UNIVERSIDAD MILITAR NUEVA GRANADA

SISTEMA INTEGRADO DE GESTIÓN	Número de Páginas: **97**	Revisión N° **1**
Nombre: **MANUAL DE GESTIÓN DE RIESGOS Y OPORTUNIDADES PARA EL SISTEMA INTEGRADO DE GESTIÓN**		

Elaborado por:	**Revisado por:**	**Aprobado por:**
Dr. José William Castro Salgado Jefe Oficina Asesora de Planeación Estratégica	Dr. José William Castro Salgado Jefe Oficina Asesora de Planeación Estratégica	M.G (R) Javier Alberto Ayala Rector UMNG

Manual de Gestión de Riesgos y Oportunidades para el Sistema Integrado de Gestión

Control de Cambios

Razones del Cambio	Cambio a la Revisión #	Fecha de emisión
• Se crea manual. • Se verifica el numeral 2.4.2.2.4 Riesgos de Corrupción en Procesos Institucionales.	1	2025/08/11

INDICE

Manual de Gestión de Riesgos y Oportunidades para el Sistema Integrado de Gestión

1. GENERALIDADES

1.1. Introducción

La Universidad Militar Nueva Granada (UMNG), en cumplimiento de sus funciones misionales y del marco normativo interno y externo que la rige, ha adoptado un enfoque integral de gestión del riesgo como componente esencial de su modelo de gobernanza y sostenibilidad institucional. Este enfoque busca anticipar, prevenir y mitigar eventos adversos que puedan afectar el logro de sus objetivos estratégicos, la ejecución de proyectos de inversión, el cumplimiento normativo, la estabilidad financiera y la reputación organizacional.

El propósito de la gestión del riesgo en la UMNG es administrar la incertidumbre de forma sistemática, estructurada y proactiva, reduciendo tanto la probabilidad de ocurrencia de riesgos como el impacto de sus consecuencias. Esta gestión trasciende el cumplimiento normativo y las exigencias de auditoría, constituyéndose en una herramienta que agrega valor a la toma de decisiones basada en evidencia, fortalece la eficiencia operativa, protege los recursos institucionales y refuerza la transparencia y la rendición de cuentas en la gestión pública.

En línea con los principios de la norma ISO 31000:2018 y la Guía para la Administración del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública – DAFP (versión 2022), la Universidad Militar Nueva Granada (UMNG) ha adoptado un modelo de gestión del riesgo integral, flexible y contextualizado, que responde a las exigencias propias de su misión educativa, investigativa, territorial y administrativa.

La ISO 31000:2018 se asume como el marco de referencia base para la gestión del riesgo institucional, dado que proporciona principios y directrices internacionalmente aceptados para la identificación, análisis, tratamiento y monitoreo de riesgos. Esta norma no es certificable, pero se considera una guía estructural para construir un enfoque sistemático, proactivo y transversal de gestión del riesgo.

Por su parte, la Guía del DAFP (versión 2022) representa el referente normativo y metodológico obligatorio en el ámbito del sector público colombiano. La UMNG ha adoptado de forma integral sus lineamientos metodológicos, especialmente en lo relacionado con las etapas del ciclo de gestión del riesgo (establecimiento del contexto, identificación, análisis, valoración, tratamiento, monitoreo y revisión), así como en la tipificación y clasificación de los riesgos institucionales.

No obstante, la implementación de estos estándares ha sido ajustada y fortalecida con componentes específicos que responden a las particularidades institucionales de la Universidad. Entre las principales adaptaciones realizadas se destacan:

- La incorporación de riesgos académicos y de investigación, dada la naturaleza universitaria de la entidad.
- El enfoque en riesgos estratégicos y territoriales, derivados de su cobertura nacional y proyección en entornos diferenciados.
- La creación de categorías de riesgo complementarias, como los riesgos de corrupción articulados al Programa de Transparencia y Ética Pública, y los riesgos asociados a procesos de acreditación y aseguramiento de la calidad.

- La integración con otros sistemas de gestión basados en normas ISO certificables (ISO 9001, ISO 14001, ISO 45001, ISO 27001, entre otras), permitiendo una visión articulada del riesgo en los ámbitos de calidad, ambiente, seguridad laboral y seguridad de la información.

Este enfoque combinado permite que la gestión del riesgo en la UMNG no solo cumpla con los requisitos legales y técnicos del orden nacional, sino que también esté alineada con las mejores prácticas internacionales, garantizando una gobernanza institucional más eficaz, anticipativa y resiliente.

Este modelo contempla, además, mecanismos permanentes de monitoreo, seguimiento y mejora continua, orientados a evaluar la eficacia de los controles, la ejecución de planes de mejora y el comportamiento de los riesgos residuales. Estos mecanismos permiten retroalimentar el proceso de gestión de riesgos y ajustar las estrategias conforme a los resultados obtenidos.

La gestión del riesgo en la UMNG abarca el análisis y control de múltiples categorías, incluyendo:

- **Riesgos Fiscales:** Son situaciones que pueden causar pérdidas de recursos públicos por errores, negligencias o decisiones inadecuadas en la gestión institucional. Se presentan cuando no se protege adecuadamente el patrimonio del Estado y pueden generar sanciones o responsabilidades fiscales.
- **Riesgos Estratégicos:** Amenazas que pueden afectar la misión, visión y objetivos institucionales establecidos en el Plan de Desarrollo Institucional (PDI).
- **Riesgos de Corrupción, Fraude:** Factores que comprometen la transparencia y la ética pública, asociados a posibles irregularidades en la gestión de recursos y la contratación pública.
- **Riesgos de Seguridad de la Información:** Amenazas a la confidencialidad, integridad y disponibilidad de la información institucional y los activos tecnológicos.
- **Riesgos Operativos:** Los riesgos de operativos comprenden aquellos eventos que pueden afectar negativamente la ejecución regular de las actividades desarrolladas por las diferentes dependencias académicas, administrativas y operativas de la Universidad. Estos riesgos pueden tener origen interno o externo y comprometer la eficacia, eficiencia y cumplimiento de los objetivos institucionales.

A continuación, se describen las principales categorías que hacen parte de los riesgos operativos:

- ✓ **Riesgos en Seguridad y Salud en el Trabajo (SST):** Condiciones físicas, organizacionales o de comportamiento que pueden afectar la integridad, salud o bienestar del talento humano vinculado a la Universidad.

- ✓ **Riesgos de Sostenibilidad:** Factores que pueden generar impactos negativos en el ambiente o en el cumplimiento de normativas ambientales, tecnológicas y financieras, comprometiendo la sostenibilidad institucional.

- ✓ **Riesgos Financieros y Contables:** Situaciones que ponen en riesgo la estabilidad financiera, la liquidez o el cumplimiento de principios contables, afectando la sostenibilidad económica de la Universidad.

- ✓ **Riesgos de Daño Antijurídico:** Posibilidad de que se generen obligaciones legales o sanciones por acciones u omisiones institucionales, derivadas del incumplimiento normativo o de litigios.

- ✓ **Riesgos en Proyectos de Investigación e Innovación:** Condiciones que pueden obstaculizar el desarrollo, financiación o continuidad de proyectos académicos, científicos o tecnológicos.

- ✓ **Riesgos del Plan de Desarrollo Institucional:** Factores que pueden comprometer el cumplimiento de los objetivos, metas y estrategias establecidos en los planes de largo plazo de la Universidad.

- ✓ **Riesgos del Plan Estratégico de Seguridad Vial:** Amenazas relacionadas con la seguridad vial dentro del entorno universitario, tales como conductas imprudentes, fallas en infraestructura o vehículos, y el incumplimiento de normas. Su adecuada gestión busca prevenir accidentes y proteger la vida e integridad de la comunidad universitaria.

La UMNG adopta un enfoque integral y preventivo, alineado con parámetros de la ISO 31000, la Guía DAFP 2022 y los lineamientos internacionales de gestión del riesgo, asegurando que todas las áreas de la Universidad participen activamente en la identificación y mitigación de riesgos.

Este Marco Integral para la Gestión del Riesgo representa un compromiso institucional con la seguridad, la eficiencia y la sostenibilidad organizacional, garantizando que la UMNG continúe liderando la educación superior con altos estándares de calidad, ética y excelencia operativa.

1.2. Objetivo

Establecer los lineamientos y disposiciones para la articulación, gestión y control de riesgos en los procesos, estrategias, proyectos y sistemas de gestión de la Universidad Militar Nueva Granada (UMNG), asegurando su integración con el direccionamiento estratégico institucional. Este marco busca contribuir al cumplimiento de los objetivos misionales, la reducción de eventos no deseados y sus impactos, la identificación y aprovechamiento de oportunidades, y la consolidación de una cultura organizacional basada en la gestión del riesgo.

1.3. Alcance

Este manual aplica a todas las unidades académico-administrativas de la Universidad Militar Nueva Granada (UMNG), así como a sus procesos estratégicos, misionales, de apoyo y de evaluación y control. Su implementación garantiza un enfoque integral en la gestión del riesgo, alineado con la planeación institucional, el Sistema Integrado de Gestión (SIG) y el Modelo Estándar de Control Interno (MECI), en cumplimiento de la normativa nacional vigente.

La metodología establecida abarca la identificación, análisis, valoración, tratamiento, seguimiento y mejora continua de los riesgos, promoviendo un enfoque transversal donde cada líder de proceso asume la responsabilidad sobre los riesgos que afectan su gestión.

Este manual se articula directamente con el **Sistema de Control Interno**, integrándose como una herramienta de gestión preventiva que fortalece la evaluación del desempeño institucional, permite

anticipar eventos adversos, mejora la toma de decisiones y soporta el aseguramiento de los objetivos institucionales.

La Oficina Asesora de Planeación Estratégica (OFIPLA) lidera la consolidación, monitoreo y reporte de los riesgos estratégicos y transversales, en coordinación con las demás dependencias responsables de los procesos institucionales. Así mismo, actúa como instancia articuladora en el Comité Institucional de Gestión y Desempeño y el Equipo Técnico de Identificación y Respuesta (ETIR) el cual lo integra un representante de Control Interno y Desempeño, un representante de División de Gestión de la Calidad y un representante de la Oficina de Planeación Estratégica.

El seguimiento a los riesgos institucionales se realiza con la siguiente periodicidad:

Riesgos de corrupción y estratégicos: seguimiento cuatrimestral, conforme a los lineamientos del Departamento Administrativo de la Función Pública (DAFP) y en coordinación con la Oficina de Control Interno de Gestión (OFICIG).

