgos contenidas en el MIGR, se cuenta con diferentes tablas para obtener el nivel de impacto que se aprecian a continuación[36].

2.4.3.2.1 Parámetros de impacto para riesgos de procesos – operativos y PAMEC

Para determinar el nivel de impacto en los riesgos de procesos operativos y PAMEC, se utilizarán las ***variables usuario, operación, imagen, sanciones y pérdidas económicas***, siendo el nivel de impacto para un riesgo el nivel de la variable que más se ve afectada por la causa.

Tabla 19 - Parámetros de impacto para riesgos de procesos - Operativos y PAMEC

Valor	Nivel	Variables				
		Usuario	**Operación**	**Imagen**	**Sanciones**	**Pérdidas económicas**
1	Insignificante	No se ven afectados los usuarios	No hay interrupción de las operaciones de la Universidad	No se ve afectada la imagen o credibilidad de la Universidad	No hay intervenciones de entes de control. No se generan sanciones económicas o administrativas	Pérdidas económicas mínimas
2	Menor	Baja afectación a los usuarios	Interrupción de las operaciones de la Universidad por algunas horas, menor a (1) un 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
5	Moderado	Afectación a un grupo reducidos de usuarios	Interrupción de las operaciones de la Universidad 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 ante los entes reguladores o una demanda de largo alcance para la entidad.	Pérdidas económicas moderadas
10	Mayor	Afectación en la ejecución del proceso	Interrupción de las operaciones de la Universidad	Imagen o credibilidad de la Universidad	Acciones por parte de los entes de control internos o	Pérdidas económicas mayores

[36] A la fecha de la elaboración del presente MIGR, se cuenta con las tablas de impacto para las tipologías de riesgos de procesos (operativos, corrupción y PAMEC), proyectos, estratégicos y ambientales. Se encuentra pendiente por definir las tablas de impacto de los riesgos de seguridad en la información, la seguridad y la salud en el trabajo, de fraude, lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva; este ejercicio deberá llevarse a cabo con los responsables que conforman la segunda línea de defensa de estas tipologías. La tabla de impacto de riesgos de procesos puede ser usada y adaptada para determinar la probabilidad de cualquier otra tipología de riesgos que no cuente con parámetros propios de impacto.

Valor	Nivel	Variables				
		Usuario	**Operación**	**Imagen**	**Sanciones**	**Pérdidas económicas**
		que repercute en una parte considerable de los usuarios	por más de (2) dos días	afectada en la región	externos que incluyen sanciones medianas.	
20	Catastrófico	Afectación en la ejecución del proceso que repercute en la mayoría de los usuarios	Interrupción de las operaciones de la Universidad por más de cinco (5) días	Imagen o credibilidad de la Universidad 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

2.4.3.2.2 Parámetros de impacto para riesgos de procesos de corrupción

El nivel de impacto en los riesgos de corrupción (limitado a los niveles 5 – moderado, 10-mayor, 20-catastrófico) será obtenido con base en los interrogantes de la tabla dispuesta por el DAFP en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas V5" que se muestra a continuación.

Tabla 20 - Parámetros (interrogantes) de impacto para riesgos de procesos – Corrupción

N.°	PREGUNTA:	RESPUESTA	
	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	**SÍ**	**NO**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
	TOTAL RESPUESTAS AFIRMATIVAS(SÍ)		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto ***moderado***.			
Responder afirmativamente de SEIS a ONCE preguntas genera un impacto ***mayor***.			
Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto ***catastrófico***.			
Si la respuesta a la pregunta 16 es afirmativa, el impacto es ***catastrófico***.			

2.4.3.2.3 Parámetros de impacto para riesgos estratégicos

Valor	Nivel	Variables	
		Pérdida económica	**Reputacional o imagen**
1	Insignificante	Afectación menor al 0,002 % del presupuesto (funcionamiento + inversión). Afectación menor a cuarenta SMMLV.	El riesgo afecta la imagen de algún área de la organización.
2	Menor	Afectación entre el 0,002 % y 0,01 % del presupuesto (funcionamiento + inversión) Afectación entre 40 y 200 SMMLV.	El riesgo afecta la imagen de la entidad internamente o con los grupos de interés.
5	Moderado	Afectación entre el 0,01 % y 0,05 % del presupuesto (funcionamiento + inversión). Afectación entre 200 y 1000 SMMLV.	El riesgo perjudica la imagen de la entidad con algunos grupos de interés que afectan el logro de los objetivos estratégicos, la misión o la visión.
10	Mayor	Afectación entre el 0,05 % y 0,1 % del presupuesto (Funcionamiento + inversión). Afectación entre 1000 y 2000 SMMLV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido en el nivel regional.
20	Catastrófico	Afectación mayor al 0,1 % del presupuesto (Funcionamiento + inversión). Afectación mayo a 2000 SMMLV.	El riesgo afecta la imagen de la entidad a nivel nacional o internacional, con efecto sostenido a nivel publicitario.

2.4.3.2.4 Parámetros de impacto para riesgos de proyectos

Para determinar el nivel de impacto en los riesgos de proyectos se utilizarán las variables contenidas en el PMBOK ***costo, tiempo, alcance y calidad***, siendo el nivel de impacto para un riesgo el nivel de la variable que más se ve afectada.

Tabla 21 - Parámetros de impacto para riesgos de proyectos

Valor	Nivel	Variable			
		Costo	**Tiempo**	**Alcance**	**Calidad**
1	Insignificante	Incremento insignificante en el costo, afectación menor al 1 %.	Retraso del cronograma menor o igual a un mes.	Afectación insignificante en el cumplimiento de las actividades, metas u objetivos que afecten el avance acumulado del proyecto en menos del 1 %.	Afectación a la calidad de una actividad, producto o entregable imperceptible.
2	Menor	Afectación entre el 1 % y menor al 5 % del costo total del proyecto.	Retraso del cronograma entre uno dos 2 meses.	Afectación menor en el cumplimiento de las actividades, metas u objetivos que afecten el avance acumulado del proyecto entre el 1 % y 5 %.	Afectación a la calidad de una actividad, producto o entregable que requiere ajustes menores.
5	Moderado	Afectación entre el 5 % y menor al 10 % del costo total del proyecto.	Retraso del cronograma entre dos y cuatro meses.	Afectación media en el cumplimiento de las actividades, metas u objetivos que afecten el avance acumulado del proyecto entre el 5 % y 10 %.	Afectación a la calidad de una actividad, producto o entregable que requiere ajustes considerables.
10	Mayor	Afectación entre el 10 % y menor al 20 % del costo total del proyecto.	Retraso del cronograma entre cuatro y seis meses.	Afectación mayor en el cumplimiento de las actividades, metas u objetivos que afecten el avance acumulado del proyecto entre el 10 % y el 20 %.	Afectación a la calidad de una actividad, producto o entregable que lo hace inaceptable para el proyecto. Ajustes mayores.
20	Catastrófico	Afectación mayor o igual al 20 % del costo total del proyecto.	Retraso del cronograma mayor a seis meses.	Afectación severa en el cumplimiento de las actividades, metas u objetivos que afecten el avance acumulado del proyecto en más del 20 %.	Afectación a la calidad de una actividad, producto o entregable que no lo hace funcional. Ajustes severos o críticos.

2.4.3.2.5 Parámetros de impacto para riesgos ambientales

Para determinar el nivel de impacto en los riesgos ambientales, se utilizarán las ***variables imagen, legal, objetivos ambientales, ambiente y económico***, siendo el nivel de impacto para un riesgo el nivel de la variable que más se ve afectada.

Tabla 22 - Parámetros de impacto para riesgos ambientales

Valor	Nivel	Variables				
		Imagen	**Legal**	**Objetivos ambientales**	**Ambiente**	**Económico**
1	Insignificante	Afecta la imagen del Responsable del SGA.	Sin incumplimiento de la legislación/Procesos disciplinarios internos.	No afecta el logro de los objetivos del SGA.	En el interior de la Universidad.	Afectación en un valor menor o igual al 1 % del presupuesto del SGA.
2	Menor	Afecta la imagen del Equipo del SGA de la sede.	N/A	N/A	N/A	Afectación en un valor entre el 1 % y el 3 % del presupuesto del SGA.
5	Moderado	Afecta la imagen de la Alta dirección de la sede.	N/A	N/A	N/A	Afectación en un valor de 3 % al 5 % del presupuesto del SGA.
10	Mayor	Afecta la imagen de la sede.	Requerimiento o sanciones económicas por parte de la autoridad ambiental.	N/A	Comunidad vecina.	Afectación en un valor del 5 % al 10 % del presupuesto del SGA.
20	Catastrófico	Afecta la imagen de Todas las sedes de la Universidad.	Suspensión actividad por parte de la autoridad ambiental.	Afecta el logro de uno o más objetivos del SGA.	Afectación de los recursos naturales del municipio o la región.	Afectación en un valor igual o superior al 10 % del presupuesto del SGA.

*Las **variables** para obtener el nivel de impacto pueden cambiar según la tipología a la que pertenezca el riesgo. **En el momento de seleccionar el nivel de impacto, se debe usar el nivel de la variable más afectada.***

2.4.3.3 Nivel de riesgo inherente, nivel de aceptabilidad y Mapa de Calor

2.4.3.3.1 Nivel de riesgo inherente – método para su obtención

El ***nivel de riesgo inherente***[37]**,** conocido como ***nivel de riesgo puro***, en cualquier tipología se debe obtener para todos los riesgos identificados, priorizados y redactados, con base en los niveles de ***probabilidad*** e ***impacto***[38] establecidos para cada uno en esta etapa de ***"Análisis del riesgo"***. Este se puede calcular de dos formas:

I. **Multiplicando** los valores de los niveles de las variables probabilidad e impacto como se aprecia en la siguiente fórmula:

$$Nivel\ de\ riesgo\ inherente: valor\ del\ nivel\ de\ probabilidad\ x\ valor\ del\ nivel\ de\ impacto$$

[37] La definición de nivel de riesgo puede consultarse en el numeral "1.5 Definiciones" de este documento. El nivel de riesgo inherente constituye la primera parte del "Perfil de riesgo".
[38] La probabilidad e impacto determinados en esta etapa se conocen como "***probabilidad inherente***" y "***riesgo Inherente***", ya que son los establecidos sin considerar la presencia de mecanismos de control.

II. ***Ubicando y cruzando*** en el ***mapa de calor***[39] los valores de los niveles de las variables probabilidad e impacto.

Sin importar el método usado para obtener el ***nivel de riesgo inherente***, al final se deben ubicar todos los riesgos con su respectiva valoración inherente en el ***Mapa de Calor***.

2.4.3.3.2 Nivel de aceptabilidad

El ***Nivel de aceptabilidad*** que hace referencia al nivel de gravedad del riesgo tanto inherente como residual ***(perfil de riesgo)*** se obtiene según el cuadrante de color resultante al ubicar en el Mapa de Calor el cruce de las variables *probabilidad* e *impacto*, o al ubicar el resultado de su multiplicación en el rango correspondiente de la tabla inferior.

Para cada ***nivel de aceptabilidad*** existen unas ***acciones*** y ***opciones de tratamiento*** que se deben implementar para gestionar el riesgo y el grado de exposición que este acarrea en los procesos, las estrategias, los proyectos, sistemas de gestión y, en general, a la institución; las opciones de tratamiento se deciden para cada riesgo con base en el ***nivel de riesgo residual*** obtenido en la siguiente etapa de ***"Valoración del riesgo"*** *(Ver numeral 2.2.4 Evaluación del riesgo – valoración del riesgo).*

Tabla 23 - Niveles de aceptabilidad del riesgo aplicables a cualquier tipología de riesgos contenida en el MGG[40]

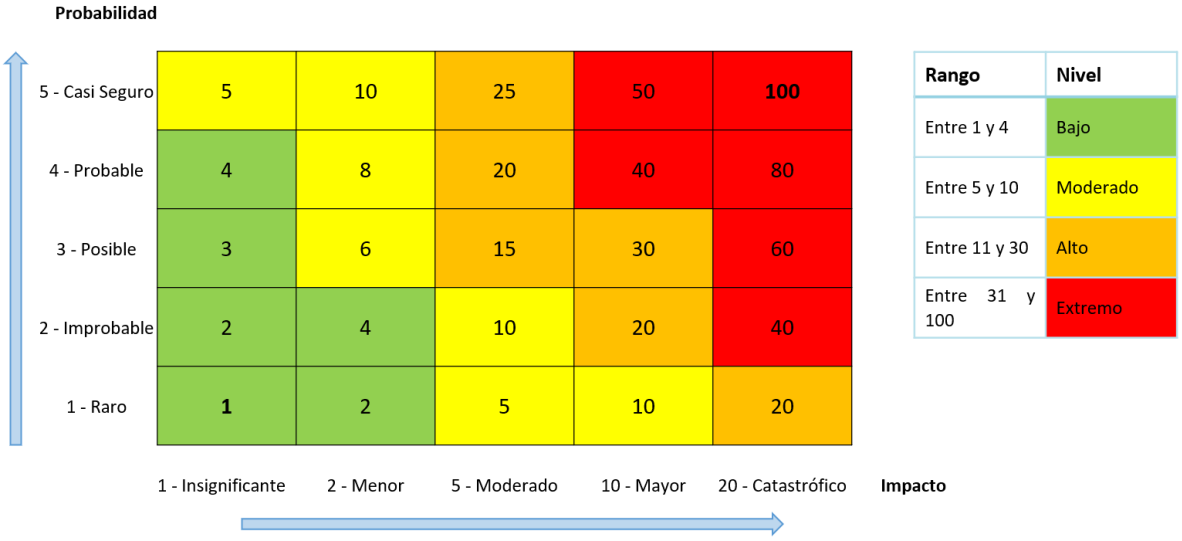
Rango	**Nivel de aceptabilidad**	**Descripción** *(después de obtener el nivel de riesgo residual)*	**Opción de tratamiento** *(después de obtener el nivel de riesgo residual)*
Entre 1 y 4	Bajo	En este nivel se pueden asumir los riesgos. **Riesgos aceptables.**	***Asumir*** (Aceptar)
Entre 5 y 10	Moderado	**Riesgos tolerables, límite de la capacidad de riesgos definida por la UNAL**	***Asumir*** (aceptar) ***Reducir*** ***Transferir***
Entre 11 y 30	Alto	**Riesgos importantes por fuera de la capacidad de riesgos definida por la UNAL**	***Opción de tratamiento*** **- *Reducir*** **- *Transferir*** **Otras acciones obligatorias** *- Definir los KRI's* *- Reportar a la instancia correspondiente.*
Entre 31 y 100	Extremo	**Riesgos inaceptables por fuera de la capacidad de riesgos definida por la UNAL**	***Opción de tratamiento*** **- *Reducir (mitigar)*** con nuevos controles, planes de acción o actividades. **- *Transferir*** **Otras acciones obligatorias** *- Definir los KRI's* *- Reportar a la instancia correspondiente.*

[39] La definición de Mapa de Calor se puede consultar en el numeral "1.5 Definiciones" de este documento.
[40] La tabla detallada de niveles de aceptabilidad, con la descripción de las opciones de tratamiento y los KRI's se describen con detalle en su apartado correspondiente; véase el numeral *2.4.5 Etapa tratamiento del riesgo.*

2.4.3.3.3 Mapa de Calor

El ***Mapa de Calor*** definido para ***cualquier tipología de riesgos*** contenida en el MIGR UNAL, excepto los riesgos de corrupción de procesos, se muestra en la ilustración 11.