1.4. Siglas

OFICIG: Oficina de Control Interno de Gestión
DAFP: Departamento Administrativo de la Función Pública
OFIPLA: Oficina Asesora de Planeación Estratégica
ETIR: Equipo Técnico Integral de Riesgos
ISO: Organización Internacional para la Estandarización
KRI's: Indicadores clave de riesgo
MIGR: Marco Integral para la Gestión del Riesgo
N/A: No aplica
NTC: Norma Técnica Colombiana
SIG: Sistema Integrado de Gestión
DIVGCA: División de Gestión de Calidad
PESV: Plan Estratégico de Seguridad Vial
MECI: Modelo Estándar de Control Interno.
PDI: Plan de Desarrollo Institucional.

1.5. Definiciones[1]

Definiciones Generales sobre Gestión del Riesgo

- **Análisis de Riesgos:** Proceso sistemático mediante el cual se identifican, comprenden y evalúan los factores que pueden afectar negativamente el cumplimiento de los objetivos institucionales, estratégicos y operativos, considerando su probabilidad de ocurrencia y el impacto potencial.
- **Causa:** Factor, condición o evento, de origen interno o externo, que da lugar a la existencia de un riesgo. Puede estar asociado a personas, procesos, tecnología, normas, decisiones, o el entorno institucional.

[1] **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 V6 del DAFP.**

- **Consecuencia:** Resultado directo o indirecto que se materializa cuando ocurre un riesgo. Puede afectar negativamente la operación, imagen, recursos, cumplimiento de metas o sostenibilidad institucional.
- **Control:** Medida, procedimiento, acción o herramienta implementada para prevenir, reducir o mitigar la probabilidad y/o el impacto de un riesgo. Los controles pueden ser administrativos, operativos, tecnológicos o financieros.
- **Evaluación del Riesgo:** Comparación del nivel de riesgo (inherente o residual) frente a criterios previamente definidos por la Universidad, con el fin de priorizarlo y decidir si se requiere tratamiento adicional.
- **Gestión del Riesgo:** Conjunto articulado de políticas, estrategias, procesos, prácticas y herramientas destinadas a identificar, analizar, tratar, monitorear y comunicar los riesgos que pueden afectar a la UMNG, garantizando la mejora continua y la toma de decisiones informada.
- **Mapa de Riesgos:** Representación gráfica y estructurada de los riesgos identificados en la Universidad, que clasifica su nivel de criticidad según la combinación de probabilidad e impacto. Es una herramienta dinámica, que se actualiza periódicamente (mínimo una vez al año o cuando ocurran eventos relevantes) como parte del ciclo de mejora continua. Sirve de insumo para la priorización, tratamiento y seguimiento de los riesgos.
- **Monitoreo de Riesgos:** Proceso continuo de revisión y verificación del comportamiento de los riesgos institucionales, sus controles y acciones de tratamiento. En la UMNG se realiza con periodicidad cuatrimestral, conforme a la Guía del DAFP (2022), e implica la actualización del estado del riesgo, análisis de desviaciones y definición de medidas correctivas o preventivas.
- **Política de Administración del Riesgo:** Conjunto de directrices aprobadas institucionalmente, que orientan la gestión de los riesgos de manera articulada con el direccionamiento estratégico, asegurando un enfoque proactivo, sistemático y transparente.
- **Probabilidad:** Estimación de la frecuencia o posibilidad de ocurrencia de un evento riesgoso, bajo determinadas condiciones institucionales.
- **Riesgo Inherente:** Nivel de riesgo que existe antes de aplicar controles o acciones de mitigación. Representa el nivel de exposición pura de la Universidad ante una amenaza.

  Ejemplo: En la UMNG, un riesgo inherente podría ser la pérdida de información académica por fallas en el servidor, cuya probabilidad e impacto podrían dar un nivel de riesgo "Alto" antes de aplicar medidas.

- **Riesgo Residual:** Nivel de riesgo que permanece después de aplicar los controles existentes o implementados. Refleja la exposición real de la institución tras haber gestionado el riesgo.

  Ejemplo: Continuando con el ejemplo anterior, si se instalan servidores redundantes, copias de seguridad automáticas y protocolos de recuperación, el riesgo residual podría disminuir a un nivel "Moderado" o incluso "Bajo".

Definiciones Asociadas a los Proyectos Institucionales

- **Alcance:** Representa los entregables previstos de un proyecto, incluyendo actividades requeridas para su cumplimiento dentro del marco estratégico de la UMNG.
- **Calidad:** Corresponde a los estándares de calidad aplicados en la gestión del proyecto y sus entregables, asegurando su alineación con los objetivos institucionales.
- **Ciclo de Vida del Proyecto:** Etapas por las cuales transcurre un proyecto en la UMNG: formulación, aprobación, ejecución, evaluación y cierre (liquidación).
- **Costo:** Representa la cantidad de recursos financieros requeridos para la ejecución del proyecto, en alineación con la planificación presupuestal institucional.
- **Impacto:** Magnitud del efecto adverso que puede generar un riesgo sobre los componentes del proyecto o en la UMNG en general.
- **Nivel de Aceptabilidad del Riesgo:** Umbral de exposición al riesgo que la UMNG considera tolerable dentro del contexto institucional y de proyectos.
- **Proyecto:** Esfuerzo temporal llevado a cabo para generar un producto, servicio o resultado alineado con los objetivos estratégicos de la UMNG.
- **Riesgo en Proyectos:** Cualquier amenaza que puede afectar el cumplimiento del alcance, metas, actividades, entregables o recursos de un proyecto institucional.
- **Tiempo:** Plazo establecido para la ejecución de un proyecto en la UMNG, sujeto a gestión del riesgo para mitigar posibles desviaciones.

Definiciones Asociadas a la Gestión del Riesgo Institucional

- **Amenaza:** Circunstancia o evento adverso que puede ocurrir en cualquier etapa de un proyecto o proceso, generando efectos negativos.
- **Componente Amenazado:** Elemento dentro de un proceso, sistema o proyecto que puede verse afectado en caso de materializarse un riesgo.
- **Comunicación y Consulta:** Procesos continuos que permiten compartir información sobre la gestión del riesgo entre diferentes actores institucionales.
- **Identificación del Riesgo:** Proceso de encontrar, reconocer y describir riesgos potenciales que pueden afectar la UMNG.
- **Riesgo Inherente o Puro:** Evaluación preliminar del riesgo en ausencia de controles o medidas de mitigación.
- **Riesgo Residual o Remanente:** Nivel de riesgo que persiste después de aplicar medidas de control.
- **Tratamiento del Riesgo:** Estrategias implementadas para modificar el nivel de riesgo, ya sea eliminándolo, mitigándolo, transfiriéndolo o aceptándolo.
- **Valoración del Riesgo:** Proceso integral de identificación, análisis y evaluación del riesgo para determinar su nivel de prioridad en la UMNG.

Definiciones Específicas para la Gestión del Riesgo en la UMNG

- **Riesgos Fiscales:** Situaciones derivadas de acciones u omisiones que pueden generar un detrimento patrimonial a la UMNG, por el uso inadecuado, ineficiente o irregular de los recursos públicos. Estos riesgos pueden materializarse en pérdidas económicas, sanciones o investigaciones fiscales por parte de los entes de control.
- **Riesgos Estratégicos:** Amenazas que pueden afectar el cumplimiento de la misión, visión y objetivos estratégicos de la UMNG.
- **Seguridad de la Información:** Vulnerabilidades que comprometen la confidencialidad, integridad y disponibilidad de la información institucional.

- **Riesgos Operativos:** Factores que pueden interferir con la ejecución y eficiencia de los procesos institucionales, incluyendo los relacionados con:

    - **Seguridad y Salud en el Trabajo:** Condiciones que pueden afectar la integridad, salud y bienestar del talento humano de la UMNG.
    - **Sostenibilidad:** Factores que generan impactos ambientales, tecnológicos o financieros que comprometen la sostenibilidad institucional.
    - **Financieros y Contables:** Situaciones que impactan la estabilidad económica, la gestión de recursos y la sostenibilidad financiera.
    - **Corrupción:** Vulnerabilidades que pueden propiciar fraudes, sobornos o prácticas contrarias a la transparencia y la ética institucional, articulado al Programa de Transparencia y Ética Pública, en cumplimiento del Decreto 124 de 2016 y su Anexo Técnico.
    - **Daño Antijurídico:** Situaciones que pueden derivar en sanciones legales o litigios contra la UMNG por incumplimiento normativo.
    - **Proyectos de Investigación e Innovación:** Factores que afectan la formulación, ejecución o sostenibilidad de iniciativas científicas y académicas.
    - **Plan de Desarrollo Institucional:** Amenazas que afectan la implementación y cumplimiento de las estrategias institucionales de largo plazo.
    - **Plan Estratégico de Seguridad Vial (PESV):** Factores que comprometen la seguridad vial en el entorno universitario, derivados del comportamiento humano, condiciones de infraestructura, fallas mecánicas o incumplimiento normativo. Su gestión busca prevenir accidentes y proteger la integridad de la comunidad UMNG.

1.6. Marco General

La formulación del mapa de gestión del riesgo es una herramienta clave dentro del Direccionamiento Estratégico, Programa de Transparencia y Ética Pública, ya que permite fortalecer los mecanismos de prevención, administración y control del riesgo institucional. Su implementación facilita el seguimiento y la mejora continua en los procesos estratégicos de la Universidad Militar Nueva Granada.

Este manual se fundamenta en normativas y estándares internacionales que garantizan una gestión eficiente del riesgo:

- ISO 9001:2015: Integra la gestión del riesgo y la identificación de oportunidades como elementos fundamentales para el reconocimiento de los grupos de interés y el cumplimiento de los objetivos institucionales.
- ISO 14001:2015: Asegura la identificación y control de riesgos y oportunidades ambientales, alineándose con requisitos legales y expectativas de las partes interesadas. Incluye el Sistema de Gestión Basura Cero.
- ISO 45001:2018: Establece directrices para la gestión de los peligros y riesgos en Seguridad y Salud en el Trabajo.
- ISO 21001:2018 - Integra la gestión del riesgo y la identificación de oportunidades como elementos fundamentales para el reconocimiento de los grupos de interés y el cumplimiento de los objetivos institucionales, específicamente en entidades educativas.
- ISO 27001: 2022 - Promueve un enfoque holístico de la seguridad de la información, definiendo actividades para la gestión de riesgos, la ciberresiliencia y la excelencia operativa.
- Sistema de Gestión Basura Cero: Promueve un enfoque sostenible, integrando la gestión de

residuos dentro de la política institucional.

Asimismo, este manual se apoya en la Guía para la Administración de Riesgos del Departamento Administrativo de la Función Pública en su versión 6 de noviembre de 2022, la NTC ISO 31000 y la GTC 137 (ISO Guide 73), asegurando que la gestión del riesgo se realice conforme a lineamientos internacionales. Para su implementación, la plataforma KAWAK proporciona un módulo especializado que facilita la identificación, contextualización, medición, control y seguimiento de los riesgos, optimizando la toma de decisiones y garantizando el cumplimiento de los objetivos institucionales.

1.7. Beneficios del Modelo Integral de Gestión del Riesgo (MIGR)

La implementación del Modelo Integral de Gestión del Riesgo (MIGR) en la Universidad Militar Nueva Granada (UMNG) permite integrar procesos, estrategias, proyectos y sistemas de gestión bajo un enfoque metodológico estructurado, alineado con el Plan de Desarrollo Institucional, la Guía para la Administración del Riesgo en Entidades Públicas del DAFP (versión 2022) y la norma ISO 31000. Este modelo fortalece la capacidad institucional para anticiparse, prevenir y responder ante eventos adversos que puedan comprometer sus objetivos.

El MIGR genera diez beneficios clave, que fortalecen la sostenibilidad institucional, promueven la mejora continua y consolidan una cultura organizacional basada en la gestión del riesgo:

1. Articula la gestión del riesgo con el Plan de Desarrollo Institucional y sistemas normativos como la Guía DAFP y la ISO 31000, asegurando el cumplimiento de estándares nacionales e internacionales.
2. Vincula la gestión del riesgo con los procesos, proyectos y sistemas de gestión académicos, administrativos y estratégicos, permitiendo su incorporación desde la planeación hasta la ejecución.
3. Proporciona lineamientos claros, metodologías prácticas y parámetros definidos para gestionar riesgos en todos los ámbitos, facilitando su apropiación por parte de líderes de procesos, supervisores y equipos de trabajo.
4. Posiciona la gestión del riesgo como una prioridad en los Comités Institucionales, respaldando decisiones con datos confiables sobre la evolución, controles y nivel de exposición de los riesgos.
5. Impulsa una cultura organizacional proactiva mediante capacitación periódica, campañas de sensibilización, actividades de apropiación institucional y la integración del MIGR con sistemas como el de gestión de calidad.
6. Minimiza riesgos que puedan afectar la misión, visión y credibilidad de la UMNG ante la comunidad universitaria, entes reguladores y aliados estratégicos.
7. Facilita el monitoreo, seguimiento cuatrimestral y actualización dinámica de los riesgos, generando oportunidades para la optimización constante de procedimientos, controles y estrategias institucionales.
8. Define con claridad qué niveles de riesgo pueden asumirse, cuáles requieren tratamiento y en qué condiciones deben reforzarse los controles, favoreciendo una gestión diferenciada y proporcional.
9. Disminuye los obstáculos que afectan el desarrollo de estrategias, proyectos e iniciativas misionales, optimizando recursos y tiempos.

10. Permite identificar debilidades internas, responder oportunamente a cambios normativos y tecnológicos, y capitalizar ventajas competitivas que posicionen a la Universidad como referente en gobernanza institucional.

2. MODELO DE GESTIÓN DE RIESGOS PARA LA UMNG

La Universidad Militar Nueva Granada (UMNG) implementa un modelo de gestión integral del riesgo fundamentado en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar), el cual permite anticipar, mitigar y monitorear las amenazas que pueden afectar sus procesos, estrategias, proyectos y sistemas de gestión.

La gestión de riesgos en la UMNG se realiza transversalmente en toda la institución, considerando los diferentes tipos de riesgo (estratégico, fiscal, operativo, de corrupción y de seguridad de la información). El ciclo PHVA se aplica de la siguiente manera:

- **Planear**: Identificación, análisis y valoración de los riesgos, así como definición de responsables, causas, impactos y controles existentes.
- **Hacer**: Implementación de medidas de tratamiento, controles y planes de mejoramiento en función del nivel de riesgo identificado.
- **Verificar**: Seguimiento periódico al comportamiento de los riesgos, evaluación de controles, medición de indicadores clave de riesgo (KRI) y análisis de los riesgos materializados.
- **Actuar**: Ajustes a las medidas implementadas, rediseño de controles o reformulación de acciones, en función de los resultados del seguimiento, auditorías o cambios en el contexto institucional.

Este enfoque permite a la UMNG cumplir con sus objetivos estratégicos y operativos, promoviendo una cultura de prevención, responsabilidad y mejora continua en todos los niveles de la organización.

2.1 POLÍTICA DE GESTIÓN DEL RIESGO

La Política de Gestión del Riesgo es un pilar fundamental del Modelo Integral de Gestión del Riesgo (MIGR) de la UMNG. Define el compromiso institucional con la prevención, mitigación y control de riesgos en todas sus dimensiones, asegurando que su gestión se integre a los procesos estratégicos de la universidad.

Esta política establece las directrices y metodologías para la administración de riesgos en el marco de los objetivos misionales de la UMNG y se articula con normativas nacionales e internacionales.

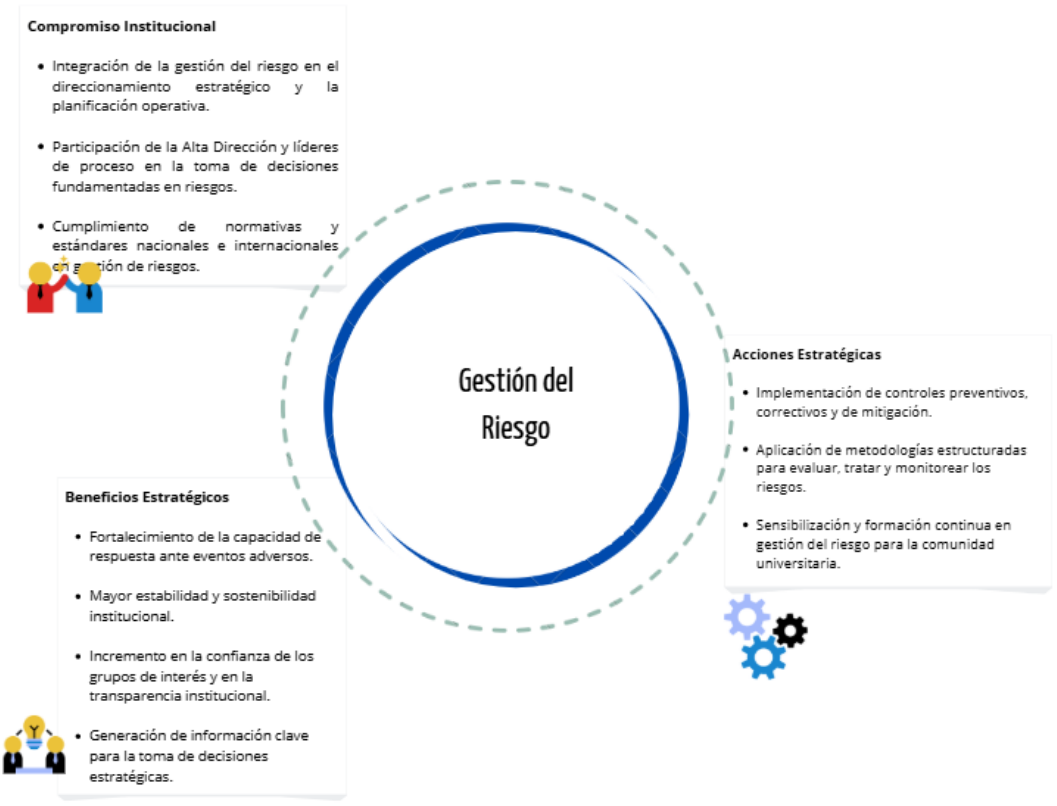
2.1.1 Declaración (Objetivo General)

La Universidad Militar Nueva Granada (UMNG) reafirma su compromiso con la transparencia y probidad institucional, garantizando un ambiente de integridad académica y administrativa mediante el monitoreo permanente y la mejora continua en la identificación, análisis, control y administración de riesgos. A través del desarrollo de competencias en la comunidad universitaria, la gestión estructurada del riesgo y la aplicación de metodologías alineadas con estándares nacionales e internacionales, la UMNG busca minimizar la materialización de riesgos, priorizando acciones según su probabilidad e impacto. Con ello, se fortalece la toma de decisiones fundamentadas, la

sostenibilidad institucional y la creación y protección del valor, asegurando el cumplimiento de sus objetivos estratégicos en un entorno seguro y sostenible.

2.1.2 Pilares de la Gestión del Riesgo

La Política Integral de Gestión del Riesgo en la UMNG se sustenta en tres pilares fundamentales:



Fuente: Elaboración Propia

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 UMNG.

2.2. Tipologías de Riesgos Contenidas en el MIGR de la UMNG

La gestión integral del riesgo en la Universidad Militar Nueva Granada (UMNG) comprende una diversidad de tipologías de riesgo que se relacionan directamente con los procesos, estrategias, proyectos y sistemas de gestión institucional. Estas tipologías permiten clasificar, priorizar y abordar los riesgos de manera más efectiva, asegurando una respuesta oportuna frente a las amenazas que puedan derivar en afectaciones económicas o reputacionales.

Cada tipo de riesgo está asociado a instancias responsables que lideran su administración, según la naturaleza del evento y el contexto institucional en el que se presente. Es importante destacar que un mismo riesgo puede estar vinculado a más de una tipología, lo cual exige una gestión coordinada y transversal entre las áreas implicadas.

Por ejemplo, un incidente de pérdida de información confidencial puede clasificarse simultáneamente como un:

- Riesgo de Seguridad de la Información, por comprometer la integridad, disponibilidad y confidencialidad de los datos;
- Riesgo de Corrupción, si se detecta acceso indebido con fines fraudulentos;
- Y eventualmente, como un Riesgo Fiscal, si dicho incidente deriva en sanciones económicas o responsabilidades fiscales por el uso inadecuado de activos públicos.

Esta interrelación entre tipologías subraya la importancia de articular esfuerzos entre las diferentes áreas responsables y asegurar que los riesgos sean analizados con un enfoque integral.

Tabla de Tipologías de Riesgos y Responsables en la UMNG

Tipo de Riesgo	Sistemas/Instancias Responsables
Riesgos Estratégicos	Oficina Asesora de Planeación Estratégica, Rectoría, Comité Institucional de Gestión y Desempeño, Consejo Superior Universitario, Dirección de Calidad.
Riesgos de Proyectos	Oficina Asesora de Planeación Estratégica, Vicerrectoría Académica, Vicerrectoría de Investigación, líderes de proyectos, supervisores e interventores, Comités Académicos y de Investigación.
Riesgos de Seguridad de la Información (SI)	Oficina Asesora de las Tecnologías de la Información y las Comunicaciones (TIC), Sistema de Gestión de Seguridad de la Información, líderes de procesos con activos de información.