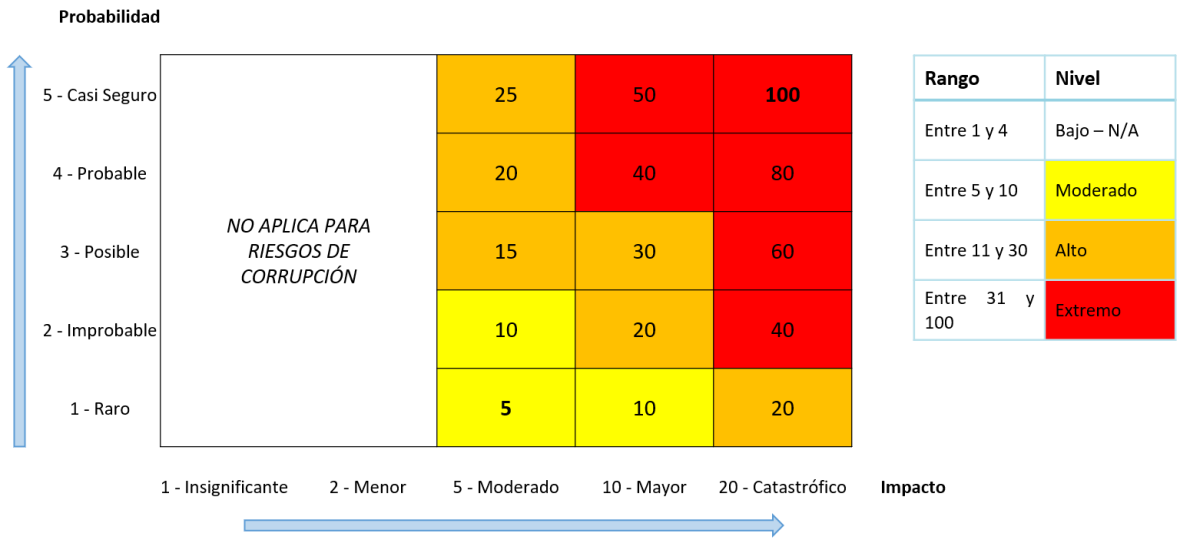
Ilustración 11 - Mapa de calor aplicable a las tipologías de riesgos contenidas en el MIGR



Rango	Nivel
Entre 1 y 4	Bajo
Entre 5 y 10	Moderado
Entre 11 y 30	Alto
Entre 31 y 100	Extremo

Considerando que en ***los riesgos de corrupción*** el impacto solo puede ser "moderado", "mayor" o "catastrófico", ***el mapa de calor aplicable única y exclusivamente para esta tipología*** es el que se expone en la ilustración 11.

Ilustración 12 - Mapa de Calor aplicable exclusivamente para los riesgos de corrupción



Rango	Nivel
Entre 1 y 4	Bajo – N/A
Entre 5 y 10	Moderado
Entre 11 y 30	Alto
Entre 31 y 100	Extremo

*- El **nivel de riesgo inherente** se debe establecer para todos los riesgos resultantes de la etapa de "Identificación del riesgo"; **se obtiene multiplicando** el valor del nivel de probabilidad con el valor del nivel de impacto, **o al ubicar** el valor de probabilidad e impacto en el Mapa de Calor.*

*- El **nivel de riesgo inherente** se obtiene sin considerar la presencia de mecanismos de control.*

*- Los **riesgos identificados,** priorizados con su respectiva redacción y nivel probabilidad, impacto y riesgo inherente, **deben ser ubicados en el Mapa de Calor.***

*- Las **acciones** y la **opción de tratamiento** para un riesgo se deciden en la etapa de **"Tratamiento del riesgo"** (numeral 2.4.5), después de obtener y tomando como referente **el nivel de riesgo residual**.*

2.4.3.4 Apetito, tolerancia y capacidad del riesgo

El ***apetito***, la ***tolerancia*** y la ***capacidad del riesgo***[41] son conceptos transversales que juegan un ***rol crucial en la gestión integral del riesgo***, ya que ***permiten articular y alinear*** la **planeación estratégica**, el ***quehacer/operación*** y la ***cultura*** institucional, el ***modelo y*** la ***estructura organizacional,*** así como la ***gestión del riesgo***, contrastando aquellos riesgos a los que la UNAL se ve expuesta con aquellos que puede, desea o está en el deber de buscar ***asumir.***

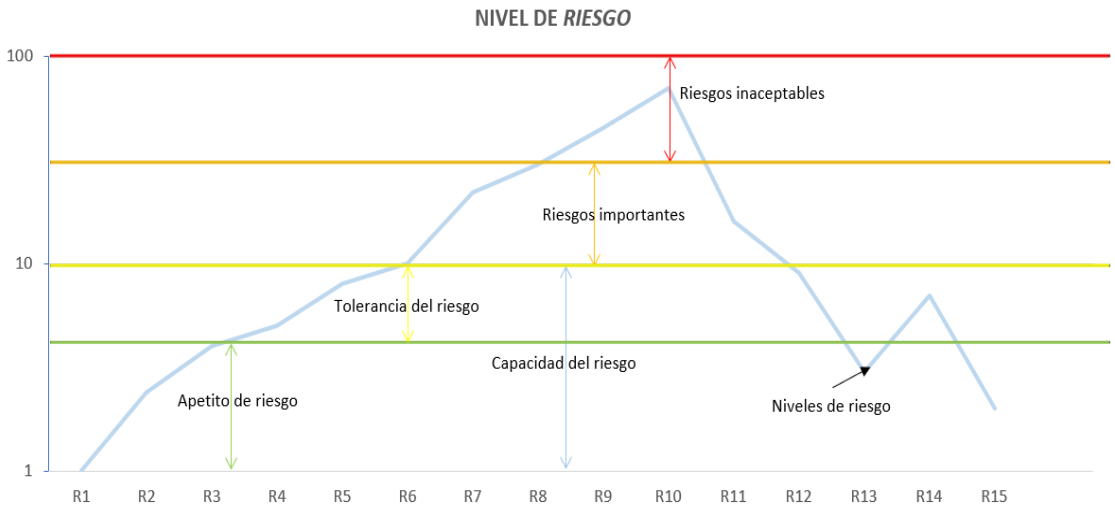
Estos conceptos influyen en la operación, la estrategia y los fines misionales de la UNAL, al igual que en la cultura de la gestión de los riesgos de las tipologías contenidas en el MIGR. La definición de dichos conceptos contempla la política integral de gestión del riesgo, los roles y las responsabilidades del modelo de las tres líneas de defensa, al igual que las pautas metodológicas de cada una de las etapas del proceso para la gestión del riesgo.

Teniendo en cuenta los elementos anteriores y las disposiciones de la alta dirección, ***el apetito de riesgo comprenderá aquellos con un nivel de riesgo residual bajo para la organización; la tolerancia del riesgo comprenderá los riesgos con un nivel de riesgo residual moderado para la UNAL; la capacidad del riesgo abarcará el umbral del apetito llegando hasta el valor máximo del umbral de tolerancia, es decir, los riesgos residuales bajos y moderados.***

Según el ***Mapa de Calor***, los ***parámetros de probabilidad e impacto, los niveles de aceptabilidad y el concepto de la alta dirección***, se encuentran definidos en la ilustración 13 los ***umbrales*** de ***apetito***, ***tolerancia*** y ***capacidad del riesgo*** para la UNAL, pensados para garantizar, en la medida de lo posible, la protección-creación de valor y el cumplimiento de los fines misionales y los objetivos de los procesos, las estrategias, los proyectos y sistemas de gestión, con base en una gestión priorizada de los riesgos significativos, implementado controles y acciones de tratamiento con la asesoría y el criterio de los expertos y de la alta dirección.

[41] Las definiciones de *apetito*, *tolerancia* y *capacidad* del riesgo pueden consultarse en el numeral "1.5 Definiciones" de este documento.

Ilustración 13 - Apetito, tolerancia y capacidad del riesgo aplicables a las tipologías de riesgo del MIGR UNAL



Concepto	Umbral
Apetito	Entre 1 y 4
Tolerancia	Entre 5 y 10
Capacidad	Entre 1 y 10
Riesgos importantes	Entre 11 y 30
Riesgos inaceptables	Entre 31 y 100

De los conceptos anteriores se infiere que: 1. El apetito de riesgo es el nivel de riesgo que la UNAL puede aceptar, y que a su vez permite el logro de los objetivos institucionales y de los procesos, las estrategias, los proyectos y/o sistemas de gestión en condiciones normales de operación. 2. La capacidad de riesgo es el nivel máximo de riesgo que la UNAL puede soportar, de manera que se delimita el punto en el cual no sería posible alcanzar el logro de los objetivos institucionales y demás. 3. La tolerancia de riesgo permite definir y limitar las acciones, complementarias a los controles, para abordar un riesgo[42].

*- La aplicación del **apetito**, la **tolerancia** y la **capacidad** del riesgo permite **tomar decisiones articuladas** con las intenciones de la **alta dirección** y la **capacidad operativa**, además de establecer las **acciones** y la **opción de tratamiento** a seguir frente a los riesgos identificados, redactados y priorizados en la etapa de "Identificación" con sus respectivos análisis del nivel de riesgo inherente y valoración del nivel de riesgo residual.*

- Los riesgos de cualquier tipología deben ser analizados cada uno por separado bajo estos conceptos, ya que todos los riesgos presentan un contexto diferente y, por tanto, unos niveles de probabilidad e impacto propios.

[42] La Fabrica del Pensamiento del Instituto de Auditores Internos de España menciona en su guía para la "Definición e implantación de Apetito de riesgos" lo siguiente: "en la determinación del apetito de riesgo, se deben contemplar además otros aspectos como la tolerancia y la capacidad de la empresa. De este modo, mientras que el apetito es el nivel de riesgo que la empresa quiere aceptar, aquel con el que se siente cómoda, su tolerancia será la desviación respecto a este nivel. Por otro lado, la capacidad de asumir riesgos será el nivel máximo de riesgo que una organización puedo soportar en la persecución de sus objetivos. Así, la tolerancia servirá como alerta para evitar que la empresa llegue al nivel establecido por su capacidad, algo que pondría en peligro la continuidad del negocio".

*Los responsables de la segunda línea de defensa de cada tipología deben facilitar e instruir en el uso de herramientas y métodos para determinar: 1. El **nivel de probabilidad e impacto**; 2. El **nivel de riesgo inherente y el nivel de aceptabilidad** con su ubicación en el **mapa de calor**; 3. El análisis del riesgo frente a los **umbrales** de **apetito, tolerancia** y **capacidad** del riesgo, para cada uno de los riesgos identificados; así, se brinda asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su gestión. Además, se debe llevar un registro y soporte de estos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios **De documentación y uso de sistemas de información para la administración de riesgos** del numeral **2.1.4.5** del presente documento.*

2.4.4 Evaluación del riesgo – Valoración del riesgo

En esta etapa se ***establecen*** y ***valoran*** para el listado de riesgos identificados, priorizados, redactados y analizados con su nivel de riesgo inherente, los ***mecanismos de control*** que se utilizarán para reducir la probabilidad de ocurrencia del riesgo y los impactos de su materialización; para ello se deben definir unos ***atributos informativos*** con miras a la correcta ***identificación de los controles***, luego, por medio de ***atributos de eficiencia y eficacia*** se evalúa el diseño y el resultado de su implementación. Los ***atributos de eficiencia*** permiten saber qué tanto disminuye el control el nivel de probabilidad o el impacto del riesgo asociado; los ***atributos de eficacia*** permiten conocer el resultado de la ejecución del control en un periodo de tiempo, mientras la combinación de ambos atributos permite establecer la ***efectividad del control***.

Posterior a la ***identificación y valoración de controles***, partiendo de la ***contribución de su diseño*** a la ***reducción de los niveles de probabilidad e impacto***, se procede a obtener el ***nivel de riesgo residual*** disminuyendo de forma acumulativa estas variables; con ello y a partir de los resultados de la etapa anterior de "Análisis del riesgo" se completa el ***perfil de riesgos*** y se procede a comprender y estudiar la criticidad del riesgo según el ***apetito***, la ***tolerancia*** y la ***capacidad del riesgo*** definidos por la institución, de modo que se establece para cada riesgo su nivel de aceptabilidad y aquellos que pueden ser ***asumidos*** para la institución, aquellos que están en el ***umbral de tolerancia*** y dentro de la ***capacidad definida***, y aquellos que están por ***fuera de la capacidad*** al ser significativos, importantes o inaceptables para la institución.

Si bien los parámetros que permiten definir y analizar un riesgo pueden variar de una tipología a otra, los ***atributos para identificar y valorar un control son iguales para cualquier tipología de riesgo*** del MIGR presente en los procesos, los proyectos, las estrategias y los sistemas de gestión de la UNAL; la ***valoración de los atributos estará sujeta al conocimiento, el criterio y la experticia del evaluador***. Para fines prácticos, la UNAL identificará y valorará sus controles y obtendrá el riesgo residual utilizando los siguientes parámetros.

2.4.4.1 Identificación de controles – tipos, características y atributos informativos

2.4.4.1.1 Tipos de controles

Los ***controles*** son mecanismos diseñados e implementados con el fin de ***modificar el riesgo***, ya que actúan sobre alguna de las dos variables de su medición (probabilidad o impacto), bien sea para

prevenirlo o ***detectarlo*** a tiempo (evitar que se materialice), o bien ***mitigarlo*** (minimizar las consecuencias).

Si bien existen en la literatura y en los referentes nacionales e internacionales diferentes clasificaciones para los controles, en el caso de la UNAL se han definido dos grandes tipos según las variables probabilidad e impacto utilizadas en el análisis y la valoración de los riesgos.

2.4.4.1.1.1 Controles de probabilidad

Recaen sobre las ***causas*** al atacar la probabilidad de ocurrencia del riesgo. Tienen como objetivo ***evitar*** que las ***causas inmediatas y/o raíz*** que ocasionan el riesgo se presenten, de manera que previenen su materialización. Los controles preventivos y algunos controles detectivos son controles de probabilidad. **Ejemplos:**

- Ejecución de programas de capacitación y entrenamiento.
- Aplicación de listas de chequeo.
- Verificación de firmas.
- Aplicación de control dual.
- Seguimiento o aplicación de normas, lineamientos y directrices.
- Segregación de funciones.
- Utilización de controles de acceso físicos (lector de huellas, tarjetas inteligentes) o digitales (sistemas de autenticación, perfiles de acceso).
- Revisiones y vistos buenos de superiores.
- Elaboración, revisión o seguimiento a informes periódicos.
- Ejecución o seguimiento a cronogramas, planes de trabajo.
- Implantación de niveles de autorización en sistemas de información.
- Registros de información.
- Aplicación de procedimientos, manuales, guías e instructivos.
- Ejecución de mantenimiento preventivo.
- Activación/generación de alertas de los sistemas de información.
- Tercerización o subcontratación de actividades.

2.4.4.1.1.2 Controles de impacto

Recaen en la ***consecuencia*** generada por la eventual ***materialización del riesgo*** y tienen como objetivo ***atacar y mitigar*** los impactos o efectos provocados por su materialización. Los controles correctivos y algunos controles detectivos son controles de impacto. **Ejemplos:**

- Ejecución de auditorías internas o externas.
- Puesta en marcha de planes de contingencia.
- Ejecución de *backup* o respaldos de información.
- Análisis y medición de indicadores.
- Realización de autoevaluaciones.
- Confrontación de información para identificar diferencias (conciliaciones).
- Ejecución de mantenimiento correctivo.
- Retroalimentación a través de comités o reuniones periódicas.
- Aplicación de pólizas y seguros.

- Evaluación del desempeño.
- Evaluación del grado de satisfacción de usuarios.
- Inspecciones no programadas.
- Seguimiento al reporte de peticiones, queja y reclamos.