Riesgos de Corrupción: Fraude, Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM)	Vicerrectoría Administrativa, Comité de Ética y Transparencia Institucional, Oficina Asesora de Planeación estratégica
Riesgos Operativos	Líderes de procesos, División de Gestión de Calidad, Jefaturas Académicas y Administrativas.
Riesgos Fiscales	Oficina de Control Interno, Oficina Asesora Jurídica, División Financiera, órganos de control fiscal.

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.

2.3. Modelo de las Tres Líneas de Defensa - Roles y Responsabilidades en la UMNG

La Universidad Militar Nueva Granada (UMNG) adopta el Modelo de las Tres Líneas de Defensa como estructura organizacional para la gestión integral del riesgo, de conformidad con los lineamientos de la Guía del DAFP (2022) y la norma ISO 31000:2018. Este modelo establece roles diferenciados y coordinados para garantizar una administración eficaz, articulada y transparente de los riesgos institucionales.

Corresponde al nivel superior de la Universidad encargado de definir las políticas y directrices del Modelo Integral de Gestión del Riesgo (MIGR), asegurar su alineación con el direccionamiento estratégico, y tomar decisiones frente a los riesgos significativos.

Responsables	Responsabilidades
Comité Institucional de Gestión y Desempeño	Aprobar el Marco Integral de Gestión del Riesgo (MIGR).
	Establecer la Política Integral de Gestión del Riesgo.
	Analizar y tomar decisiones frente a riesgos estratégicos o críticos escalados por las otras líneas.
	Aprobar los informes de seguimiento y definir estrategias de intervención.

Primera Línea de Defensa - Autocontrol y Gestión Operativa de Riesgos

Es la línea responsable de gestionar directamente los riesgos asociados a sus procesos, proyectos o funciones. Implementa los controles definidos, realiza el seguimiento operativo y promueve una cultura de autocontrol.

Esta línea está compuesta por Vicerrectores, Decanos, Directores, Jefes de División, Coordinadores de procesos, responsables de proyectos, responsables de áreas transversales y líderes operativos.

Responsables	Responsabilidades
Líderes de procesos y proyectos	Identificar, analizar, valorar y documentar los riesgos de su área en la plataforma KAWAK.
	Implementar controles y planes de mitigación.
	Ejecutar acciones correctivas frente a desviaciones.
	Garantizar la trazabilidad de los riesgos y su gestión.
Líderes de Gestión Ambiental	Identificar y mitigar riesgos ambientales.
	Asegurar el cumplimiento de normativas ambientales vigentes.
	Implementar controles para la sostenibilidad institucional.
Responsables de Seguridad y Salud en el Trabajo (SST)	Evaluar y controlar los riesgos laborales.
	Implementar medidas preventivas y de protección del personal.
	Promover condiciones laborales seguras.
Responsables de Seguridad de la Información	Gestionar riesgos de ciberseguridad y protección de datos.
	Garantizar la integridad, confidencialidad y disponibilidad de la información institucional.

Segunda Línea de Defensa - Seguimiento, Evaluación y Asesoría

Brinda acompañamiento técnico y metodológico a la primera línea. Evalúa la efectividad de los controles, realiza seguimiento cuatrimestral, y promueve la mejora continua mediante recomendaciones, retroalimentación y análisis de resultados.

Mecanismos de seguimiento institucional:

- Revisión cuatrimestral de riesgos estratégicos y de corrupción institucional.
- Verificación de trazabilidad entre riesgos, controles, indicadores y planes de acción.
- Aplicación de autoevaluaciones, auditorías internas y herramientas de monitoreo.
- Emisión de alertas, recomendaciones y retroalimentaciones escritas a líderes de proceso.

Responsables	Responsabilidades
Oficina Asesora de Planeación Estratégica	Realizar monitoreos, asesorar y realizar seguimiento cuatrimestral a los riesgos.

	Evaluar el contexto para la formulación de reformulación o implementación de nuevos riesgos.
	Monitorear la implementación de planes de acción y su impacto en la mitigación de riesgos.
	Evaluar la efectividad de los controles implementados y generar informes de gestión del riesgo.
División de Gestión de Calidad	- Asegurar la integración de la gestión del riesgo dentro de los procesos y procedimientos del Sistema Integrado de Gestión Institucional (SIGI).
	- Identificar y documentar los riesgos institucionales en conjunto con los líderes de proceso, así como los responsables de la gestión de controles.
	- Brindar capacitación y asesoría a los líderes de proceso sobre metodologías de gestión de riesgos.
	- Validar el cumplimiento de estándares normativos en los controles implementados.

Tercera Línea de Defensa - Evaluación Independiente

Responsabilidad de la Oficina de Control Interno de Gestión, que actúa de forma independiente, evaluando objetivamente la eficacia del sistema de control interno y la gestión del riesgo institucional.

Responsables	Responsabilidades
Oficina de Control Interno de Gestión	- Evaluar la efectividad del Sistema de Control Interno con un enfoque basado en riesgos.
	- Realizar auditorías y seguimiento independiente a la gestión de riesgos.
	- Emitir alertas y recomendaciones para prevenir incumplimientos o deficiencias en la gestión de riesgos. - Verificar la implementación de medidas correctivas. - Promover la cultura del control y la transparencia institucional.

2.4 Metodología para la Gestión Integral de Riesgos

La gestión integral del riesgo en la Universidad Militar Nueva Granada (UMNG) se fundamenta en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública (DAFP) – versión 6 de noviembre de 2022, junto con los principios esenciales de la Norma Técnica Colombiana ISO 31000:2018 y otros estándares internacionales como ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, ISO 21001:2018 e ISO 27001:2022.

Este enfoque metodológico permite estructurar la gestión del riesgo de forma alineada con los estándares internacionales, las mejores prácticas del sector público y académico, y el modelo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar). Su aplicación está integrada al Sistema de Control Interno y al Sistema Integrado de Gestión Académica, Administrativa y Ambiental (SIGA), asegurando la cobertura de riesgos en todos los niveles de la institución.

La formulación y actualización del Mapa de Gestión del Riesgo Institucional se desarrolla en cinco fases interdependientes, que garantizan un enfoque estructurado y sistemático:

Fuente: Elaboración Propia

- **Análisis del Contexto Institucional:** Consiste en la evaluación de factores internos (estructura, procesos, cultura organizacional, recursos) y externos (marco normativo, entorno político, tecnológico, social y ambiental) que pueden influir en la aparición y gestión de riesgos, en coherencia con los objetivos estratégicos, misionales y operativos de la UMNG.

- **Identificación del Riesgo:** Implica la detección y caracterización de amenazas y oportunidades que puedan afectar el cumplimiento de los objetivos institucionales. Este ejercicio se realiza con el apoyo de herramientas como listas de verificación, análisis de procesos, revisión de experiencias previas, grupos focales y consulta a líderes de procesos.

- **Análisis y Valoración del Riesgo:** Se lleva a cabo mediante la aplicación de matrices de impacto y probabilidad, así como del uso del Mapa de Calor definido institucionalmente. Esta etapa permite estimar el nivel de riesgo inherente y residual, clasificarlos por criticidad (bajo, moderado, alto o extremo), y priorizar aquellos que requieren una intervención urgente o especial.

- **Tratamiento de los riesgos:** En esta fase se definen las estrategias más adecuadas para cada riesgo, como la reducción, transferencia, aceptación o eliminación, teniendo en cuenta su nivel de criticidad y tolerancia institucional. Se formulan planes de acción, con responsables, plazos y recursos asignados, los cuales se registran y hacen seguimiento a través de la plataforma tecnológica KAWAK.

- **Seguimiento y Revisión:** Esta fase garantiza la trazabilidad, actualización y mejora continua en la gestión de riesgos. El seguimiento se realiza con **periodicidad cuatrimestral**, conforme a lo establecido en la Guía del DAFP, y está acompañado por los siguientes mecanismos:

    - **Indicadores clave de riesgo (KRI):** Se utilizan para alertar sobre cambios en la exposición al riesgo o en la eficacia de los controles. Ejemplos: número de incidentes reportados, cumplimiento de acciones correctivas, evolución de niveles de riesgo residual.
    - **Auditorías internas y autoevaluaciones:** Aplicadas a través del Sistema Integrado de Gestión, permiten verificar la adecuación de los controles implementados y su efectividad.
    - **Reportes periódicos de seguimiento:** Elaborados por la Oficina Asesora de Planeación Estratégica y la División de Calidad, incluyen análisis de desviaciones, hallazgos y recomendaciones.
    - **Revisión por los Comités Institucionales:** Especialmente el Comité Institucional de Gestión y Desempeño, que evalúa los riesgos significativos y aprueba las decisiones estratégicas de intervención.
    - **Herramientas tecnológicas de control:** La plataforma KAWAK permite registrar y monitorear los riesgos, controles, responsables, planes de acción y su nivel de avance, generando alertas y trazabilidad de cada fase del ciclo de gestión.

Este enfoque permite retroalimentar continuamente el mapa de riesgos, adaptarse a nuevos escenarios y garantizar que la gestión del riesgo sea efectiva, dinámica y alineada con la mejora continua institucional.

2.4.1. Contexto Interno y Externo

El establecimiento del contexto es una etapa fundamental en la gestión integral del riesgo, ya que permite comprender de manera amplia y sistémica los entornos en los que opera la Universidad Militar Nueva Granada (UMNG). Esta comprensión resulta clave para anticiparse a los eventos que puedan afectar el cumplimiento de los objetivos institucionales y definir estrategias de gestión del riesgo acordes con la realidad institucional.

El análisis del contexto tiene como propósito identificar de forma estructurada los factores internos y externos que pueden influir positiva o negativamente en los procesos, estrategias, proyectos y sistemas de gestión de la Universidad. Este ejercicio facilita la identificación de retos, fortalezas, oportunidades y amenazas, en coherencia con la dinámica del sector educativo y el marco normativo aplicable.

Una vez comprendida la relevancia del contexto, se hace necesario sustentar este análisis con información proveniente de fuentes institucionales y sectoriales confiables. En ese sentido, se debe tener en cuenta insumos como:

- El diagnóstico estratégico del Plan de Desarrollo Institucional (PDI),
- Los informes de Autoevaluación Institucional,
- Los Planes Operativos de las Unidades Académico-Administrativas,
- Los resultados de auditorías y planes de mejoramiento,
- Estudios del entorno social, político, económico, tecnológico y ambiental,
- Análisis del comportamiento de los grupos de interés y partes interesadas.

Adicionalmente, el establecimiento del contexto implica alinear la gestión del riesgo con los lineamientos estratégicos, metas institucionales y prioridades definidas, lo que permite asignar recursos de manera eficaz, estructurar respuestas oportunas y facilitar la toma de decisiones orientadas a la sostenibilidad institucional.

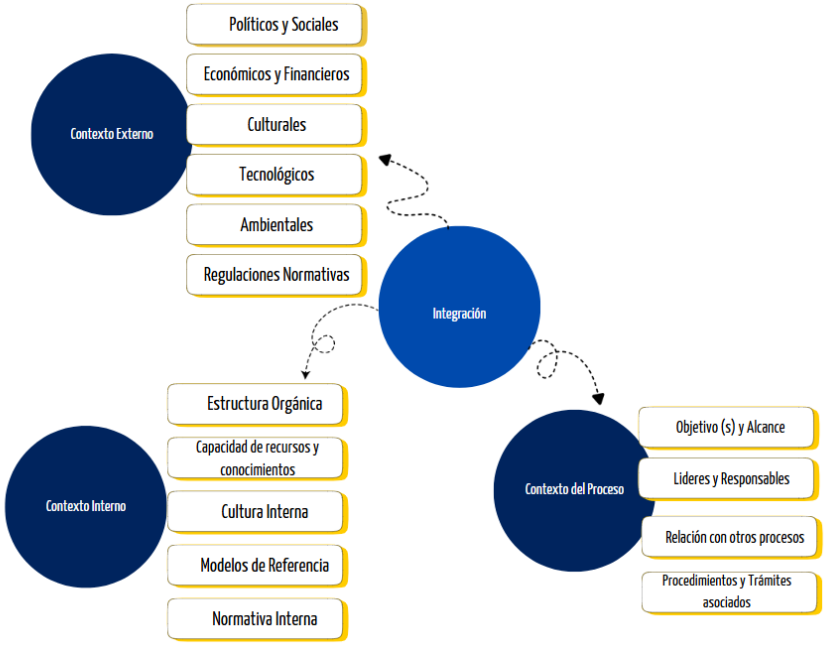
Un aspecto central en este proceso es el Modelo de Operación Institucional, que articula todos los procesos y dependencias que soportan la actividad universitaria, garantizando la coherencia entre la gestión de riesgos y el cumplimiento de la misión y visión de la UMNG. Este modelo proporciona información clave sobre la interacción entre procesos, productos, servicios, proyectos y grupos de valor, lo cual permite una identificación más precisa de los riesgos relevantes para la Universidad.

Además, la implementación del Modelo Integral de Gestión de Riesgos (MIGR) exige un conocimiento profundo de la UMNG, que abarque su estructura organizacional, visión estratégica, valores, cultura, estados financieros, recursos físicos y tecnológicos, procesos académicos y administrativos, así como sus relaciones con el entorno.

Por ello, también se debe contemplar el contexto externo, el cual incluye factores sociales, culturales, tecnológicos, económicos, normativos y ambientales, que pueden incidir directa o indirectamente en la gestión del riesgo universitario.

Finalmente, este proceso debe ejecutarse bajo el enfoque de mejora continua (PHVA: Planear, Hacer, Verificar, Actuar), permitiendo que la gestión del riesgo sea un ejercicio dinámico, iterativo y adaptable a los cambios institucionales o del entorno. La recopilación, análisis y documentación de esta información será responsabilidad de los líderes de proceso y de los responsables por tipología de riesgo, quienes deberán garantizar el cumplimiento de los principios de trazabilidad, evidencia y uso de sistemas de información establecidos por la Universidad.

Variables del contexto interno y externo y de procesos:



Fuente: Elaboración Propia

2.4.2. Identificación del Riesgo

La identificación del riesgo es una fase fundamental en la gestión integral del riesgo, ya que permite reconocer las fuentes, causas, áreas de impacto y consecuencias que pueden afectar el cumplimiento de los objetivos institucionales. Este proceso busca generar un listado estructurado de riesgos que puedan perjudicar los procesos, estrategias, proyectos y sistemas de gestión de la Universidad Militar Nueva Granada (UMNG).

La identificación debe estar alineada con los factores internos y externos definidos en el Establecimiento del Contexto, y ser responsabilidad de los actores de la primera línea de defensa, conformada por los líderes de proceso, jefes de división, decanos, directores, vicerrectores y demás responsables operativos que conocen de primera mano los riesgos asociados a sus áreas de gestión.

Para garantizar una identificación oportuna y completa, es importante considerar los siguientes aspectos:

- Partir del análisis del entorno interno y externo establecido previamente.
- Revisar periódicamente si las causas o agentes generadores del riesgo han cambiado.

- Identificar:
    - Riesgos que se han materializado recientemente.
    - Riesgos mitigados o que han perdido vigencia.
    - Debilidades convertidas en oportunidades.
    - Nuevas amenazas que emergen del entorno institucional o normativo.

2.4.2.1 Identificación y Priorización de Riesgos

La identificación y priorización de riesgos constituye una etapa fundamental en la gestión integral de riesgos de la UMNG, pues permite reconocer de manera sistemática las amenazas que pueden afectar el logro de los objetivos estratégicos, misionales, de apoyo y de control, así como asignar esfuerzos y recursos de manera eficiente.

Este proceso busca no solo reconocer los riesgos existentes, sino establecer un mecanismo que facilite priorizar aquellos más críticos, con base en criterios objetivos, permitiendo la toma de decisiones, la implementación de controles y la formulación de planes de mejoramiento oportunos.

Este ejercicio corresponde a los actores de la Primera Línea de Defensa: Directores, Vicerrectores, Decanos, jefes de División, Coordinadores de procesos, proyectos y sistemas de gestión, quienes son los responsables directos de la gestión de riesgos en sus respectivas áreas y deben garantizar la correcta identificación, formulación, análisis y priorización de los riesgos bajo su gestión.

Recomendaciones prácticas para la identificación de riesgos

Partir de los factores internos y externos previamente identificados en la etapa de establecimiento del contexto.

Revisar periódicamente la evolución de los riesgos, considerando:

- Cambios en causas, amenazas o agentes generadores.
- Riesgos que han pasado de posibles a materializados.
- Riesgos mitigados, controlados, unificados o excluidos.
- Nuevas amenazas emergentes no consideradas anteriormente.

La UMNG ha definido un conjunto de criterios estructurados que permiten evaluar los riesgos de manera integral, favoreciendo la priorización de aquellos que puedan tener mayores impactos o requerir atención inmediata.

La priorización garantiza que los recursos limitados sean direccionados a los riesgos más relevantes para la institución, permitiendo una gestión eficaz, la definición de controles, la asignación de responsabilidades y la formulación de planes de mejora o mitigación.

A continuación, se presentan los criterios definidos por la UMNG para la priorización de riesgos:

Criterio	Descripción
Impacto en los objetivos institucionales	Se priorizan los riesgos que pueden afectar el cumplimiento de los procesos, estrategias, proyectos y sistemas de gestión.
Afectación a la misión y visión institucional	Se consideran los riesgos que pueden comprometer la sostenibilidad y desarrollo estratégico de la UMNG.
Historial de materialización	Se revisan los riesgos que han ocurrido en periodos anteriores, evaluando su reincidencia y tendencia.
Afectación a productos y servicios	Se priorizan los riesgos que pueden interrumpir la prestación de servicios académicos, administrativos o investigativos.
Impacto en indicadores clave	Se evalúa la repercusión de los riesgos en el cumplimiento de metas y KPI institucionales.
Hallazgos de auditorías y evaluaciones externas	Se identifican riesgos que han generado hallazgos críticos o recurrentes en auditorías internas o externas.
Gobernabilidad del riesgo	Se consideran los riesgos que están dentro del ámbito de control y gestión de la UMNG.
Complejidad y alcance del riesgo	Se priorizan los riesgos con mayor nivel de propagación o repercusión institucional.
Velocidad de materialización	Se identifican los riesgos que pueden impactar rápidamente la operatividad de la Universidad.
Persistencia del impacto	Se priorizan los riesgos cuyo efecto negativo puede prolongarse en el tiempo.
Capacidad de recuperación institucional	Se evalúa el grado de dificultad para que la Universidad pueda retornar a la normalidad tras la materialización del riesgo.

La priorización de riesgos puede realizarse mediante herramientas como:

- Matriz de riesgos (probabilidad x impacto): que permite visualizar gráficamente el nivel de riesgo.
- Escalas de puntuación cualitativa o semicuantitativa: que asignan un valor del 1 al 5 para cada criterio, facilitando un ranking total.
- Análisis de riesgo residual: para priorizar aquellos que, a pesar de los controles existentes, siguen representando una amenaza relevante.

Ejemplo aplicado

Riesgo	Interrupción de los sistemas tecnológicos de información
Impacto en la misión	Alto (afecta clases, pagos, evaluaciones, inscripción, etc.).
Velocidad de materialización	Alta (una caída puede ser súbita y sin previo aviso).
Capacidad de recuperación	Media (requiere soporte técnico especializado y posibles inversiones).

Este análisis permite clasificar este riesgo como prioritario, exigiendo acciones inmediatas para su mitigación y monitoreo.

La identificación y priorización de riesgos no es un proceso estático. Debe ser documentado, revisado y actualizado de manera continua como parte del seguimiento al Mapa de Riesgos Institucional, asegurando que:

- Se registren en los sistemas dispuestos por la UMNG (KAWAK u otros).
- Se mantenga la trazabilidad de las decisiones.
- Se garantice la mejora continua, transparencia y alineación con el ciclo de gestión PHVA.

2.4.2.2 Redacción de riesgos

Una vez identificados y priorizados los riesgos, es fundamental redactarlos de manera clara, precisa y comprensible para todos los actores involucrados, asegurando que la información permita una correcta gestión y mitigación. La redacción de los riesgos debe incluir elementos clave que permitan su fácil comprensión, tanto para los responsables de procesos, estrategias, proyectos y sistemas de gestión, como para actores externos a la Universidad Militar Nueva Granada (UMNG).

Para garantizar uniformidad y claridad en la redacción de los riesgos, se establecen elementos obligatorios y una estructura sugerida de redacción.