2.4.4.1.2 Características de los controles

Se recomienda, en el momento de identificar los controles de probabilidad e impacto para un riesgo de cualquier tipología, verificar el cumplimiento de las características que se exponen en la ilustración 14.

Ilustración 14 - Características de los controles

Oportunidad	•El control debe ser aplicado en el momento adecuado respecto al evento que se espera controlar.
Economía (costo - beneficio)	•El costo del control no debe superar el beneficio derivado de su aplicación. Su representación en tiempo y dinero debe justificarse con las ventajas reales de los resultados que se obtengan.
Significancia	•Los controles deben corresponder con actividades importantes dentro del proceso y no con cuestiones sin trascendencia.
Operatividad	El control debe ejecutarse con facilidad sin crear confusiones. Si un control resulta incomprensible para el usuario, a la larga este será ignorado.
Funcionalidad	El control debe guardar estrecha relación con los riesgos asociados a través de su objetivo, es decir, se debe tener claridad en cuanto a qué se busca con la aplicación de dicho control.
Viabilidad técnica	•Se debe estimar si es posible que el control se ejecute con las condiciones tecnológicas, los conocimientos y las herramientas disponibles.
Apego jurídico (opcional)	•El control debe estar sujeto a la legislación que rige a la institución y subordinado al principio de legalidad.

2.4.4.1.3 Identificación de controles – atributos informativos

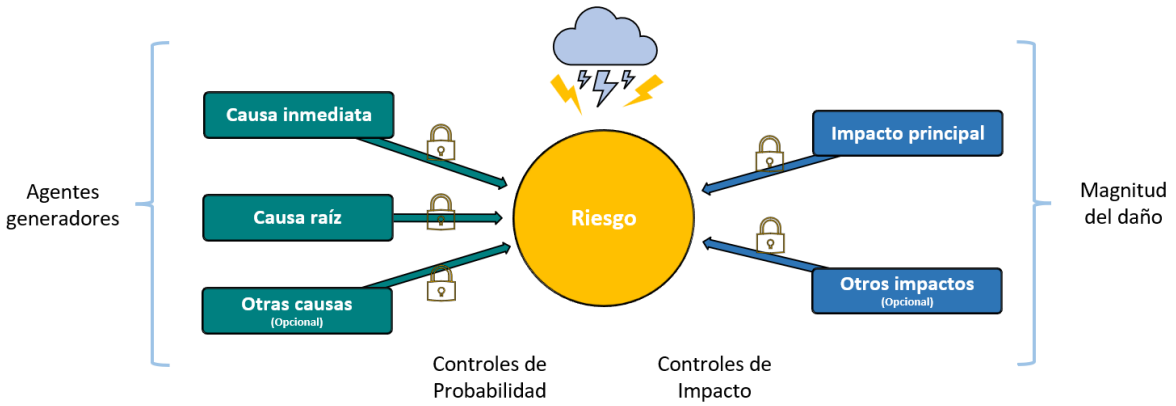
En el momento de ***identificar los controles*** de probabilidad e impacto que debe tener cada riesgo ***se debe garantizar*** que existan controles para el ***impacto*** y las ***causas*** que lo conforman. Para esto, cada riesgo debe contar con al menos dos o tres controles, uno para el impacto y uno o dos para la causa inmediata y/o la causa raíz. Es posible que en el momento de identificar dichos controles, el mecanismo propuesto para la causa inmediata sea igual para la causa raíz o viceversa. Asimismo, que existan ciertos riesgos a los cuales no se les pueda asociar un control de probabilidad o un control de impacto, por ejemplo, los riesgos con causas relacionadas a fenómenos naturales (como,

por ejemplo, terremotos o erupciones volcánicas), en los que no es posible utilizar controles de probabilidad para evitar la aparición de este tipo de causas, o los riesgos de corrupción a los cuales no es posible asociar controles de impacto por reglamentación del Departamento Administrativo de la Función Pública[43].

Para los casos en los que no sea posible establecer un control de probabilidad para las causas (inmediata y/o raíz) o impacto, se debe justificar el porqué e informar al responsable de la segunda línea de defensa correspondiente a la tipología del riesgo, instancia que revisará el caso con el fin de establecer el curso de acción que podrá ser monitorear o escalar a la Coordinación SIGA o al ETIR, los cuales evaluarán la situación y asesorarán sobre el curso a seguir; algunos casos podrán ser escalados del ETIR al CNSCSI para su análisis y la toma de decisiones correspondiente.

La ***relación*** de los dos ***tipos de controles*** con las ***causas*** e ***impactos*** se puede apreciar en la ilustración 15, en esquema de corbatín.

Ilustración 15 - Identificación de controles en esquema de corbatín



Luego de identificar los posibles controles de un riesgo, se debe establecer para cada control los ***atributos informativos*** que se muestran en la tabla 24.

Tabla 24 - Atributos informativos para identificar un control

Atributo	Descripción	Ejemplo[44]
Código	Identificador único que permite diferenciar el control de un riesgo de cualquier otro control.	CTI.013
Nombre	Nombre asignado al control; se sugiere en su redacción que este tenga implícita una acción acompañada de un sustantivo.	Creación de copias de seguridad para los sistemas de información.

[43] La guía para la administración del riesgo y el diseño de controles en entidades públicas V5 menciona en la página 70 que "[tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento".
[44] El control utilizado en el ejemplo es para fines ilustrativos. La información contenida en los campos es una elaboración propia y no hace referencia a ningún control usado en la institución. Este ejemplo será utilizado a lo largo de esta etapa.

Atributo	Descripción	Ejemplo[44]
Responsable	Funcionario, dependencia, procesos, sistema, tecnología o área encargada de su implementación.	Funcionario de seguridad de la DNED.
Objetivo (¿Qué hace?)	Establece para qué se realiza la actividad del control.	Mantener respaldos de la información que reposa en los aplicativos en un servidor /*data center* alterno para su uso en caso de emergencia – pérdida de información.
Descripción (¿cómo lo hace?) ***y*** ***Desviaciones***	**Descripción:** instrucción, procedimiento o paso a paso llevado a cabo para cumplir con la actividad /objetivo del control. **Desviaciones:** hace alusión al curso a seguir ante las observaciones encontradas durante la implementación del control.	**Descripción:** 1. Por medio del sistema de información, opción respaldos, se procede a crear y descargar la copia de seguridad. 2. La copia de seguridad generada es probada en el ambiente de pruebas del sistema, garantizando el cargue exitoso de la información. 3. La copia de seguridad es almacenada en el servidor "Copias de seguridad SI", en la carpeta correspondiente nombrándolo "AAAAMMDD backup SI". **Desviaciones:** 1. Si en la actividad de crear y descargar la copia de seguridad ocurre algún incidente, reintente el proceso nuevamente. En caso de persistir el error comuníquese con el área encargada a través de la mesa de ayuda. 2. Si en el momento de probar la copia de seguridad en el ambiente de pruebas del sistema correspondiente ocurre un error, se debe crear y descargar la copia nuevamente del ambiente de producción, y proceder nuevamente con su verificación en el ambiente de pruebas; si persiste el error comuníquese con el área encargada a través de la mesa de ayuda. 3. Si no puede tener acceso o no encuentra el servidor "Copias de seguridad SI", comuníquese con el área encargada a través de la mesa de ayuda.
Frecuencia de ejecución	Periodicidad con la que se ejecuta el control. Esta puede ser: - Permanente, diaria o constante. - Periódica: semanal, quincenal, mensual, bimestral, trimestral, semestral, anual… - Ocasional o por evento.	Mensual
Fecha de evaluación	Fecha en la que se está realizando la identificación, el seguimiento del control, la valoración de su eficiencia o eficacia.	01/02/2023
Variable que reduce	Variable "Probabilidad" (causa inmediata y/o raíz) o "Impacto" que se espera combatir con el control.	Impacto: Pérdida de información.
Documentado	Establece si el control cuenta con documentación controlada o no relacionada sobre su descripción y/o uso, o si se encuentra definido en alguna normatividad aplicable.	Si, Guía de implementación en el Sistema SoftExpert Código. U.GU.11.005.013. Incluido en la Política de Copias de seguridad emitida por la DNED.

Atributo	Descripción	Ejemplo[44]
Tipo de evidencia	Define cuál es el soporte de la ejecución del control que permita validar en algún momento la eficacia de su implementación.	Copia de seguridad en archivo comprimido almacenada en un servidor en la nube.

- Se debe garantizar en la medida de lo posible que existan **controles de probabilidad e impacto para cada riesgo**. *En los casos que no se pueda garantizar y según el nivel de riesgo residual, se debe escalar a la segunda línea de defensa (responsable de la tipología de riesgo, Coordinación SIGA o ETIR).*

- En los ***riesgos de corrupción no se identifican controles para disminuir el impacto*** *por reglamentación del DAFP.*

- Para ***identificar correctamente un control*** *se deben definir con claridad todos sus* ***atributos informativos, de eficiencia y de eficacia.***

2.4.4.2 Evaluación de controles - atributos de eficiencia y eficacia, obtención de la efectividad

Una correcta ***evaluación del control*** permite obtener una ***medida del éxito en su aplicación*** a través de su ***eficiencia*** (diseño) y su ***eficacia*** (resultado de su ejecución y logro del objetivo), en relación estrecha y directa de un ***riesgo en particular***; lo anterior porque un control que es efectivo para la reducción de un riesgo específico puede que no lo sea para otro diferente. A fin de evaluar el aporte de un control a la gestión de un riesgo de cualquier tipología se tendrán en cuenta las siguientes variables con sus lineamientos para determinarlas.

2.4.4.2.1 Eficiencia

Establece qué tan ***bien diseñado*** está un control con relación al riesgo que espera prevenir, detectar o mitigar; se obtiene en el momento de identificar el control (atributos informativos) para el riesgo y se debe evaluar periódicamente ante posibles cambios. Los ***atributos de eficiencia*** para determinarla se aprecian en la tabla 25.

Tabla 25 - Atributos de eficiencia para valorar un control

Atributo		Descripción	Peso	Ejemplo[45]
Naturaleza del control (25 %) (momento en el que actúa)	Preventivo	Control accionado antes o al inicio de que se realice la actividad originadora del riesgo.	**25 %**	Correctivo (15 %)
	Detectivo	Control accionado durante la ejecución de la actividad detectando el riesgo, permitiendo corregir o evitar sus deficiencias, pero generan reprocesos.	**20 %**	

[45] Para fines ilustrativos se continuará con el control de ejemplo "Creación de copias de seguridad para los Sistemas de información", usado en los atributos informativos.

Atributo		Descripción	Peso	Ejemplo[45]
	Correctivo	Control que actúa al finalizar la actividad o después que se materializa el riesgo, algunos suelen tener costos implícitos.	**15 %**	
Nivel de automatización (10 %)	Automático	Controles embebidos en la infraestructura tecnológica o sistemas de información que se ejecutan sin intervención humana, suelen ser actividades de procesamiento o validación de información.	**10 %**	Automático (10 %)
	Semiautomático	Controles que no son automáticos, pero sí involucran el uso de TIC (tecnologías de la información y las comunicaciones) y talento humano.	**7 %**	
	Manual	Controles que no involucran el uso de tecnologías de información, son ejecutados por personas y tienen implícitos el error humano.	**5 %**	
Cobertura (25 %)	Total	Control aplicado a todos los eventos que pueden desencadenar la causa u ocasionar el impacto sin importar sus características. Son usados a discreción de una persona, por un procedimiento, una normatividad o una tecnología específica.	**25%**	Parcial (15 %)
	Parcial	Control aplicado a una parte considerable de los eventos que pueden desencadenar la causa u ocasionar el impacto, limitado a sus características. Se usa a discreción de una persona, por un procedimiento, una normatividad o una tecnología específica.	**15 %**	
	Nula	Controles que se aplican a una pequeña porción o a ninguno de los eventos que pueden desencadenar la causa u ocasionar el impacto.	**0%**	
Nivel de periodicidad de ejecución (15 %)	Optimo	El control se realiza con la misma periodicidad que se ejecuta que actividad que conlleva al riesgo.	**15%**	Bueno (10%)
	Bueno	El control se realiza la mayoría de las veces que se ejecuta la actividad que conlleva a riesgo.	**10%**	
	Malo	El control se ejecuta con una escasa periodicidad con relación a la ejecución de la actividad que conlleva al riesgo.	**5 %**	
Madurez del control (25 %)	Definido, documentado, implementado socializado y seguimiento	El control se encuentra con información documentada y/o evidencias de su ejecución, hace parte del quehacer del proceso, la estrategia, el proyecto y/o el sistema de gestión; es conocido y aplicado por las personas involucradas y se realiza seguimiento para la toma de decisiones.	**25 %**	Definido, documentado, implementado y socializado (20 %)

Atributo		Descripción	Peso	Ejemplo[45]
	Definido, documentado, implementado y socializado	El control se encuentra con información documentada y/o evidencias de su ejecución; hace parte del quehacer del proceso, la estrategia, el proyecto y/o el sistema de gestión, y es conocido y aplicado por las personas involucradas.	**20 %**	
	Definido, documentado, implementado	El control cuenta con información documentada y/o evidencias de su ejecución y hace parte del quehacer del proceso, estrategia, proyecto y/o sistema de gestión.	**15%**	
	Definido y documentado	El control cuenta con información documentada y/o evidencias de su ejecución.	**10 %**	
	Definido	El control se encuentra operando de manera informal.	**5 %**	
Máximo % de eficiencia	***100 %***	***Porcentaje (%) de eficiencia del control***		***70 % - Medio***

Nivel	Rango	Descripción	Disminución *(en los niveles de probabilidad o impacto)*
Alto	Mayor o igual (>=) a 80 %	El control presenta un diseño eficiente.	***2***
Medio	Mayor o igual a 60 % y menor a 80 %	El control presenta un buen diseño ***susceptible de ser mejorado***.	***1***
Bajo	Menor (<) a 60 %	El control presenta deficiencias en su diseño, ***requiere acciones de mejora***, ***ser excluido*** o ***reemplazado por otro***.	***0***

La ***máxima eficiencia*** que podría tener un control es ***100*** % equivalente a la ***suma de los valores más altos de cada atributo***. El ***porcentaje (%) de eficiencia*** se obtiene con base en la siguiente fórmula:

$$\%\ Eficiencia\ del\ control = A1 + A2 + A3 + A4 + A5$$

Donde A1, A2, A3, A4, A5 hacen referencia al peso de cada uno de los atributos de eficiencia de control seleccionados.

El ***porcentaje de eficiencia*** del control se ubica en la escala de rangos para saber su nivel de eficiencia y con él la disminución de niveles en la probabilidad o impacto para el riesgo respectivo.

2.4.4.2.2 Eficacia

Hace referencia al ***resultado del control en su implementación*** y al ***cumplimiento de su objetivo*** en un periodo determinado con relación al riesgo que se espera prevenir, detectar o mitigar; se obtiene en el momento de identificar (atributos informativos) y diseñar (atributos de eficiencia) el control, o, como es más usual, en un intervalo de tiempo posterior a su identificación[46]; se debe evaluar periódicamente. La eficacia se obtiene por autoevaluación a cargo de los integrantes de la primera

[46] La eficacia de algunos controles de impacto se evalúa cuando ocurre el evento y se materializa el riesgo, por ejemplo, la aplicación de pólizas de seguro por robo o desastres naturales.

o segunda línea de defensa o por auditorías realizadas por la ONCI. Los ***atributos de eficacia*** para determinarla se exponen en la tabla 26.

Tabla 26 - Atributos de eficacia para valorar un control

Atributo		Descripción	Peso	Ejemplo[47]
Cumplimiento del objetivo (35 %)	Alto	Se cumplió completamente o en alta proporción el objetivo definido para el control durante su implementación.	**35 %**	Alto (35 %)
	Medio	Se cumplió medianamente o en una media proporción el objetivo definido para el control durante su implementación.	**20 %**	
	Bajo o nulo	Se cumplió nulamente, escasamente o en una baja proporción el objetivo definido para el control durante su implementación.	**0 %**	
Complejidad (15 %)	Simple	Se observa que el control es de fácil aplicación y se encuentra apropiado en el proceso, la estrategia, el proyecto, el sistema de gestión u objeto evaluado.	**15 %**	Simple (15 %)
	Complejo	NO Se observa que el control sea de fácil aplicación y/o que se encuentre apropiado en el proceso, la estrategia, el proyecto, sistema de gestión u objeto evaluado.	**5 %**	
Pertinencia de ejecución (20 %)	Pertinente	El control es ejecutado con la frecuencia y por el responsable definido en los ***atributos informativos.***	**20 %**	No pertinente (0%)
	No pertinente	El control NO es ejecutado con la frecuencia y/o por el responsable definido en los ***atributos informativos.***	**0 %**	
Evidencia de la ejecución del control (30 %)	Evidencia suficiente	Se cuenta con soportes suficientes y pertinentes para garantizar la correcta implementación y trazabilidad del control.	**30 %**	Evidencia suficiente (30 %)
	Evidencia insuficiente	NO se cuenta con soportes suficientes y pertinentes para garantizar la correcta implementación y trazabilidad del control.	**0 %**	
Máximo % Eficacia	***100 %***	***Porcentaje (%) de eficacia del control***		***80 % - Alto***

Nivel	Rango	Descripción
Alto	Mayor o igual (>=) a 80 %	El control presenta un óptimo funcionamiento y cumplimiento de su objetivo.
Medio	Mayor o igual a 60 % y menor a 80 %	El control presenta un buen funcionamiento y cumplimiento de su objetivo, ***susceptible de ser mejorado.***
Bajo	Menor (<) a 60 %	El control presenta deficiencias en su funcionamiento y/o cumplimiento de su objetivo, ***requiere acciones.***

La ***máxima eficacia*** que podría tener un control es ***100*** %, equivalente a la ***suma de los valores más altos de cada atributo***. El ***porcentaje (%) de eficacia*** se obtiene con base en la siguiente fórmula:

[47] Para fines ilustrativos se continuará con el control de ejemplo "Creación de copias de seguridad para los Sistemas de información", usado en los atributos informativos y de eficacia.

$$\%\ Eficacia\ del\ control = A1 + A2 + A3 + A4$$

Donde A1, A2,A3, A4 hacen referencia al peso de cada uno de los atributos de eficacia de control seleccionados.

El ***porcentaje de eficacia*** del control se ubica en la escala de rangos para saber su nivel de eficacia y con él el éxito de su implementación y cumplimiento del objetivo.

2.4.4.2.3 Efectividad

Permite obtener una ***valoración del éxito de un control*** a través de su ***eficiencia*** (diseño) y ***eficacia*** (funcionamiento y logro del objetivo) en relación estrecha y directa de un riesgo en particular. El ***Porcentaje (%) de Efectividad*** de un control se obtiene con la siguiente fórmula:

$$\%\ Efectividad\ del\ control = \%\ Eficiencia\ (0{,}35) + \%Eficacia(0{,}65)$$

El ***porcentaje de efectividad*** del control se ubica en la escala de rangos para conocer su nivel de éxito.

Tabla 27 - Niveles y rangos de efectividad de controles

Nivel	Rango	Descripción
Alto	Mayor o igual (>=) a 80 %	El control presenta un diseño y funcionamiento ***óptimos.***
Medio	Mayor o igual a 60 % y menor a 80 %	El control presenta un buen diseño y funcionamiento, ***susceptible(s) de ser mejorado(s).***
Bajo	Menor (<) a 60 %	El control presenta deficiencias en su diseño y/o funcionamiento, ***requiere acciones de mejora*** en su diseño (eficiencia) y/o al momento de su ejecución (eficacia).

*- Para **evaluar** correctamente el **diseño** e **implementación** de un control se deben **definir** con **claridad** sus **atributos de eficiencia y eficacia**; luego de obtenerlos se deben de operar para determinar la **efectividad del control.***

- El porcentaje obtenido al sumar los pesos de los atributos de eficiencia de un control permite establecer el número de niveles (uno o dos) de probabilidad o impacto que este ayuda a disminuir.

- El porcentaje obtenido al sumar los pesos de los atributos de eficacia de un control permite establecer el nivel de cumplimiento de su objetivo y el resultado de su implementación en la práctica.

*- Se debe obtener para **cada control** de un riesgo el **porcentaje de eficiencia, eficacia y efectividad**.*

2.4.4.3 Controles institucionales para la gestión de causas transversales

Este capítulo que está pensado a futuro para la próxima versión del MIGR. Pretende, de la mano de los actores de los procesos, de las estrategias, los proyectos y sistemas de gestión de las múltiples

tipologías de riesgos, construir un catalogó de controles que estén implementados en el quehacer institucional para combatir los riesgos de cualquier tipología generados por ciertas causas transversales. Con este se pretende optimizar los recursos de la institución en el momento de combatir los riesgos al poder implementarse estos controles en múltiples eventos, y dar un apoyo a los integrantes de la primera línea de defensa encargados de identificar los controles para cada riesgo.

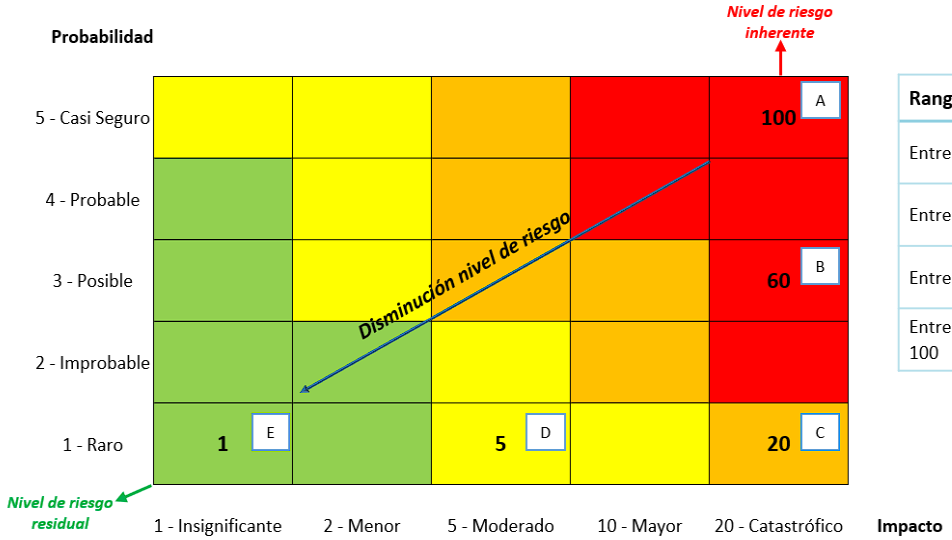
2.4.4.4 Cálculo del nivel de riesgo residual

El ***nivel de riesgo residual*** conocido como ***nivel de riesgo remanente,*** es aquel que persiste ***después de haberse aplicado los controles*** que corresponden con el evento identificado, partiendo de la premisa que el riesgo nunca podrá ser nulo a menos que desaparezca la actividad o causa que lo podría generar y/o los activos amenazados, y que la intensión de su gestión es generar un grado de confianza razonable en el cumplimiento de los objetivos del proceso, estrategia, proyecto o sistema de gestión, llevando los riesgos a un nivel ***aceptable*** (asumible) o ***tolerable***.

Para el cálculo del ***nivel riesgo residual*** y el ***nivel de aceptabilidad*** se parte de la calificación del ***nivel de riesgo inherente*** y se comienza a reducir la variable ***probabilidad*** restando el número de casillas que se hayan identificado en la evaluación de la ***eficiencia*** de los controles de este tipo y recalculando el riesgo residual. Lo mismo sucede con la reducción de la variable ***impacto***. Esta operación es ***acumulativa***, lo que quiere decir que en la medida que se van asociando los controles se toma el valor parcial del riesgo que se obtuvo con el control anterior para seguir disminuyendo su valoración. Para entender mejor ésta dinámica a continuación se muestra un ejemplo:

"Se tiene un evento con un nivel de riesgo inherente en zona extrema con calificación 100 (5x20), al que se le identificaron cuatro controles: dos de probabilidad y dos de impacto, todos con un porcentaje de eficiencia superior al 80 %, esto quiere decir que individualmente cada control contribuye a disminuir dos niveles en el mapa de calor" (véase la ilustración 16).

Ilustración 16 - Ejemplo: cálculo del nivel de riesgo residual



Rango	Nivel
Entre 1 y 4	Bajo
Entre 5 y 10	Moderado
Entre 11 y 30	Alto
Entre 31 y 100	Extremo

Momento	Probabilidad	Impacto	Nivel
A. Riesgo inherente	5 – Casi seguro	20 - Catastrófico	100 - Extremo
B. Control 1 Probab *(Riesgo Residual parcial)*	3 - Probable	20 - Catastrófico	60 - Extremo
C. Control 2 Probab *(Riesgo Residual parcial)*	1 - Raro	20 - Catastrófico	Alto
D. Control 3 Imp *(Riesgo Residual parcial)*	1 - Raro	5 - Moderado	5 - Moderado
E. Control 4 Imp *(Riesgo residual Final)*	1 - Raro	1 - Insignificante	Extremo

Analizando la ilustración 16 se observa que el control 1 afecta la probabilidad al disminuir dos niveles, por lo tanto, pasa de ser un riesgo 5 "casi seguro" a ser 3 "posible", y su nivel residual parcial es de 60 extremo (3x20). El siguiente control también es de probabilidad y disminuye dos niveles más esta variable, por lo que el riesgo continúa disminuyendo, al pasar de 3 "posible" a 1 "raro" y su nivel residual parcial es de 20 Moderado (1x20).

El tercer control es de impacto, por lo tanto, se comienza a disminuir dos niveles. Esta variable pasa de 20 "catastrófico" a 5 "moderado", y en este caso el nivel residual parcial es 5 Bajo (1x5). Finalmente, el cuarto control de impacto reduce dos niveles más, llevando esta variable al nivel 1 "insignificante", dando como resultado que el **nivel de riesgo residual** *final es 1 "Bajo" (1x1).*

Luego de obtener el ***nivel de riesgo residual***, se deben ubicar todos los riesgos con su respectiva valoración en el ***Mapa de Calor***.

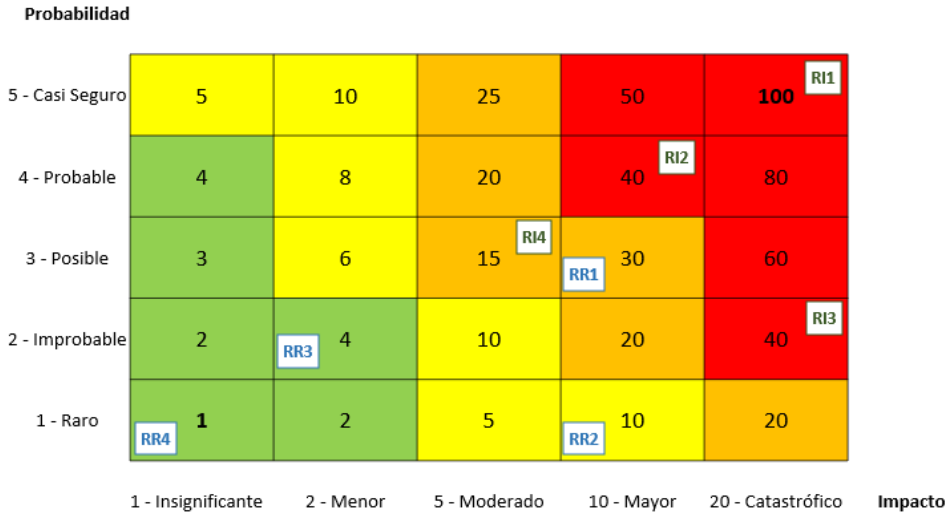
*- El **nivel de riesgo residual** se obtiene con base en los resultados de la etapa de análisis, utilizando la **evaluación de eficiencia** del control para **disminuir** el **nivel de probabilidad o impacto**.*

*- El **nivel de riesgo residual** se contrasta la valoración inherente del **perfil del riesgo** y el **apetito**, la **tolerancia** y la **capacidad** del riesgo definidas por la UNAL, permitiendo así conocer el nivel de aceptabilidad del riesgo y con este las **acciones** y **opciones de tratamiento** que se deben surtir para su gestión de acuerdo con su nivel de criticidad.*

2.4.4.5 Perfil de riesgos

Es el ***resultado consolidado de la medición permanente de los riesgos*** a los que se ve expuesta la Universidad. Este puede obtenerse para uno o varios riesgos y tipologías de riesgo en uno o más periodos de tiempo y se determina con los resultados del ***nivel de riesgos inherente y residual***, es decir, el perfil de riesgos puede entenderse como las "Fotografías" de la valoración de los riesgos tanto inherente como residual de la entidad, que se va revisando y modificando a través del tiempo. En las ilustraciones 17-18 se aprecian algunos ejemplos de perfil de riesgos[48].

Ilustración 17 - Perfil de riesgo para múltiples riesgos en un periodo de tiempo

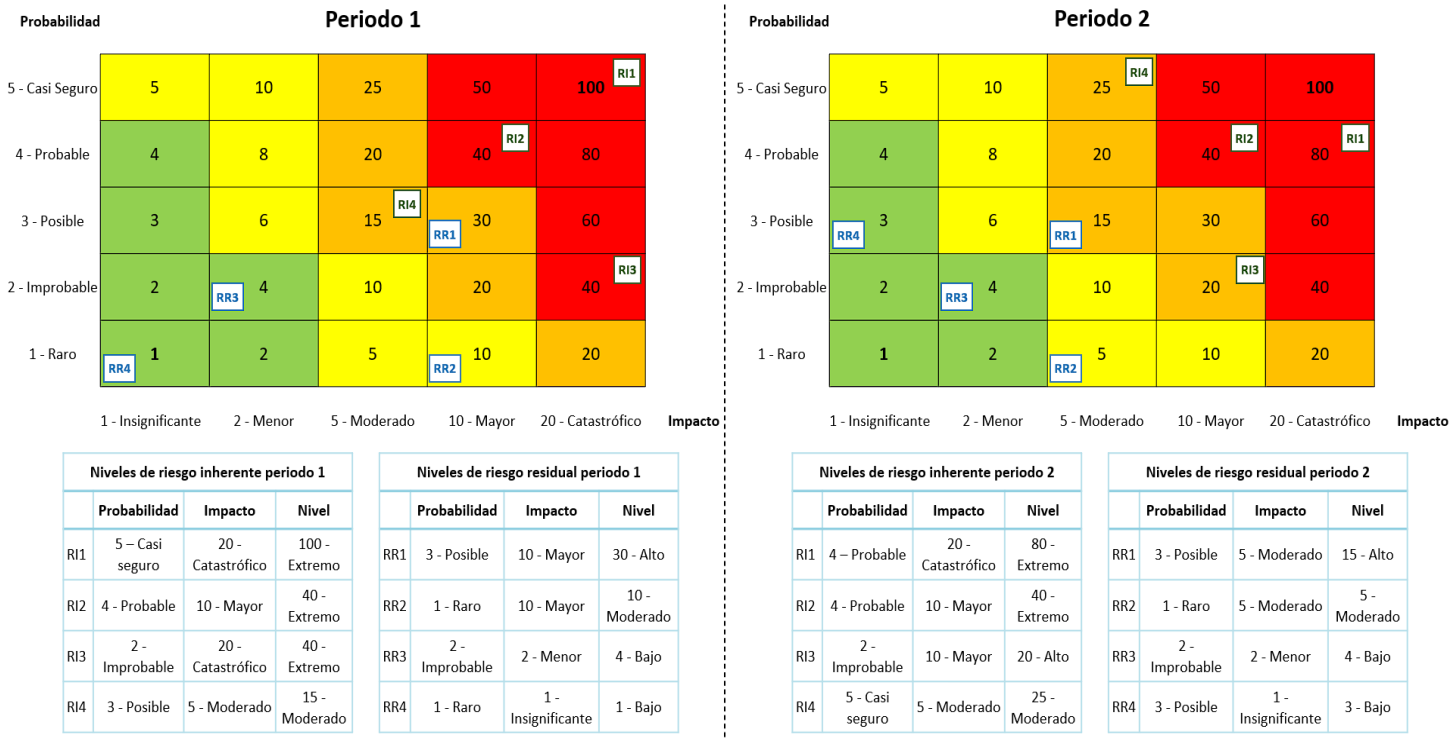


Niveles de riesgo inherente			
	Probabilidad	**Impacto**	**Nivel**
RI1	5 – Casi seguro	20 - Catastrófico	100 - Extremo
RI2	4 - Probable	10 - Mayor	40 - Extremo
RI3	2 - Improbable	20 - Catastrófico	40 - Extremo
RI4	3 - Posible	5 - Moderado	15 - Moderado

Niveles de riesgo residual			
	Probabilidad	**Impacto**	**Nivel**
RR1	3 - Posible	10 - Mayor	30 - Alto
RR2	1 - Raro	10 - Mayor	10 - Moderado
RR3	2 - Improbable	2 - Menor	4 - Bajo
RR4	1 - Raro	1 - Insignificante	1 - Bajo

[48] Las ilustraciones usadas en los ejemplos del perfil de riesgos son de referencia, pueden elaborarse o combinarse otras gráficas que expresen las "Fotografías" de las valoraciones inherentes y residuales de uno o más riesgos en uno o múltiples periodos de tiempo para una o varias tipologías de riesgo.