2.4.2.2.1 Elementos Obligatorios para la Definición de Riesgos

En el momento de definir un riesgo de cualquier tipología, con el fin de que este sea comprensible tanto para los integrantes de los procesos, estrategias, proyectos y sistemas de gestión, como para actores externos a la UMNG, se deben incluir los siguientes elementos en su redacción o mención explícita:

Impacto	Causa Inmediata	Causa Raíz
• Describe la consecuencia o efecto negativo que tendría la materialización del riesgo.	• Identifica cómo podría ocurrir el riesgo debido a factores evidentes o circunstancias	• Es la razón subyacente o estructural por la cual puede originarse el riesgo.

• Puede afectar objetivos, productos, servicios, activos, recursos, procedimientos y actividades del proceso, estrategia, proyecto o sistema de gestión. • Debe ser claro, específico y medible.	inmediatas. • Se refiere a las condiciones más próximas que podrían propiciar la materialización del riesgo. No es necesariamente la causa principal, sino el detonante más evidente o superficial.	• No corresponde a factores inmediatos, sino a aquellos más profundos que requieren análisis. • Su correcta identificación permite diseñar controles y estrategias de mitigación más eficaces.

Nota: En algunos casos, la causa inmediata y la causa raíz pueden coincidir o estar estrechamente relacionadas. En tales situaciones, se debe justificar claramente esta relación, asegurando que se ha realizado un análisis adecuado del origen del riesgo.

2.4.2.2.2 Forma de redacción sugerida para un riesgo de cualquier tipología

Para facilitar la comprensión y gestión efectiva de los riesgos por parte de todos los actores institucionales, se recomienda una redacción clara, concisa y orientada a la acción. La redacción debe reflejar con precisión la relación entre el impacto, la causa inmediata y la causa raíz del riesgo.

Fuente: Elaboración Propia

Formas sugeridas para iniciar la redacción de un riesgo:

- Posibilidad de que...
- Existe el riesgo de que...
- Probabilidad de que se presente...
- Peligro de que se materialice...

Estas expresiones permiten estandarizar la forma en que se describen los riesgos, evitando ambigüedades y favoreciendo un lenguaje común en toda la Universidad.

Recomendaciones adicionales para la redacción:

- Los riesgos deben ser formulados en forma afirmativa y concreta, evitando ambigüedades como “podría afectar” o “puede impactar”.

- Se recomienda utilizar expresiones como: “afectará si no se toman medidas adecuadas”, para destacar la necesidad de intervención y gestión.

- Evitar el uso de términos genéricos o demasiado amplios. En su lugar, utilizar descripciones específicas que permitan identificar claramente el riesgo y su origen.

Estructura:

"Existe la posibilidad de que [impacto], debido a [causa inmediata], originada por [causa raíz]."

Ejemplo:
Existe la posibilidad de que se interrumpa el acceso a los sistemas académicos de la UMNG, debido a una falla en el servidor principal, originada por la falta de mantenimiento preventivo en la infraestructura tecnológica.

Esta estructura facilita la evaluación, tratamiento y monitoreo del riesgo, al permitir una lectura clara y comprensible para todos los niveles de la organización.

En la formulación de un riesgo, es fundamental considerar tres elementos esenciales que permitan su adecuada comprensión y gestión: impacto, causa inmediata y causa raíz.

Impacto: Se refiere a las consecuencias negativas que puede generar la materialización del riesgo en los objetivos, servicios, activos, recursos, usuarios, procedimientos y actividades de los procesos, estrategias, proyectos o sistemas de gestión de la Universidad Militar Nueva Granada (UMNG).

Causa Inmediata: Representa los factores o circunstancias más evidentes y próximas que pueden detonar la ocurrencia del riesgo. Si bien contribuyen a su materialización, no necesariamente constituyen la causa principal.

Causa Raíz: Es el origen estructural o fundamental del riesgo. Representa el motivo principal, menos evidente y más profundo, por el cual el riesgo puede presentarse. La correcta identificación de la causa raíz es clave para diseñar estrategias de mitigación y definir controles eficaces.

Es obligatorio que cada riesgo identificado y priorizado incluya el "Impacto" y al menos una de las causas ("Inmediata" o "Raíz") para garantizar su trazabilidad y gestión efectiva.

Asimismo, en la medida de lo posible y según la tipología del riesgo, se deben formular riesgos alineados con los objetivos estratégicos de los procesos, estrategias, proyectos y sistemas de gestión. Estos riesgos deben ser gestionados de manera que se asegure, de forma razonable, el cumplimiento de las metas institucionales y la mitigación de impactos adversos.

2.4.2.2.3 Redacción de riesgos operativos de procesos y riesgos estratégicos

Los riesgos operativos y estratégicos asociados a los procesos y estrategias institucionales deben redactarse conforme a la estructura metodológica definida en el numeral anterior. Esta forma de redacción permite identificar claramente el impacto, la causa inmediata y la causa raíz de cada

riesgo, facilitando su monitoreo dentro del ciclo de mejora continua PHVA (Planear - Hacer - Verificar - Actuar), y su alineación con los planes de mejora institucional.

A continuación, se presentan ejemplos de riesgos estructurados según esta metodología, aplicables a diferentes procesos de la Universidad Militar Nueva Granada (UMNG):

Ejemplos de riesgos operativos de procesos

Proceso	Frase inicial	Impacto (¿Qué?)	Causa inmediata (¿Cómo?)	Causa raíz (¿Por qué?)
Gestión administrativa de bienes y servicios	Posibilidad de	Afectación económica	Por multas y sanciones del ente regulador	Debido a la 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 inejecución de actividades en los planes de acción derivados de auditoría de certificación	Provocado por limitaciones y alta rotación del 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 accesos y modificaciones no autorizadas en los sistemas de información institucionales	Generado por vulnerabilidades en el control de acceso y deficiencias en la gestión de permisos de usuarios
Servicios generales y de apoyo administrativo	Posibles	Pérdidas económicas	Por daños o deterioro en bienes (muebles) y equipos de oficina	Debido a carencia de recursos monetarios, personal y tiempo para los mantenimientos preventivos, correctivos y predictivos requeridos

Direccionamiento estratégico institucional	Posibles	Afectaciones a la imagen y gestión institucional	Por proyectos de inversión desarticulados de los objetivos estratégicos, misión y visión institucional	Debido a falta de capacitación, apropiación e interiorización de los directores de proyectos y sus equipos de trabajo

Una correcta formulación de riesgos no solo mejora su comprensión, sino que facilita:

- Su evaluación y priorización, en función de los impactos institucionales.
- La planificación de controles y medidas preventivas.
- El monitoreo continuo dentro del ciclo PHVA y su trazabilidad en plataformas institucionales como KAWAK.

Antes de registrar un riesgo, se recomienda verificar que cumpla con los siguientes criterios:

Criterio	Pregunta guía
Claridad	¿El riesgo se comprende fácilmente sin ambigüedades?
Especificidad	¿Se identifica claramente el evento, el área afectada y el origen del riesgo?
Medición	¿El impacto puede ser evaluado con indicadores o evidencias objetivas?
Relevancia	¿El riesgo tiene relación directa con los objetivos estratégicos o misionales?

2.4.2.2.4 Riesgos de Corrupción en Procesos Institucionales

La Universidad Militar Nueva Granada (UMNG), como institución pública de educación superior, reconoce que la transparencia, la ética y la integridad son pilares fundamentales para el cumplimiento de sus funciones misionales: la docencia, la investigación, la extensión y la proyección social. En ese sentido, se articula de manera decidida con el Programa de Transparencia y Ética Pública, en cumplimiento del Decreto 124 de 2016 y su Anexo Técnico, adoptando los lineamientos del Departamento Administrativo de la Función Pública (DAFP).

Esta articulación institucional trasciende el marco normativo, reflejándose en acciones orientadas a fortalecer la gobernanza universitaria, la confianza ciudadana, la rendición de cuentas y la prevención de prácticas indebidas. En este contexto, la UMNG implementa la **Gestión Integral de Riesgos de Corrupción** como un componente estratégico de su sistema institucional de gestión, permitiendo identificar, evaluar, prevenir, mitigar y monitorear los riesgos asociados a actos de corrupción, considerando las particularidades del entorno académico y su impacto en la misión institucional de

formar ciudadanos íntegros y comprometidos con el país.

Para la correcta identificación y redacción de riesgos de corrupción, se adopta la estructura metodológica definida por la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6* del DAFP, la cual se basa en los siguientes cuatro componentes clave:

Fuente: Elaboración Propia

- **Acción u omisión:** Hecho que representa un posible comportamiento indebido, ya sea por acción directa o por negligencia.
- **Uso del poder:** Capacidad del servidor público para incidir en decisiones, recursos o resultados institucionales.
- **Desviación de la gestión de lo público:** Inobservancia de la normativa, los principios del servicio público o los fines institucionales.
- **Beneficio privado:** Ganancia o ventaja obtenida personal o indebidamente, directa o indirectamente.

Esta metodología permite la redacción precisa de riesgos, que posteriormente son integrados al Mapa de Riesgos de Corrupción de la Universidad, junto con los controles institucionales, consultas participativas, y actividades de formación y sensibilización dirigidas a fortalecer una cultura de integridad.

Asimismo, la Universidad incorpora a su estrategia el cumplimiento del Sistema de Administración del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (SARLAFT/FP). Este modelo preventivo se aplica de forma proporcional a la naturaleza de la institución, con controles específicos orientados a evitar que las operaciones, actividades o canales de la Universidad sean utilizados como instrumentos para ocultar activos ilícitos o financiar actividades criminales. En este sentido, se promueve un enfoque de gestión de riesgos que también contempla la reputación institucional, la trazabilidad financiera y la seguridad jurídica.