Ilustración 18 - Perfil de riesgo para múltiples riesgos en dos periodos de tiempo



Niveles de riesgo inherente periodo 1			
	Probabilidad	**Impacto**	**Nivel**
RI1	5 – Casi seguro	20 - Catastrófico	100 - Extremo
RI2	4 - Probable	10 - Mayor	40 - Extremo
RI3	2 - Improbable	20 - Catastrófico	40 - Extremo
RI4	3 - Posible	5 - Moderado	15 - Moderado

Niveles de riesgo residual periodo 1			
	Probabilidad	**Impacto**	**Nivel**
RR1	3 - Posible	10 - Mayor	30 - Alto
RR2	1 - Raro	10 - Mayor	10 - Moderado
RR3	2 - Improbable	2 - Menor	4 - Bajo
RR4	1 - Raro	1 - Insignificante	1 - Bajo

Niveles de riesgo inherente periodo 2			
	Probabilidad	**Impacto**	**Nivel**
RI1	4 – Probable	20 - Catastrófico	80 - Extremo
RI2	4 - Probable	10 - Mayor	40 - Extremo
RI3	2 - Improbable	10 - Mayor	20 - Alto
RI4	5 - Casi seguro	5 - Moderado	25 - Moderado

Niveles de riesgo residual periodo 2			
	Probabilidad	**Impacto**	**Nivel**
RR1	3 - Posible	5 - Moderado	15 - Alto
RR2	1 - Raro	5 - Moderado	5 - Moderado
RR3	2 - Improbable	2 - Menor	4 - Bajo
RR4	3 - Posible	1 - Insignificante	3 - Bajo

*El **perfil de riesgos** permite **comparar uno o más riesgos** de una o múltiples tipologías según su **nivel de riesgo inherente – residual** y su **ubicación** en el **Mapa de Calor**, en uno o varios **periodos de tiempo**, dando información de su comportamiento.*

2.4.4.6 Priorización de riesgos (riesgos residuales significativos)

La ***priorización*** de riesgos es el ***insumo principal*** para la etapa de ***"Tratamiento del riesgo"*** (véase el numeral 2.4.5); en esta se parte del nivel de riesgo residual, de manera que permite priorizar los riesgos por sus niveles de aceptabilidad ***Bajo***, ***moderado***, ***Alto*** o ***Extremo***.

Los **riesgos** residuales ***significativos*** son aquellos eventos con un ***nivel de riesgo residual Alto*** (entre 11 y 30) y ***Extremo*** (Entre 31 y 100); estos son ***priorizados*** para su ***tratamiento*** sobre los riesgos con un nivel residual ***Moderado*** (entre 5 y 10) y ***Bajo*** (entre 1 y 4).

*- La **priorización de riesgos,** partiendo del **nivel de riesgo residual**, permite identificar aquellos **más significativos** (Altos y Extremos) para los procesos, las estrategias, los proyectos y sistemas de gestión, más **NO permite excluir** aquellos que entran en la **capacidad** del riesgo (Bajos y Moderados) definida por la institución.*

*- Si existen eventos con **niveles de riesgo residual moderados, altos y extremos**, se **prioriza** la gestión de los riesgos residuales significativos **altos y extremos**; Si existen solamente riesgos residuales bajos y moderados, si es viable y beneficioso para la institución, se puede optar por opciones de tratamiento para reducirlos.*

- Los riesgos identificados por la primera línea de defensa y valorados con un nivel de riesgos residual alto o extremo deberán ser reportados a los responsables de la segunda línea de defensa de la tipología correspondiente para su seguimiento.

*Los responsables de la segunda línea de defensa de cada tipología deben facilitar e instruir en el uso de herramientas y métodos para determinar: 1. Los **controles para la(s) causa(s) e impacto** del riesgo; 2. Los **atributos informativos, de eficiencia y eficacia** del control; 3. El **nivel de riesgo residual** y el **nivel de aceptabilidad** con la respectiva disminución de la probabilidad y el impacto generada por la eficiencia de los controles identificados y su ubicación en el **mapa de calor**. 3. La **comprensión del riesgo** frente al **perfil del riesgo** y los **umbrales** de **apetito**, **tolerancia** y **capacidad** del riesgo, para cada uno de los riesgos identificados, brindando asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su gestión. Además, se debe llevar un registro y soporte de estos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios **De documentación y uso de sistemas de información para la administración de riesgos** del numeral **2.1.4.5** del presente documento.*

2.4.5 Tratamiento del riesgo

Está claro que no todos los riesgos tienen el mismo ***nivel de criticidad*** y que su gestión implica una serie de ***esfuerzos*** en los que deben incurrir los procesos, las estrategias, los proyectos, los sistemas de gestión y, en general, la institución, de ahí la importancia de establecer cuáles de ellos son ***aceptables*** (bajos y moderados) y cuáles son ***inaceptables*** (altos y extremo) para saber cómo y por dónde empezar a gestionarlos.

Par entender las ***acciones*** y definir la ***opción de tratamiento*** y los ***KRI's*** de cada riesgo de cualquier tipología se debe tener en cuenta el ***nivel de riesgo residual*** con su respectivo nivel de aceptabilidad obtenido, así como los conceptos de ***apetito***, ***tolerancia*** y ***capacidad*** del riesgo establecidos por la UNAL, tal como se aprecia en la tabla 28.

Tabla 28 - Tratamiento de los riesgos de cualquier tipología con base en el nivel de riesgo residual

Nivel R Residual	Nivel de aceptabilidad	Acción	Opción de tratamiento
Entre 1 y 4	Bajo	Los riesgos en esta zona se encuentran en un nivel que puede gestionarse con los controles establecidos en la entidad. Ello requiere asumir los riesgos. **Riesgos aceptables.**	***Asumir*** (aceptar) con la implementación de los controles definidos.

Nivel R Residual	Nivel de aceptabilidad	Acción	Opción de tratamiento
Entre 5 y 10	Moderado	Se deben implementar los controles establecidos en la entidad y en lo posible tomarse las medidas necesarias complementarias a los controles para llevar los riesgos a la zona baja. **Riesgos tolerables, límite de la capacidad de riesgos definida por la UNAL.**	***Asumir*** (aceptar) con la implementación de los controles definidos. ***Reducir (mitigar)*** con más controles, planes de acción o actividades. ***Transferir***
Entre 11 y 30	Alto	Se deben tomar las medidas necesarias complementarias a los controles establecidos para llevar los riesgos al nivel "bajo" o "moderado". Se deben establecer los indicadores clave de riesgo (KRI's) y reportar a la instancia correspondiente. **Riesgos importantes por fuera de la capacidad de riesgos definida por la UNAL.**	***Opción de tratamiento*** ***- Reducir (mitigar)*** con más controles, planes de acción o actividades. ***- Transferir*** **Otras acciones obligatorias** *- Definir los KRI's.* *- Reportar a la instancia correspondiente (Segunda línea de defensa: responsable tipología de riesgos, Coordinación SIGA o ETIR).*
Entre 31 y 100	Extremo	Deben tomarse las medidas prioritarias necesarias, complementarias a los controles establecidos, a fin de disminuir el nivel de riesgo (medidas orientadas a reducir la probabilidad de ocurrencia, los impactos o eliminar la causa que genera el riesgo). Se deben establecer los indicadores clave de riesgo (KRI) y escalar a la instancia correspondiente. **Riesgos inaceptables por fuera de la capacidad de riesgos definida por la UNAL.**	***Opción de tratamiento*** ***- Reducir (mitigar)*** con más controles, planes de acción o actividades. ***- Transferir*** **Otras acciones obligatorias** *- Definir los KRI's.* *- Reportar a la instancia correspondiente (segunda línea de defensa: responsable tipología de riesgos, coordinación SIGA o ETIR).*
***Nota**: la opción de tratamiento "**Evitar**" está disponible para cualquier nivel de aceptabilidad, no se incluye en la columna 4 de tabla debido a que implica eliminar la actividad que genera el riesgo, siendo posible solo con el consenso y aprobación de las diferentes instancias de la UNAL implicadas, siempre y cuando la normatividad interna y externa aplicable lo permita.*			

2.4.5.1 Opciones de tratamiento del riesgo

Las opciones de tratamiento aplicables para un riesgo de cualquier tipología según su nivel de riesgo residual se muestran en la tabla 29.

Tabla 29 - Opciones de tratamiento para un riesgo de cualquier tipología

Opción	Descripción
Asumir (aceptar)	Implica aceptar el riesgo y las consecuencias que conlleve en caso de que llegue a materializarse. Generalmente, esta opción se toma cuando la probabilidad y el impacto no son altos y no se arriesga la estabilidad de la institución, o bien cuando el tratamiento es demasiado costoso y no representa un mayor beneficio. Esta opción también aplica para aquellos riesgos que, a pesar de haber implementado mecanismos de mitigación, no es posible reducir su nivel de riesgo residual al nivel de tolerancia (bajo o moderado) definido por la UNAL; ello acarrea un monitoreo más frecuente y exigente.
Reducir	Busca reducir la probabilidad de ocurrencia del riesgo o el impacto de su materialización, incluyendo más controles o diseñando y ejecutando planes de acción.

Opción	Descripción
Transferir (Compartir)	Trasladar a un tercero ajeno al proceso, estrategia, proyecto o sistema de gestión la administración del riesgo. Lo más usual es recurrir a la tercerización o la adquisición de pólizas o seguros.
Evitar	Usada cuando no se va a proceder con la actividad que tiene la posibilidad de generar el riesgo, al evitar el riesgo se puede: - Decidir no ejecutar la actividad que conlleva al riesgo. - Eliminar la actividad que conlleva al riesgo. - Sustituir la actividad que desencadena el riesgo por otra menos riesgosa. Esta opción de tratamiento puede implicar el diseño y la ejecución de planes de acción.

*Se debe **definir** para cada riesgo de cualquier tipología la **opción de tratamiento** a seguir con base en el **nivel de riesgos residual** determinado en la etapa de **Valoración del Riesgo**.*

2.4.5.2 Planes de acción

Los planes de acción son ***medidas de tratamiento complementarias a los controles*** que buscan ***conducir*** los riesgos al ***apetito*** (nivel "Bajo") o al umbral de ***tolerancia*** (nivel "Moderado") establecido por la UNAL, partiendo del ***nivel de riesgo residual*** obtenido en la etapa anterior de "Valoración del Riesgo" (véase el numeral 2.4.4).

Estas medidas de tratamiento deben centrarse en los riesgos, adaptarse a las necesidades y limitaciones de recursos de la Universidad y cumplir con las siguientes condiciones:

- Priorizarse dependiendo de cuáles tienen una mejor relación costo beneficio en el nivel institucional.
- Definir con claridad la(s) actividad(es) que conformarán el plan de acción.
- Designar a los funcionarios responsables de la implementación y el seguimiento de las actividades del plan de acción.
- Destinar los recursos necesarios para su desarrollo buscando minimizar los retrasos o incumplimientos.
- Definir las fechas para su ejecución.
- Establecer los resultados esperados para medir su eficacia y el grado en que el riesgo se modifica con su implementación.
- Cumplir con lo dispuesta por la Coordinación SIGA Nivel Nacional para la creación y la gestión de planes de acción.

Existen diversos ***tipos de planes de acción*** que pueden implementarse para 1. Reducir los riesgos residuales al apetito o tolerancia definidos por la UNAL; 2. Evitar los riesgos al no proceder con la actividad que lo genera; 3. Gestionar los riesgos materializados.

Tabla 30 - Tipos de planes de acción aplicables a cualquier tipología de riesgo

Tipo de plan	Descripción
Diseñar nuevo control	Conjunto de actividades planificadas y ejecutadas para obtener como resultado un nuevo control de probabilidad o impacto para el riesgo asociado. Se utilizan para los riesgos residuales con opción de tratamiento ***Reducir.***
Mejorar control	Conjunto de actividades planificadas y ejecutadas a fin de obtener como resultado la mejora/optimización de un control de probabilidad o impacto para el riesgo asociado. Se utilizan en los riesgos residuales con opción de tratamiento ***Reducir.***
Gestionar causas	Actividades planificadas y ejecutadas para combatir, reducir o eliminar la(s) causa(s) asociadas al riesgo. Se utilizan en los riesgos residuales con opción de tratamiento ***Reducir*** o ***Evitar.***
Gestionar riesgos materializados	Actividades planificadas y ejecutadas para: - disminuir los impactos de un evento materializado, o - volver a las condiciones normales luego de la materialización del riesgo (conocido como plan de contingencia o plan de recuperación de desastres), o - implementar mecanismos para evitar la repetición de un riesgo materializado.

- Se debe definir un **plan de acción** *para los* ***riesgos residuales "Extremos", "Altos" y "Moderados" (Opcional)*** *a los que se haya establecido como opción de tratamiento "****Reducir****".*

- Se debe definir un plan de acción para los riesgos que se hayan materializado.

- Aquellos riesgos residuales significativos posibles o materializados donde no haya sido posible definir un plan de acción deben ser escalados a la Coordinación SIGA o al ETIR, los cuales analizarán, tomarán acciones y establecerán el curso a seguir frente al riesgo; aquellos en los que no se pueda tomar ninguna acción, se deberán escalar y comunicar al Comité SIGA para su análisis y toma de decisiones correspondiente.

2.4.5.3 Indicadores clave de riesgo (KRI's)

Los ***Indicadores clave de riesgo (KRI's)*** —traducidos del inglés *Key Risk Indicators*— son ***métricas*** que se asignan a los riesgos con el fin de ***determinar cambios significativos*** y derivados de la aparición de sus causas o incrementos en el nivel de gravedad de sus consecuencias, con el fin de tomar las medidas o acciones oportunas. Los ***KRI's*** pueden entenderse como una especie de alarma, sensor o detector que se encarga de ***informar***, ***avisar*** o ***alertar*** cuando un riesgo no se está comportando o actuando como debería. Es importante en el momento de establecer los ***KRI's*** para los riesgos que se establezca su frecuencia y los estados (rangos) de medición que permitan determinar el nivel de alerta sobre el riesgo.

Adicional a la ***opción de tratamiento*** y la definición de ***planes de acción*** (si aplica), deberán ***establecerse*** y ***medirse KRI's*** para los ***riesgos residuales*** ubicados en los niveles de aceptabilidad "***Alto***" y "***Extremo***", teniendo en cuenta los ***atributos*** que se muestran en la tabla 31.

Tabla 31 - Atributos para definir un Indicador Clave de Riesgo

Atributo	Descripción
Nombre	Nombre asignado al indicador, debe ser conciso y orientado a medir la causa (Raíz y/o inmediata) o el impacto.
Descripción o fórmula (opcional)	Descripción del indicador relacionada con su uso u obtención. También hace alusión a la fórmula para la medición del indicador.
Frecuencia de medición	Establece cada cuanto se debe obtener el indicador y verificar su estado.
Estados de alerta	Indican los rangos - niveles de alerta del indicador con base a tres estados: - **Bueno (sin alerta)**: el indicador está en un rango tal que no implica una señal de alerta. - **Regular (en alerta):** el indicador está en un rango tal que requiere una revisión para definir si se deben emprender acciones para su seguimiento especial, disminución o retorno a los valores "sin alerta". - **Malo (alerta crítica):** el indicador está en un rango tal que requiere de manera prioritaria emprender acciones obligatorias para su disminución o retorno a la normalidad (sin alerta).
Resultado del indicador	Es el valor de la medición del indicador se obtiene con base en la frecuencia de medición establecida y la fórmula (opcional) para su obtención.

En la tabla 32 se presenta un ejemplo de KRI's.

Tabla 32 - Ejemplo de KRI's para un riesgo residual significativo

Riesgo	Nivel de riesgo residual y tratamiento	Indicador clave de riesgo (KRI's)	Frecuencia de medición	Resultado indicador	Estados de alerta			Acciones por realizar
					Bueno (sin alerta)	Regular (en alerta)	Malo (estado crítico)	
Insatisfacción de los estudiantes ocasionada por la exclusión de beneficios de matrícula, debido a las regulaciones y políticas del Ministerio de Educación Nacional referentes a la Política de	***25 – Alto*** ***Reducir***	Estudiantes excluidos del beneficio de matrícula de la política de gratuidad	Semestral	**47**	<= 50	51-150	>150	Ninguna
		Dineros asumidos por la UNAL por no pago del concepto de matrículas de estudiantes no beneficiados de la política de gratuidad	Semestral	**$21.013.000**	Menor o igual a $19.999.999	Entre $20.000.000 y $50.000.000	Mayor a $50.000.000	Requiere seguimiento más constante, o, acciones para retornar al estado Sin Alerta

Riesgo	Nivel de riesgo residual y tratamiento	Indicador clave de riesgo (KRI's)	Frecuencia de medición	Resultado indicador	Estados de alerta			Acciones por realizar
					Bueno (sin alerta)	Regular (en alerta)	Malo (estado crítico)	
Gratuidad en la Educación Superior		Tutelas y derechos de petición de estudiantes excluidos del beneficio de la política de gratuidad	Trimestral	**8**	<=3	entre 4 y 6	> 6	Requiere acciones prioritarias para su gestión o retornar al estado Sin Alerta

*- Se deben definir **KRI's** para los **riesgos** que presenten un **nivel de riesgo residual significativo** (Alto o extremo), siendo crucial garantizar su **medición** con base en la **frecuencia establecida.***

*- Cuando un **KRI's** presente un **estado de Alerta crítico** se deben emprender acciones prioritarias para su gestión con el fin de conducirlo a un estado Bueno (sin alerta).*

*Los responsables de la segunda línea de defensa de cada tipología deben facilitar e instruir en el uso de herramientas y métodos para definir: 1. La opción de tratamiento de un riesgo; 2. Planes de acción; 3. Los KRI's para los riesgos residuales en nivel Alto y Extremo, dando asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa en su gestión. Además, se debe llevar un registro y soporte de estos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios **De documentación y uso de sistemas de información para la administración de riesgos** del numeral **2.1.4.5** del presente documento.*

2.4.6 Seguimiento y revisión

La etapa de seguimiento y revisión consiste en un proceso sistemático de ***recolectar***, ***analizar*** y ***usar*** información, a fin de hacer una ***observación minuciosa*** del desarrollo de la gestión del riesgo, en el sentido que se cumplan los objetivos y se guíen las decisiones futuras. Se asemeja a tomar una ***fotografía*** (Perfil de riesgos) de la gestión del riesgo en el momento en el que se realiza la observación.

La ***gestión integral del riesgo*** implica que los eventos incluidos en los ***Mapas de riesgos*** deben ser gestionados a través del tiempo, al igual que los riesgos nuevos y emergentes, por medio de los mecanismos de control, los planes de acción, los KRI's y las opciones de tratamiento definidas para cada uno; es crucial una adecuada ***planificación y ejecución*** del seguimiento y la revisión.

El ***seguimiento y la revisión*****,** llevados a cabo por los integrantes de los procesos, de las estrategias, los proyectos y sistemas de gestión involucrados, de las diferentes tipologías que conforman el MIGR deben:

- Ser dirigidos por los responsables de la segunda línea de defensa de cada tipología.

- Ser ejecutados por la primera línea de defensa con el acompañamiento y asesoría de los responsables de la segunda línea de defensa de cada tipología.
- Contar con la participación de la Coordinación SIGA y el ETIR para el seguimiento de los riesgos altos y extremos posibles o materializados escalados por los responsables de la segunda línea de defensa de cada tipología.

2.4.6.1 Periodicidad del seguimiento y revisión

La ***periodicidad*** de las ***acciones de seguimiento y revisión*** para los riesgos incluidos en los mapas de calor de cada tipología se realizará tomando como referencia su ***nivel de riesgo residual***, tal como se aprecia en la tabla 33.

Tabla 33 - Periodicidad estimada de seguimiento según el nivel de riesgo residual

Tipo de riesgo	**Nivel de riesgo residual**			
	Bajo	**Moderado**	**Alto**	**Extremo**
Procesos – operativos y corrupción	Anual	Anual	Semestral	Cuatrimestral
Procesos - PAMEC	Anual	***Por definir***	***Por definir***	***Por definir***
Estratégicos	Anual	Anual	Semestral	Semestral
Proyectos	Anual	***Por definir***	***Por definir***	Trimestral/Bimestral
Ambientales	***Por definir***			Trimestral/Bimestral
Seguridad de la Información	***Por definir***			Trimestral/Bimestral
Seguridad y Salud en el Trabajo	Anual	Semestral	Mensual	Mensual
Fraude, LA, FT y FPADM	***Por definir***			Trimestral/Bimestral

El seguimiento y revisión de la ***Política integral de gestión del riesgo*** se realizará teniendo en cuenta los principios definidos en el numeral ***2.1.4.1 Para la definición, operación y seguimiento de la Política Integral de Gestión del Riesgo.***

Por otro lado, la Metodología integral de gestión del riesgo, la política integral de gestión del riesgo, el modelo de las tres líneas de defensa y, en general, el Presente MIGR, deben ser revisados y actualizados cada trienio o cuando se considere pertinente por la Coordinación SIGA Nivel Nacional y ETIR, y aprobado por el Comité SIGA[49], con el fin de garantizar:

- Los criterios para la calificación de los riesgos.
- La definición idónea del apetito, la tolerancia y la capacidad del riesgo.
- La periodicidad del seguimiento y la revisión.
- La forma como se mide la gestión del riesgo.
- La definición y los objetivos de la política integral de gestión del riesgo.
- Los roles y las responsabilidades frente a la gestión integral del riesgo.
- Entre otros.

[49] La Política Integral de Gestión del Riesgo debe ser aprobada por el CNCSCI.

El seguimiento y la revisión de los riesgos debe realizarse periódicamente según su nivel de riesgo residual.

2.4.6.2 Caducidad de los riesgos asumibles con nivel de riesgo residual "Bajo"

Considerando que uno de los objetivos de la gestión del riesgo es ***priorizar los eventos más significativos*** en pro de ***aprovechar y optimizar al máximo los recursos institucionales*** invertidos para su gestión, los ***riesgos que se mantengan en el nivel residual bajo por un tiempo definido*** y que cumplan con las siguientes ***condiciones*** podrán ser ***excluidos*** en la siguiente vigencia de los ***mapas de riesgos*** de cualquier tipología:

- Sin materializar durante el tiempo definido.
- Nivel de riesgo "bajo" y opción de tratamiento "asumir" durante el tiempo definido.
- Sin observaciones o hallazgos de entes de control en el tiempo definido.
- Controles eficientes y eficaces durante el tiempo definido.

En la tabla 34 se aprecia el ***tiempo definido*** para la ***exclusión*** de un ***riesgo asumible con nivel de riesgo residual "bajo"*** para las tipologías que componen el MIGR UNAL.

Tabla 34 - Tiempos definidos para la caducidad de riesgos asumibles con nivel de riesgo residual "Bajo"

Tipo de riesgo	**Tiendo definido para su caducidad** (Riesgo asumibles con nivel de riesgo residual bajo)
Procesos	Operativos y corrupción: cuatro a cinco años PAMEC: ***Por definir***
Estratégico	***Por definir***
Proyecto	Al finalizar el ciclo de vida del proyecto, aplica para cualquier nivel de riesgo residual.
Ambiental	***Por definir***
Seguridad Información	***Por definir***
Seguridad y Salud en el Trabajo	No aplica
Fraude, LA, FT y FPADM	***Por definir***

- Si un riesgo asumible excluido del mapa de riesgos se materializa en el futuro, este debe incluirse nuevamente en el mapa de riesgos de la tipología correspondiente.

- La exclusión de un riesgo del mapa correspondiente no implica que los controles definidos dejen de ejecutarse; estos deben mantener su operación dentro de los procesos, las estrategias, los proyectos y sistemas de gestión de la institución.

Los ejercicios de seguimiento y revisión dirigidos por los responsables de cada tipología de riesgos y ejecutado en mayor medida por los integrantes de la primera línea de defensa deben contener lo dispuesto en los numerales 2.4.6.3 a 2.4.6.11:

2.4.6.3 Actualización del contexto

Según el tipo de contexto (estratégico, sistema de gestión, proceso, proyecto, otros) de la tipología de riesgos, se debe contemplar en la planificación y ejecución de las acciones de seguimiento la actualización de los factores internos y externos de los riesgos incluidos en el Mapa de Calor ***(Véase el numeral 2.4.1 Establecimiento del contexto).***

2.4.6.4 Reporte y seguimiento de riesgos residuales significativos posibles o materializados

Para el caso de los riesgos residuales significativos posibles o materializados contenidos en los mapas de calor, como medida para su gestión y en pro de disminuir en lo posible las afectaciones drásticas /severas para los procesos, estrategias, proyectos, sistemas de gestión y, en general, para la institución, los actores de la primera línea de defensa o los responsables de la segunda línea de cada tipología deben implementar los lineamientos que se exponen en la ilustración 19 para su administración.

Ilustración 19 - Reporte y seguimiento de riesgos residuales significativos

1. **Reporte del riesgo residual significativo:** los actores de la primera línea de defensa custodios de los riesgos, deben ***reportar*** en los ***periodos de seguimiento y revisión*** aquellos por fuera de la ***capacidad de riesgo*** definida por la institución (***nivel de riesgo residual "Alto" y "Extremo"***) a los responsables de la segunda línea de defensa de cada tipología.

2. ○**Seguimiento periódico:** los actores de la primera línea de defensa y los responsables de la segunda línea de defensa de la tipología respectiva deben ***realizar el seguimiento y la revisión periódicos*** de los ***riesgos residuales significativos ("Alto" y "Extremo")*** según los lineamientos estipulados a lo largo de esta etapa del proceso para la gestión integral del riesgo.

3. ○**Escalamiento: l**os riesgos residuales significativos deberán ser comunicados por los responsables de la segunda línea de defensa de cada tipología a la Coordinación SIGA Nivel Nacional para su seguimiento periódico. Esta coordinación escalará al ETIR aquellos riesgos significativos que por diferentes situaciones requieran de su análisis experto para la toma de acciones y la definición del curso a seguir con miras a su mitigación; los riesgos donde el ETIR no pueda tomar ninguna acción ni establecer la ruta a seguir serán reportados al Comité SIGA para su toma de decisiones correspondiente.

Ilustración 20 - Reporte y seguimiento de riesgos mater

1. **Reportar y evaluar el impacto del riesgo materializado:** el responsable del riesgo de la primera línea de defensa ***reportará*** la materialización del riesgo apenas sea ***detectada*** al delegado de la segunda línea de defensa de la tipología respectiva si considera que esta tiene un ***impacto institucional o importante*** para el proceso, la estrategia, el proyecto o sistema de gestión. Por lo general, son ***riesgos residuales significativos*** los que tienen este tipo de afectación, pero pueden existir algunos dentro de la capacidad definida por la UNAL – nivel de riesgo residual bajo y moderado – que se materialicen y su impacto sea mucho mayor al esperado.

2. ○**Elaborar el plan para la gestión de riesgos materializados**: **e**l responsable de la segunda línea de defensa ***revisará*** la situación reportada validando la materialización del riesgo y la magnitud del impacto provocado; además, ***acompañará*** y ***asesorará*** al responsable de la primera línea de defensa en el establecimiento del ***plan para la gestión de riesgos materializados***. (***Véase el numeral 2.4.5.2 Planes de acción).***

3. ○**Ejecutar el plan de acción: e**l responsable del riesgo, junto con los actores involucrados, ***ejecutarán*** las actividades del ***plan de acción para la gestión de riesgos materializados*** en los tiempos planificados.

4. ○**Seguimiento del plan de acción:** el responsable del riesgo y los delegados de la segunda línea de defensa de la tipología asociada realizarán ***seguimiento*** al ***plan de acción para la gestión de riesgos materializados***, según los lineamientos estipulados a lo largo de esta etapa del proceso para la gestión integral del riesgo.

   Los responsable de la segunda línea de defensa informarán a la Coordinación SIGA sobre el riesgo materializado de alto impacto para su seguimiento periódico.

5. ○**Escalamiento y asesoría del riesgo materializado de alto impacto:** en caso de ser requerido y solicitado, la Coordinación SIGA acompañará y asesorará a los responsables de la primera y segunda línea de defensa en la gestión del riesgo materializado (pasos 1,2,3 y 4); esta coordinación escalará al ETIR aquellos riesgos materializados de alto impacto que por diferentes situaciones requieran de su análisis experto para la toma de acciones y la definición del curso a seguir para su mitigación, los riesgos donde el ETIR no pueda tomar ninguna acción ni establecer la ruta a seguir serán reportados al Comité SIGA para su toma de decisiones correspondiente.

ializados

2.4.6.5 Evaluación de controles

Se debe incluir en las actividades de seguimiento y revisión la ***evaluación de los atributos informativos, de eficiencia y eficacia de los controles*** asociados a los riesgos sujetos de valoración

que se hayan ejecutado en el periodo de seguimiento[50], con el fin de ***garantizar*** de una manera razonable el ***cumplimiento de su objetivo, la idoneidad de su diseño y una implementación eficaz***. ***(Véase el numeral 2.4.4 Evaluación del riesgo – Valoración del riesgo).***

2.4.6.6 Ejecución Seguimiento a planes de acción

Se debe realizar el ***reporte de la ejecución*** (Primera línea de defensa) y ***el seguimiento*** (Segunda línea de defensa) a los ***planes de acción*** véase el ***numeral 2.4.5.2 Planes de acción)***.