A continuación, se presentan ejemplos de riesgos de corrupción redactados conforme a esta estructura, incluyendo algunos alineados específicamente con el Programa de Transparencia y Ética Pública y el Decreto 124 de 2016:

Ejemplos de Riesgos de Corrupción Redactados con Base en la Estructura del DAFP

Proceso	Explicación	Acción u omisión	Uso del poder	Desviación de la gestión de lo público	Beneficio privado

Gestión administrativa de bienes y servicios	Riesgo vinculado a un posible favorecimiento contractual por intereses personales.	Posibilidad de recibir o solicitar	Cualquier dádiva o beneficio	A nombre propio o de terceros	Para favorecer la adjudicación de un contrato
Divulgación de la producción académica	Riesgo asociado a conflictos de interés en la evaluación de publicaciones.	Selección de evaluadores académicos	Que emitan concepto favorable a una obra	Sin cumplimiento de criterios de imparcialidad	En beneficio de un funcionario o tercero
Servicios generales y de apoyo administrativo	Posible manipulación del proceso de contratación mediante incentivos personales.	Recibir dádiva	A nombre propio o de terceros	Favorecer a un proveedor de servicios	Generando sobrecostos o ventajas indebidas
Contratación docente (Decreto 124 de 2016)	Riesgo de designación de personal sin méritos académicos ni proceso de selección claro.	Designar sin evaluación objetiva	Intervenir en procesos de selección	Sin acatar los lineamientos de mérito y transparencia	Favorecer a personas cercanas o recomendadas
Convenios de cooperación interinstitucional (Decreto 124 de 2016)	Riesgo de celebración de convenios sin verificación de idoneidad del aliado estratégico.	Omitir evaluación técnica y jurídica	Firmar convenios sin soporte objetivo	En contravía de la normativa y principios de contratación	Obtener beneficios económicos o políticos
Movilidad internacional (Decreto 124 de 2016)	Riesgo de asignación de becas o pasantías sin criterios de equidad.	Alterar criterios de selección	Usar influencia para beneficiar candidatos	Contravenir los principios de igualdad de oportunidades	Favorecer indebidamente a familiares o allegados

Con esta estrategia integral, la Universidad Militar Nueva Granada reafirma su compromiso con una gestión ética, segura y transparente, alineada con los estándares nacionales e internacionales, y se posiciona como un referente institucional en la prevención de riesgos de corrupción en la educación superior.

2.4.2.2.5. 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.

Estructura de redacción para riesgos de proyectos:

Fuente: Elaboración Propia

Conforme a la metodología PMBOK (Project Management Body of Knowledge), los riesgos en proyectos pueden impactar las siguientes variables:

- Costo: Representa el presupuesto necesario para ejecutar las actividades del proyecto.
- Tiempo: Hace referencia al cronograma y plazos previstos.
- Alcance: Incluye los productos, servicios o resultados finales del proyecto.
- Calidad: Asegura la conformidad con los requisitos establecidos y la adecuación para el uso.

Subtipologías de riesgos aplicables a proyectos: Los riesgos en proyectos pueden categorizarse en las siguientes subtipologías:

Subtipología	Descripción
Administrativos o de gestión	Relacionados con la planificación, ejecución y control de los proyectos, afectando áreas como gestión contractual, financiera, estructura organizacional y normatividad interna.
Técnicos u operacionales	Impactan el alcance, tiempo, costo o calidad del proyecto debido a deficiencias en procesos técnicos, tecnología, recursos o requisitos mal definidos.
Externos (naturales, socioculturales, regulatorios)	Provienen de fuentes externas a la Universidad y pueden afectar la ejecución del proyecto, incluyendo cambios normativos, desastres naturales, problemas de infraestructura o conflictos sociales.

A continuación, se presentan ejemplos de riesgos en proyectos alineados con la estructura metodológica propuesta en la Universidad Militar Nueva Granada (UMNG), aplicables en proyectos de inversión, extensión, investigación y regalías.

Subtipología de Riesgo	Componente Amenazado	Amenaza (Causa)	Consecuencia (Impacto)
Administrativo o de gestión	Entregables y actividades	Retrasos en la transferencia de recursos financieros.	Desfase del cronograma general y afectación del cumplimiento de hitos del proyecto.
Administrativo o de gestión	Metas y actividades	Insuficiencia o alta rotación del personal encargado de la ejecución.	Retrasos en la ejecución y posible incumplimiento de los resultados esperados.

Administrativo o de gestión	Actividades y productos	Falta de apropiación de herramientas tecnológicas para la gestión del proyecto.	Reducción en la eficiencia operativa y errores en la ejecución técnica del proyecto.
Técnico u operacional	Metas y productos	Uso inadecuado o desconocimiento de herramientas tecnológicas.	Baja calidad en los entregables y necesidad de reprocesos.
Técnico u operacional	Entregables y activos	Fallas del contratista o proveedor.	Incumplimiento en los tiempos de entrega o calidad inferior a lo requerido.
Externo	Activos y recursos	Hurto de equipos, herramientas o materiales por parte de terceros.	Pérdida de recursos esenciales y suspensión temporal de las actividades del proyecto.
Externo	Metas y entregables	Fenómenos naturales (lluvias intensas, deslizamientos, sismos, etc.).	Daños a infraestructura, retrasos prolongados o pérdida parcial del avance del proyecto.
Externo	Actividades y entregables	Fallas en servicios esenciales (energía eléctrica, conectividad, etc.).	Interrupción de las actividades y desajuste en el cronograma operativo.

2.4.2.2.6 Recomendaciones para la Correcta Redacción de Riesgos

Una redacción clara y estructurada de los riesgos es esencial para garantizar su comprensión, monitoreo y tratamiento adecuado. Al formular un riesgo, se deben evitar confusiones comunes que comprometen su utilidad dentro del Sistema de Gestión Institucional. A continuación, se presentan recomendaciones clave para evitar errores frecuentes al momento de redactar riesgos de cualquier tipología:

I. No describir como riesgos las omisiones, desviaciones o negaciones de controles.

Los siguientes ejemplos son incorrectos porque describen la ausencia de controles, no un riesgo como tal:

- 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 por debilidades en procedimientos y actividades asociadas.
- Ausencia de controles de acceso que garanticen la confidencialidad e integridad de la información.

II. No redactar causas como si fueran riesgos.

Las causas son elementos que deben analizarse para entender el riesgo, pero no son riesgos en sí mismos:

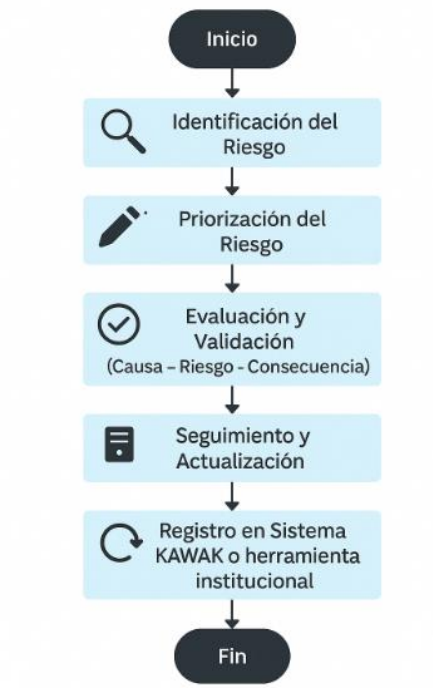
- Inadecuado funcionamiento de la plataforma estratégica.
- Debilidades en la articulación de procedimientos académico-administrativos.

III. Evitar clasificar riesgos como “transversales”; lo que puede ser transversal son sus causas.
Ejemplos de causas transversales:

- Pérdida de información en medios físicos o digitales.
- Limitaciones o alta rotación de personal de planta o contratista.
- Ausencia de normatividad o políticas para la gestión de procesos.

IV. No confundir riesgos con problemas, hallazgos o no conformidades.
Los riesgos tienen un carácter potencial, mientras que los problemas ya están materializados.

Diagrama de flujo



Fuente: Elaboración Propia

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 el 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.

Ejemplos de Causas de Riesgos en la Institución

Tipo	Categoría	Definición	Ejemplos de Causas de Riesgos
Interna	**Personal**	Factores relacionados con el desempeño, comportamiento o condiciones del personal.	Falta de personal capacitado, alta rotación de empleados, condiciones de estrés laboral, actos de fraude interno, gestión ineficaz del talento humano.

	Infraestructura y Activos	Eventos relacionados con las instalaciones y bienes de la institución.	Deterioro de instalaciones, obsolescencia de equipos, mantenimiento inadecuado, exposición a riesgos físicos como incendios o inundaciones.
	Procesos	Debilidades en procedimientos y ejecución de actividades.	Procesos mal definidos, deficiencias en los procedimientos de liquidación que generan errores en cálculos de pagos, fallos en la trazabilidad de documentos, falta de articulación con proveedores.
	Tecnología	Problemas con la infraestructura tecnológica y de comunicación.	Interrupciones en el servicio de red, fallas recurrentes de software o hardware, ausencia de actualizaciones, vulnerabilidades en ciberseguridad.
	Estructura Organizacional	Factores relacionados con el organigrama y la gestión institucional.	Duplicidad de funciones, falta de articulación entre dependencias, toma de decisiones centralizada, estructura rígida.
	Cultura Organizacional	Factores relacionados con la forma en que se trabaja en la institución.	Ausencia de liderazgo transformacional, débil apropiación de valores institucionales, resistencia al cambio, baja motivación interna.
	Económicos	Disponibilidad y uso de los recursos financieros.	Insuficiencia presupuestal, planificación financiera deficiente, ejecución inadecuada del gasto, acumulación de deudas.
	Normas y Directrices	Cumplimiento y aplicación de normativas internas.	Desactualización de manuales y políticas, desconocimiento de procedimientos, falta de socialización de reglamentos institucionales.

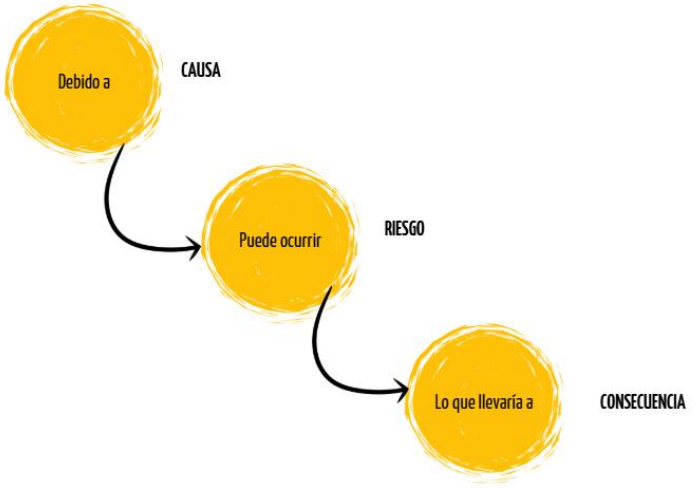
Ejemplos de Consecuencias Asociadas a los Riesgos

Los riesgos identificados pueden generar diversas consecuencias que afectan los procesos, estrategias, proyectos y sistemas de gestión de la institución. A continuación, se presentan algunos ejemplos de estas posibles afectaciones:

Categoría	Ejemplos de Consecuencias
Financieras	Pérdidas económicas, insostenibilidad financiera, sobrecostos.
Legales y Normativas	Incumplimientos normativos internos o legales externos, sanciones, llamados de atención, procesos judiciales.
Operacionales	Reprocesos, afectaciones en la ejecución de actividades, incumplimientos en cronogramas, ajustes en el alcance de proyectos.