2.4.6.7 Seguimiento a los KRI's

Se debe incluir en las actividades de seguimiento y revisión la medición (Primera línea de defensa) y el monitoreo (Segunda línea de defensa) a los KRI's establecidos para los riesgos residuales significativos (Altos y Extremos) ***(Véase el numeral 2.4.5.3 Indicadores clave de riesgos KRI's).***

2.4.6.8 Actualización riesgos vigentes

Adicional a la actualización del contexto, la revisión de la materialización de riesgos, el seguimiento a los planes de acción y a los KRI's se debe incluir en las actividades de seguimiento y revisión de la actualización de la otra información resultante asociada a cada uno de los riesgos incluidos en el mapa de calor.

2.4.6.9 Gestión de nuevos riesgos y riesgos emergentes

Ante los ***cambios*** en los ***factores internos y externos*** del contexto de los procesos, las estrategias, los proyectos y sistemas de gestión de las múltiples tipologías de riesgo, es posible que surjan ***riesgos emergentes*** de causas de vigencias anteriores que se mantienen, o ***nuevos riesgos*** de las nuevas causas internas o externas; estos deben ser gestionados e incluidos en los mapas de riesgos correspondientes.

2.4.6.10 Análisis del perfil de riesgos

Se debe incluir en las actividades de esta etapa, partiendo de la información recolectada en el periodo de seguimiento y revisión vigente y de otros anteriores, la ***comprensión del perfil de riesgos*** de uno o más eventos de una o múltiples tipologías ***en al menos dos periodos de tiempo*** (el periodo de seguimiento vigente y el periodo de seguimiento anterior, y se puede extender a otros periodos anteriores) ***(Véase el numeral 2.4.4.5 Perfil de riesgos)***.

2.4.6.11 Indicadores y estadísticas

Para contribuir con la **medición *de los resultados de la gestión del riesgo*** se han establecido los siguientes ***indicadores*** y ***estadísticas*** que se deben obtener periódicamente por parte de los responsables de la segunda línea de defensa de cada tipología y por parte de la Coordinación SIGA[51]:

[50] Según la naturaleza del control, este puede actuar con cierta frecuencia para prevenir, detectar o corregir la causa o el impacto de los riesgos, por tanto, es posible que en algunos periodos de seguimiento el control no sea ejecutado.
[51] La Coordinación SIGA Nivel Nacional, partiendo de la información reportada de cada tipología, establecerá los indicadores globales de la gestión integral del riesgo para toda la institución.

Sigla	Nombre	Descripción	Fórmula
IVI	Índice de vulnerabilidad inherente (%)	Nivel de exposición de una tipología de riesgos frente a estos, sin tener en cuenta los mecanismos de control.	IVI(%) = Promedio NRI*/ 100***
IVR	Índice de vulnerabilidad residual (%)	Nivel de exposición de una tipología de riesgos frente a estos, teniendo en cuenta los mecanismos de control diseñados e implementados.	IVR(%) = Promedio NRR*/ 100***
IPDC	Índice promedio de eficiencia de los controles (%)	Media aritmética de la eficiencia (diseño) de los controles implementados en una tipología de riesgos.	IPDC(%) = Promedio % eficiencia de controles
IPIC	Índice promedio de eficacia de los controles (%)	Media aritmética de la eficacia de los controles implementados en una tipología de riesgos.	IPIC(%) = Promedio % eficacia de controles
IPEC	Índice promedio de efectividad de los controles (%)	Media aritmética de la efectividad (eficiencia + eficacia) de los controles existentes en una tipología de riesgos.	IPEC(%) = Promedio % efectividad de controles
COB	Cobertura de la gestión del riesgo (%)	Porcentaje de procesos, estrategias, proyectos, sistemas de gestión, …, que cuenta con matriz/listado de riesgos.	*COB*(%) = *Varia según la tipología de riesgo*
PCP	Promedio de controles por Riesgo (%)	Media aritmética de los controles por riesgo de una tipología.	PCP(%) = #Total Controles por riesgo/#Total de riesgos
NRM	Nivel de riesgos materializados (%)	Razón expresada en forma porcentual entre los riesgos materializados y el total de riesgos de una tipología.	NRM(%) = #Total riesgos materializados/#Total de riesgos
NCP	Nivel de controles preventivos (%)	Razón expresada en forma porcentual entre el total de controles preventivos y el total de controles de una tipología.	NCP(%) = #Total controles preventivos/#Total de controles
NCP	Nivel de controles automáticos (%)	Razón expresada en forma porcentual entre el total de controles automáticos y el total de controles de la tipología.	NCP(%) = #Total controles automáticos/#Total de controles
NRIS	Nivel de riesgos inherentes significativos (%)	Razón expresada en forma porcentual entre el total de riesgos inherentes ubicados en zona alta-extrema y el total de riesgos de una tipología.	NRIS(%) = #Total Riesgos inherentes significativos/#Total de riesgos
NRRS	Nivel de riesgos residuales significativos (%)	Razón expresada en forma porcentual entre el total de riesgos residuales ubicados en zona alta-extrema y el total de riesgos de una tipología.	NRRS(%) = #Total Riesgos residuales significativos/#Total de riesgos
PRT	Participación de los riesgos de una tipología específica (%)	Razón expresada en forma porcentual entre el total de riesgos de una tipología y el total de riesgos de la UNAL.	NRT(%) = #Total Riesgos de una tipología/#Total de riesgos UNAL

*NRI: Nivel de riesgo inherente, es el valor obtenido al multiplicar la probabilidad y el impacto inherentes asignados al riesgo en la etapa de "Análisis del riesgo".
**NRR: Nivel de riesgo residual, es el valor obtenido al multiplicar la probabilidad y el impacto residuales (luego de aplicar controles) en la etapa de "Evaluación del riesgo".
*** 100 hace referencia al Máximo valor posible de multiplicar el nivel de probabilidad (5 – Casi seguro) por el nivel de impacto (20 - Catastrófico).
Nota: *La fórmula de cada indicador /estadística se puede utilizar para una o más tipologías de riesgos, uno o varios mapas de riesgos, y para obtener el valor global (institucional, partiendo de la información suministrada de cada tipología de riesgo)*.

- Los indicadores y las estadísticas deben ser calculados en cada periodo de seguimiento y revisión por parte de los responsables de la segunda línea de defensa de cada tipología y la Coordinación SIGA Nivel Nacional.

- Los indicadores y las estadísticas pueden ser obtenidos en una o más tipologías de riesgos, uno o varios mapas de riesgos, y para calcular su valor global para la UNAL.

Los responsables de la segunda línea de defensa de cada tipología y la Coordinación SIGA Nivel Nacional deben facilitar e instruir en el uso de herramientas y métodos para definir: 1. La periodicidad del seguimiento y revisión; 2. La caducidad de los riesgos asumibles; 3. La actualización del contexto; 4. El reporte de riesgos residuales significativos y la gestión de riesgos materializados; 5. La revisión de los controles; 6. El seguimiento a los planes de acción y los KRI's; 7. La actualización de los riesgos vigentes y la gestión de los nuevos riesgos y los riesgos emergentes; y 8. La comprensión del perfil de riesgos, al brindar asesoría, acompañamiento y seguimiento a los responsables de la primera línea de defensa y otros actores involucrados en su gestión. Además, se debe llevar un registro y soporte de estos vigencia tras vigencia, cumpliendo siempre con lo estipulado en los principios ***De documentación y uso de sistemas de información para la administración de riesgos*** *del numeral* ***2.1.4.5*** *del presente documento.*

2.4.7 Comunicación y consulta

El objetivo de esta etapa es el ***intercambio de información y la comprensión de la gestión por los Grupos de interés,*** lo que conllevará a la ***toma de decisiones sobre la base de una información confiable y consistente.***

La ***comunicación*** busca promover la ***toma de conciencia*** y la ***comprensión del riesgo***; la ***consulta*** implica ***obtener retroalimentación e información*** para apoyar la ***toma de decisiones*** frente a la gestión integral y particular del riesgo. Esta etapa es ***permanente*** y se debe desarrollar de manera ***participativa*** en todas y cada una de las ***etapas del proceso para la gestión del riesgo*** descritas en el presente documento.

Para el desarrollo de esta etapa se pueden utilizar diferentes estrategias y herramientas, como lo son el diseño y la ejecución de planes de comunicación, la comunicación por medios oficiales y electrónicos, reuniones virtuales o presenciales y espacios de trabajo colaborativo, entre otros.

El correcto desarrollo de esta etapa permitirá:

- Identificar y redactar correctamente los riesgos.
- Valorarlos en función de las consecuencias para la Universidad y la probabilidad de ocurrencia, bajo criterios estándar.
- Comprender su probabilidad e impacto.
- Fijar prioridades para su tratamiento.
- Informar y contribuir a que se involucren los Grupos de interés.
- Monitorear la eficacia de las medidas de tratamiento.

- Revisar con regularidad la metodología de gestión integral del riesgo para detectar oportunidades de mejora.
- Fomentar en la Institución la adopción del pensamiento basado en riesgos.
- Promover la cultura integral de gestión del riesgo.

*La **comunicación y la consulta** son **permanentes** y se deben desarrollar de manera **participativa** en todas y cada una de las **etapas del proceso** para la gestión del riesgo.*

2.4.8 Registro e informe

Esta etapa tiene como principales objetivos ***comunicar las actividades de gestión del riesgo y sus resultados*** a lo largo de la UNAL, ***proporcionar información para la toma de decisiones*** estratégicas y operativas, así como ***asistir la interacción con los Grupos de interés,*** principalmente con aquellos que tienen la responsabilidad de rendir cuentas de las actividades de gestión del riesgo (estipuladas en el Modelo de las tres líneas de defensa, numeral 2.3).

Entendiendo que esta etapa busca presentar los resultados de la gestión integral del riesgo ante las instancias correspondientes para la toma de decisiones, es crucial la **difusión de los informes** a: la Alta Dirección, representada por el Comité SIGA, el ETIR, la Coordinación SIGA Nivel Nacional, los entes de control interno y externo y los líderes o coordinadores de los procesos, las estrategias, los proyectos y sistemas de gestión de la institución, entre otros.

Los ***informes generales y particulares*** resultantes de la gestión de riesgos realizada por cada una de las tipologías que componen el MIGR y otros actores transversales, junto con su periodicidad y las instancias que los elaboran y reciben se presentan en la tabla 35.

Tabla 35 – Periodicidad de los informes de gestión del riesgo

Tipo	Informe	Instancia(s) que elabora(n)	Instancia(s) que recibe(n)	Periodicidad
Institucional - general	Informe institucional de Gestión integral del riesgo (Insumo: informes de cada tipología de riesgos del MIGR UNAL)	Coordinación SIGA Nivel Nacional	Comité SIGA, ETIR, responsables de la segunda línea de defensa de cada tipología, ONCI	Anual
Institucional – general	Informe de seguimiento a la Política Integral de Gestión del Riesgo	Coordinación SIGA Nivel Nacional	ETIR, Comité SIGA, responsables de la segunda línea de defensa de cada tipología, ONCI	Semestral/Anual
Proceso	Informe de Gestión de riesgos de corrupción	Coordinadores del SGC Nivel Nacional y Sedes	ETIR, Coordinación SIGA NN, Coordinadores del SGC de sede, Líderes de los procesos, ONCI	Semestral
	Informe de Gestión de riesgos operativos-PAMEC	Coordinadores del SGC nivel nacional y sedes	ETIR, Coordinación SIGA NN, Coordinadores del SGC de sede, Líderes de los procesos, ONCI	Anual
Estratégico	Informe de gestión de riesgos estratégicos	DNPE, Oficinas de Planeación y estadística de sede	ETIR, Coordinación SIGA NN, Oficinas de planeación y estadística de sede, Alta Dirección, ONCI, Líderes de estrategias, Comité Nacional de Planeación Estratégica	Anual

Tipo	Informe	Instancia(s) que elabora(n)	Instancia(s) que recibe(n)	Periodicidad
Proyecto	Informe de Gestión de riesgos de proyectos de inversión	DNPE, Oficinas de Planeación y estadística de sede	Líderes de los proyectos de inversión, Oficinas de Planeación y Estadística de sede	Anual ***(Por validar y aprobar)***
	Informe de Gestión de riesgos de proyectos de extensión	DNEIPI ***(Por validar y aprobar)***	Líderes de los proyectos de extensión, Comité Nacional de Extensión o QHSV	Anual ***(Por validar y aprobar)***
	Informe de Gestión de riesgos de proyectos de investigación	DNIL ***(Por validar y aprobar)***	Líderes de los proyectos de investigación, Comité Nacional de Investigación o QHSV	Anual ***(Por validar y aprobar)***
	Informe de Gestión de riesgos de proyectos de regalías	VRI, DNPE ***(Por validar y aprobar)***	Líderes de los proyectos de regalías, Comité Directivo VRI o QHSV, Comité Nacional de Planeación Estratégica	Anual ***(Por validar y aprobar)***
	Informe consolidado de gestión de riesgos de proyectos (Insumo: informes de cada tipo de proyectos)	***Por definir***	ETIR, Coordinación SIGA NN, responsables de la segunda línea de defensa de cada tipo de proyecto, ONCI	Anual ***(Por validar y aprobar)***
Ambiental	***Por definir***	***Por definir***	ETIR, Coordinación SIGA NN, ***Otros por definir***	***Por definir***
Seguridad información	***Por definir***	***Por definir***	ETIR, Coordinación SIGA NN, ***Otros por definir***	***Por definir***
Seguridad y salud trabajo	Revisión por la Alta dirección, autoevaluación e indicadores SST	Reas de SST	ETIR, Coordinación SIGA NN, Vicerrectorías de sede, Direcciones de sede	Mensual y Anual
Fraude, LA, FT y FPADM	***Por definir***	***Por definir***	ETIR, Coordinación SIGA NN, ***Otros por definir***	***Por definir***
Nota: *Los entes de control interno (ONCI) y externo, así como otros entes gubernamentales podrán solicitar estos informes en cualquier momento que sea pertinente a los encargados de su elaboración.*				

Los **informes de gestión del riesgo** *son una parte crucial para la gobernanza de la UNAL, ayudan a mejorar la calidad del diálogo con los actores involucrados y son un insumo crucial para el Comité SIGA, el ETIR y la Coordinación SIGA Nivel Nacional en el cumplimiento de sus responsabilidades frente al MIGR.*

2.4.9 Ejemplo de riesgo aplicando la metodología para la gestión integral de riesgos

A fin de facilitar el entendimiento de la Metodología para la gestión integral de riesgos[52] se ha elaborado un ejemplo con un riesgo de prueba que contiene los campos con la información resultante de la implementación de las pautas metodológicas contenidas en dicho proceso53.

[52] Basada en las etapas del proceso para la gestión del riesgo de la NTC ISO 31000:2018
[53] Aclaraciones:

Los campos (columnas) del ejemplo son los mínimos que debe contener un riesgo de cualquier tipología contenida en el MIGR, sin incluir los campos correspondientes a la etapa seguimiento y revisión.

- La información del riesgo relacionada se proporción a manera de ejemplo y fue elaborada a partir de supuestos que disciernen de la realidad institucional.
- Las etapas incluidas en el ejemplo son: Identificación del riesgo, análisis del riesgo, valoración del riesgo y tratamiento del riesgo.
- No se incluirán para el riesgo de ejemplo información relacionada de las etapas de "Establecimiento del Contexto" y "Seguimiento y Revisión".
- Las etapas de "Comunicación y consulta" y "Registro e informe" no generan información trascendental para incluir en el riesgo de ejemplo.

Tabla 36 - Ejemplo de riesgo aplicando la metodología integral de gestión del riesgo UNAL

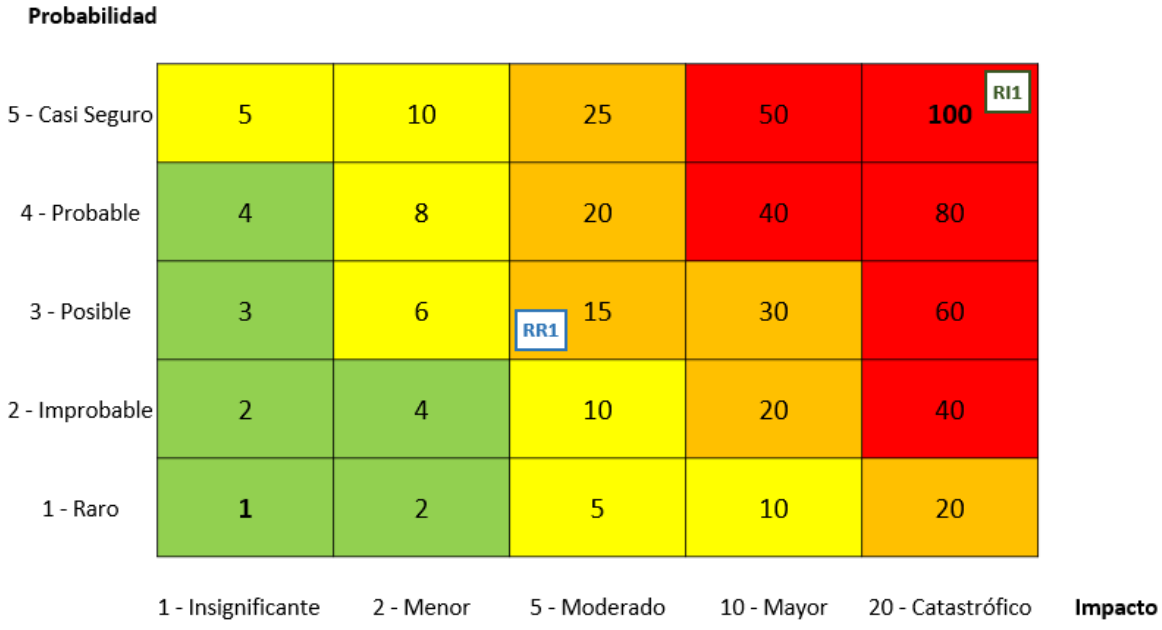
I. Etapa "Identificación del riesgo"							II. Etapa "Análisis del riesgo"		
Código	**Redacción del riesgo**				**Responsable**	**Estado del riesgo**	**Perfil de riesgo inherente**		
	Frase inicial	**Impacto (¿Qué?)**	**Causa inmediata (¿Cómo?)**	**Causa raíz (¿Por qué?)**			**Nivel probabilidad**	**Nivel impacto**	**Nivel de RI (aceptabilidad)**
RE-013	Posible	Insatisfacción de los estudiantes	ocasionada por la exclusión de descuentos de matrícula provenientes del Fondo Solidario para la Educación	por debilidades al implementar las regulaciones y políticas del Ministerio de Educación Nacional referentes a la Política de Gratuidad en la educación superior al interior de la UNAL	Líder de la Política de gratuidad en el interior de la UNAL	Materializado	5 - Casi Seguro	20 - Catastrófico	100 - Extremo

III. "Etapa Evaluación del riesgo - Identificación del control"												
Riesgo	**Atributos informativos del control**											
	Código	**Nombre**	**Responsable**	**Objetivo**	**Descripción**	**Frecuencia de ejecución**	**Fecha evaluación**	**Causa/impacto (que combate)**	**Variable que reduce**	**Documentado**	**Tipo evidencia**	**Desviaciones**
Insatisfacción de los estudiantes ocasionada por la exclusión de descuentos de matrícula provenientes del Fondo solidario para la Educación, por debilidades al implementar las regulaciones y lineamientos del Ministerio de Educación Nacional referentes a la Política de Gratuidad al interior de la UNAL	CRE-04	Adopción del reglamento operativo para la aplicación de la política de gratuidad	Direcciones de bienestar, Oficinas de Registro, VRA, GNFA, Rectoría	Incorporar en la dinámica institucional los lineamientos de la Política de gratuidad	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*	Permanente	01/10/2022	**Causa Raíz:** debilidad en la incorporación de la política de gratuidad	Probabilidad	Si, en el reglamento operativo del MEN	Soportes de la ejecución del procedimiento U.PR.018 implementación de la …	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*
	CRE-05	Verificar la información de los estudiantes marcados y no marcados en la certificación inicial ajustada	DINARA, Secciones de tesorería, DNB	Validar y cruzar en los sistemas de información académica, financieros y de entes externos (Icetex), la información de los estudiantes marcado y no marcados en la Certificación Inicial Ajustada	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*	Periódico - Semestral	03/10/2022	**Causa inmediata:** exclusión de descuentos de matrícula a estudiantes beneficiados de la Política de gratuidad	Probabilidad	NO	Documental, Certificación inicial ajustada y reportes de sistemas de información usados para obtenerla	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*
	CRE-06	Implementación del mecanismo para la atención de reclamos de estudiantes sobre Política de gratuidad	Sistema Aranda de PQR's, Funcionarios designados	Implementar el mecanismo desarrollado en el sistema Aranda para gestionar de manera prioritaria las solicitudes estudiantiles relacionadas con exclusiones u otros de la Política de gratuidad	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*	Por evento	05/10/2022	Impacto: Insatisfacción de los estudiantes de pregrado	Impacto	Si, en el manual del sistema Aranda	Registros en el sistema de información Aranda	*Contenido muy extenso para la celda, sin definir por fines ilustrativos*

Riesgo	III. "Etapa Evaluación del riesgo Parte - evaluación del control y nivel de riesgo residual"																
	Atributos de eficiencia del control							Atributos de eficacia del control					% Efectividad	Perfil de riesgo residual			
	Código	Naturaleza del control	Nivel Automatización	Cobertura	Nivel de Periodicidad de ejecución	Madurez del control	% Eficiencia	Cumplimiento objetivo	Complejidad	Pertinencia de ejecución	Evidencia de la ejecución del control	% Eficacia		Probabilidad residual	Impacto residual	Nivel de RR	Riesgo significativo (S/N)
Insatisfacción de los estudiantes ocasionada por la exclusión de descuentos de matrícula provenientes del Fondo solidario para la Educación, por debilidades al implementar las regulaciones y lineamientos del Ministerio de Educación Nacional referentes a la Política de Gratuidad al interior de la UNAL	CRE-04	Preventivo (25 %)	Manual (5%)	Total (25 %)	Optimo(15%)	Definido y documentado (10 %)	70% - Medio	Bajo (0 %)	Complejo (5 %)	No pertinente (0 %)	Evidencia suficiente (30 %)	35 % - Bajo	47 % - Baja	4 - Probable	20 - Catastrófico	80 - Extremo	Si, es Significativo *Riesgo **residual "15 Alto"***
	CRE-05	Detectivo (20 %)	Semiautomático (7 %)	Parcial (15 %)	Malo (5 %)	Definido, Documentado, implementado (15 %)	62 % - Medio	Medio (20 %)	Complejo (5 %)	Pertinente (20 %)	Evidencia suficiente (30 %)	75 % - Medio	70 % - Medio	3- Posible	20 - Catastrófico	60 - Extremo	
	CRE-06	Correctivo (15 %)	Automático (10 %)	Total (25 %)	Bueno (10 %)	Definido, documentado, implementado y socializado (20 %)	80 % - Alto	Alto (35 %)	Complejo (5 %)	Pertinente (20 %)	Evidencia suficiente (30 %)	90 % - Alto	87 % - Alto	3- Posible	5 - Moderado	15 - Alto ***(Riesgo residual)***	

Riesgo	IV. "Etapa Tratamiento del riesgo e Indicadores clave de riesgo KRI's"															
	Opción de tratamiento	Datos del plan de acción								Datos del KRI's			Estados de alerta de los KRI's			Acciones por realizar al indicador
		Tipo Plan	Actividad	Responsable	Fecha inicio	Fecha Fin	Entregable	Costo estimado	Verificación de la eficacia del plan	Indicador clave de riesgo (KRI's)	Frecuencia de medición	Resultado indicador	Bueno (sin alerta)	Regular (en alerta)	Malo (estado crítico)	
Insatisfacción de los estudiantes ocasionada por la exclusión de descuentos de matrícula provenientes del Fondo solidario para la Educación, por debilidades al implementar las regulaciones y lineamientos del Ministerio de Educación Nacional referentes a la Política de Gratuidad al interior de la UNAL	Reducir	Mejorar control	Revisar y actualizar el procedimiento U.PR.018 con base al reglamento operativo de la Política de gratuidad emitido por el MEN para el semestre 2023-1	VRA, Oficinas de Registro, Secciones de Tesorería, Direcciones de Bienestar, GNFA	01/01/2023	30/01/2023	Procedimiento U.PR.018 actualizado en una nueva versión	150 horas	Se verificará a inicios del mes de agosto de 2023	Estudiantes excluidos del beneficio de matrícula de la política de gratuidad	Semestral	47	<= 50	51-150	>150	Ninguna
			Socializar y aprobar el procedimiento actualizado	VRA, DNB, GNFA	01/02/2023	15/02/2023	Listas de asistencia, grabaciones, presentaciones, comunicaciones	20 horas		Dineros asumidos por la UNAL por no pago del concepto de matrículas de estudiantes no beneficiados de la política de gratuidad	Semestral	$21.013.000	Menor o igual a $19.999.999	Entre $20.000.000 y $50.000.000	Mayor a $50.000.000	Requiere seguimiento más constante, o acciones para retornar al estado Sin Alerta
			Realizar seguimiento a la implementación del procedimiento actualizado con el fin de encontrar y corregir debilidades	VRA, DNB, GNFA	01/03/2023	30/07/2023	Informe con los resultados del seguimiento	30 horas		Tutelas y derechos de petición de estudiantes excluidos del beneficio de la política de gratuidad	semestral	8	<=3	entre 4 y 6	> 6	Requiere acciones prioritarias para su gestión o retornar al estado Sin Alerta

Ilustración 21 Ubicación en el Mapa de Calor (perfil de riesgo) del riesgo de ejemplo



Nivel de riesgo inherente			
	Probabilidad	**Impacto**	**Nivel RI**
RI1	5 – Casi seguro	20 - Catastrófico	100 - Extremo

Nivel de riesgo residual			
	Probabilidad	**Impacto**	**Nivel RR**
RR1	3 - Posible	5 - Moderado	15- Alto

3 ESTRATEGIA: ADOPCIÓN E IMPLEMENTACIÓN DEL MIGR UNAL

Posterior a la aprobación del presente documento, se ha propuesto la siguiente estrategia para implementarlo en los procesos, los proyectos, las estrategias y los sistemas de gestión de la institución en los que se administran las tipologías de riesgos contenidas en el MIGR (en lo restante del trienio 2022-2024[54]).

Tabla 37 - Estrategia para la adopción e implementación del MIGR UNAL trienio 2022-2024.

Parte	Nombre	Descripción	Duración estimada
I	Prueba piloto del MIGR en el proceso "Mejoramiento de la Gestión"	La Coordinación SIGA Nivel Nacional, de la mano de los integrantes del proceso estratégico "Mejoramiento de la Gestión", realizarán una prueba piloto para la implementación de la Metodología integral de gestión del riesgo contenida en el MIGR (véase numeral 2.4), con el fin de detectar mejoras y retroalimentar las pautas metodológicas propuestas.	2 a 3 meses
II	Implementación del MIGR en los riesgos de procesos	Se iniciará la implementación del MIGR en la gestión de riesgos de procesos operativos, corrupción y PAMEC a cargo del Sistema de Gestión de Calidad. Para ello la Coordinación SIGA capacitará, asesorará y acompañará a los Coordinadores de Calidad de las sedes integrantes de la segunda línea de defensa que participarán, junto con los líderes e integrantes de los procesos de la UNAL (primera Línea de defensa), en la incorporación del MIGR en la administración de sus riesgos.	12 a 18 meses
III	Conformación del ETIR	La alta dirección representada por la Comité SIGA, de la mano de los responsables de las tipologías de riesgos, definirá, estructurará, asignará recursos y seleccionará a los funcionarios que conformarán el Equipo Técnico Integral de Riesgos.	12 meses
IV	Retroalimentación e implementación del MIGR en los riesgos estratégicos y de proyectos	La Coordinación SIGA retroalimentará con los responsables de la segunda línea de defensa de los riesgos estratégicos y de proyectos el MIGR en lo que concierna a estas tipologías. Posteriormente, con los actores involucrados de la primera línea de defensa iniciarán la implementación de la Metodología Integral de gestión del riesgo (véase el numeral 2.4).	18 a 24 meses
V	Definición/retroalimentación e implementación del MIGR en los riesgos asociados a los sistemas de gestión y otros:	La Coordinación SIGA definirá o retroalimentará (según el estado de la tipología de riesgos) con los responsables de la segunda línea de defensa de los riesgos ambientales, de seguridad de la información, de seguridad y salud en el trabajo, de fraude, lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva el MIGR en lo que concierna a estas tipologías. Posteriormente, con los actores involucrados de la primera línea de defensa, iniciarán la implementación de la Metodología integral de gestión del riesgo (véase el numeral 2.4)	18 a 24 meses

[54] La adopción y retroalimentación del MIGR para algunas tipologías puede extenderse a trienios posteriores.

Parte	Nombre	Descripción	Duración estimada
VI	Informe: retroalimentación e implementación del MIGR.	La Coordinación SIGA Nivel Nacional elaborará un informe con el resultado de la retroalimentación e implementación del MIGR durante el trienio 2022-2024; este será revisado por el ETIR, el cual compartirá los resultados con el Comité SIGA para la toma de decisiones correspondiente.	2 a 3 meses *(primeros meses del año 2025)*

Notas:

- Después de la finalización de la prueba piloto del MIGR se pueden ejecutar de forma simultánea: 1. La implementación del MIGR en los riesgos de procesos; 2. La retroalimentación e implementación en los riesgos estratégicos, de proyectos, de los sistemas de gestión y otros; 3. La conformación del ETIR.
- La responsabilidad de implementar la metodología integral de gestión del riesgo reposará sobre los encargados de las tipologías de la segunda línea de defensa y los actores involucrados de la primera línea de defensa. La coordinación SIGA Nivel Nacional brindará asesoría a estos para su correcta adopción.
- Considerando los recursos limitados y la capacidad estratégica y operativa de la UNAL frente a la gestión del riesgo, los tiempos estimados para las acciones que componen la estrategia de adopción e implementación del MIGR pueden extenderse.

CONTROL DE CAMBIOS

- **Elaboración Versión 0:**

Elaboró:	Daniel Soto Restrepo.	Revisó:	Gloria Inés Cardona Giraldo.	Aprobó:	Integrantes Comité SIGA.
Cargo:	Contratista VRG – Profesional especializado.	Cargo:	Asesora VRG.	Cargo:	N/A
Fecha:	02/03/2023	Fecha:	03/03/2023	Fecha:	06/03/2023