Reputacionales	Afectaciones a la imagen institucional a nivel interno y externo, disminución de la confianza de la comunidad universitaria y stakeholders.
Académicas y Científicas	Impacto en la calidad educativa, disminución en la producción científica, afectación a proyectos de investigación.
Sociales y de Gobernanza	Impactos en la gobernabilidad y gobernanza institucional, insatisfacción de grupos de interés, incremento de quejas y reclamos.
Seguridad y Bienestar	Daños a la integridad física de personas, afectaciones a la infraestructura y tecnología, pérdida de información, afectación del bienestar general.
Tecnológicas y de Información	Pérdida de datos, vulnerabilidad en la confidencialidad, integridad y disponibilidad de la información.
Competitividad y Sostenibilidad	Reducción de la competitividad institucional, disminución de oportunidades de alianzas estratégicas, impactos en el desarrollo sostenible.

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:



Fuente: Elaboración Propia

Los responsables de la segunda línea de defensa serán quienes faciliten e instruyan 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.

2.4.3. Análisis de riesgos

El análisis de riesgos es una fase fundamental de la gestión del riesgo que permite evaluar la gravedad y posibles consecuencias de los eventos que pueden afectar a la Universidad Militar Nueva Granada (UMNG). Este análisis considera tanto la **probabilidad** de ocurrencia como el **impacto** que tendría la materialización del riesgo.

Para lograr un análisis más completo y estratégico, se deben tener en cuenta dos momentos clave:

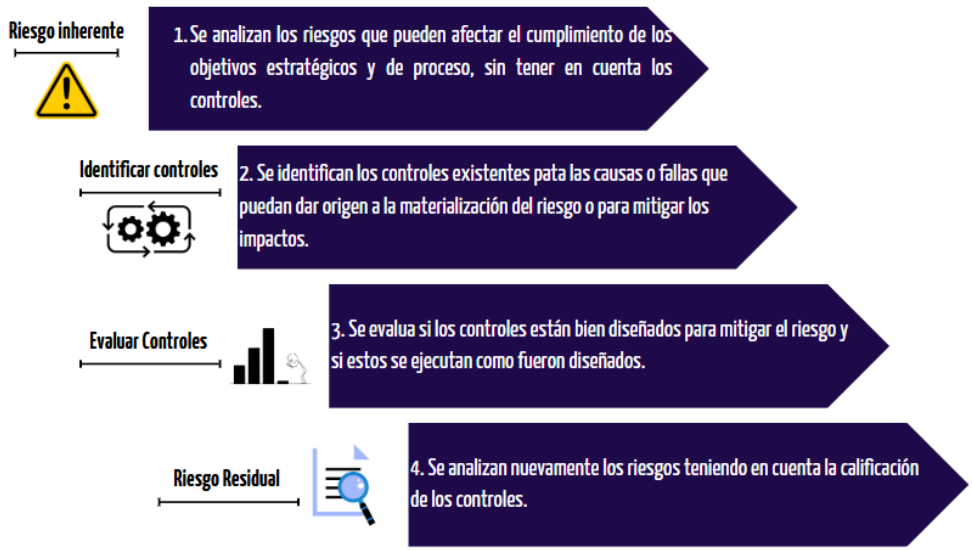
- **Riesgo Inherente:** Es el nivel de riesgo que se presenta antes de aplicar cualquier medida de control. Representa la exposición natural al riesgo, considerando solo el entorno y la operación normal de los procesos o actividades.
- **Riesgo Residual:** Es el nivel de riesgo que permanece después de aplicar los controles diseñados para prevenir o mitigar el riesgo. Refleja el riesgo real al que está expuesta la Universidad considerando las medidas actuales.

Ejemplo:

En un proceso de contratación pública, un riesgo inherente podría ser la "posibilidad de adjudicar un contrato a un proveedor no idóneo por falta de verificación en requisitos legales".

Si la UMNG implementa controles como listas de chequeo y validación jurídica previa, el riesgo residual correspondería a la probabilidad e impacto que permanece aún con estos controles aplicados.

Análisis antes (riesgo inherente) y después de controles (riesgo residual)



Análisis de Riesgo: Antes (Inherente) y Después (Residual)

En esta etapa, se califican los riesgos de acuerdo con parámetros de probabilidad e impacto que, combinados, determinan el nivel de riesgo. Estos resultados permiten ubicar cada riesgo en un mapa de calor y determinar si es aceptable, tolerable o inaceptable, en función de la capacidad de riesgo definida por la UMNG.

Este análisis depende de la información recopilada en la fase de identificación y se complementa con la experiencia de los responsables del proceso, proyecto o estrategia involucrados.

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 UMNG calificará sus diferentes tipologías de riesgo utilizando los siguientes parámetros.

La probabilidad de ocurrencia de un riesgo puede determinarse utilizando tres criterios principales:

1. Frecuencia de Materialización del Riesgo: Se mide con base en el número de veces que el riesgo se ha presentado en el pasado dentro de un periodo determinado.
2. Frecuencia de Ejecución de la Actividad: Se usa cuando no se cuenta con registros previos del riesgo, pero sí con información sobre la recurrencia de la actividad que podría generarlo.
3. Factibilidad: Se emplea cuando no existen datos históricos, pero sí indicios o condiciones que podrían propiciar su ocurrencia. En este caso, la probabilidad se mide en función del conocimiento y percepción del evaluador.

Cada tipología de riesgo tiene características particulares, por lo que se definen diferentes escalas de probabilidad según corresponda, en las siguientes tablas se presenta la forma de obtener el nivel de probabilidad:

2.4.3.1. Parámetros de Probabilidad

Para los Riesgos de Procesos, 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.

Valor	Nivel	Frecuencia de Materialización	Frecuencia de la Actividad	Factibilidad
1	**Raro**	No se ha presentado en los últimos 5 años.	La actividad se ejecuta máximo 2 veces por año.	Solo ocurre en circunstancias excepcionales. Probabilidad muy baja.
2	**Improbable**	Se ha presentado al menos una vez en los últimos 5 años.	Se ejecuta entre 3 y 24 veces por año.	Puede ocurrir en algún momento. Probabilidad baja.
3	**Posible**	Se ha presentado al menos una vez en los últimos 2 años.	Se ejecuta entre 25 y 499 veces por año.	Podría ocurrir en algún momento. Probabilidad media.
4	**Probable**	Se ha presentado al menos una vez en el último año.	Se ejecuta entre 500 y 5,000 veces por año.	Probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.
5	**Casi seguro**	Se ha presentado más de una vez al año.	Se ejecuta más de 5,000 veces por año.	Se espera que ocurra en la mayoría de las circunstancias. Probabilidad muy alta.

Probabilidad para Riesgos Estratégicos

Para riesgos estratégicos, se analiza su probabilidad considerando un periodo de seis años, acorde con la duración de los planes estratégicos y el periodo rectoral.

Valor	Nivel	Factibilidad	Frecuencia de Materialización

1	**Raro**	Ocurre solo en circunstancias excepcionales. Probabilidad muy baja.	No se ha presentado en los últimos 6 años.
2	**Improbable**	Puede ocurrir en algún momento. Probabilidad baja.	Se ha presentado al menos una vez en los últimos 6 años.
3	**Posible**	Podría ocurrir en algún momento. Probabilidad media.	Se ha presentado al menos una vez en los últimos 3 años.
4	**Probable**	Probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.	Se ha presentado al menos una vez en el último año.
5	**Casi seguro**	Se espera que ocurra en la mayoría de las circunstancias. Probabilidad muy alta.	Se ha presentado más de una vez al año.

Probabilidad para Riesgos en Proyectos

El análisis de la probabilidad en proyectos está limitado a su ciclo de vida, considerando la cantidad de veces que podría ocurrir el riesgo dentro del proyecto.

Valor	Nivel	Factibilidad	Frecuencia de Ocurrencia en el Proyecto[2]
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] 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.

2	**Improbable**	El evento puede ocurrir en algún momento. Probabilidad baja. Ocurre en pocos proyectos.	Puede ocurrir máximo una vez durante el proyecto. 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.

Probabilidad para Riesgos Ambientales

Los riesgos ambientales pueden evaluarse según la frecuencia con la que han ocurrido en los últimos cinco años y su probabilidad de ocurrencia futura.

Valor	Nivel	Frecuencia
1	**Raro**	Ocurre solo en circunstancias excepcionales. No ha ocurrido en los últimos 5 años.
2	**Improbable**	Puede ocurrir en algún momento. Se ha presentado al menos una vez en los últimos 5 años.
3	**Posible**	Podría ocurrir en algún momento. Se ha presentado al menos una vez en los últimos 2 años.
4	**Probable**	Probablemente ocurrirá en la mayoría de los casos. Se ha presentado al menos una vez en el último año.

5	**Casi seguro**	Se espera que ocurra con alta frecuencia. Se ha presentado más de una vez al año.

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, se cuenta con diferentes tablas para obtener el nivel de impacto que se aprecian a continuación.

Parámetros de Impacto para Riesgos de Procesos – Operativos

Valor	Nivel	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 reducido de usuarios	Interrupción de las operaciones de la Universidad	Imagen o credibilidad institucional afectada localmente	Acciones por parte de los entes de control internos o externos que pueden incluir	Pérdidas económicas moderadas

			por un (1) día		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.	
10	Mayor	Afectación en la ejecución del proceso que repercute en una parte considerable de los usuarios	Interrupción de las operaciones de la Universidad por más de (2) dos días	Imagen o credibilidad de la Universidad afectada en la región	Acciones por parte de los entes de control internos o externos que incluyen sanciones medianas.	Pérdidas económicas mayores
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

Parámetros de Impacto para Riesgos de Corrupción

El nivel de impacto en los riesgos de corrupción 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 V6" que se muestra a continuación.

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***.			

Fuente: Guía de Riesgos DAFP

Con base en los resultados obtenidos a partir de la aplicación de la tabla anterior, se establece una clasificación del impacto en función del número de respuestas afirmativas. Esta clasificación permite medir el grado de afectación que la materialización del riesgo de corrupción puede generar en la entidad, considerando aspectos como la reputación institucional, la estabilidad financiera, el cumplimiento de la misión y la afectación a terceros:

Valor	Nivel	Criterios de Evaluación
1	Insignificante	No hay respuestas afirmativas en el test de impacto de corrupción (DAFP).
2	Menor	1-2 respuestas afirmativas en el test de impacto de corrupción (DAFP).
5	Moderado	3-5 respuestas afirmativas en el test de impacto de corrupción (DAFP).
10	Mayor	6-11 respuestas afirmativas en el test de impacto de corrupción (DAFP).

20	Catastrófico	12-19 respuestas afirmativas o respuesta positiva en la pregunta sobre pérdida de vidas humanas.

Parámetros de Impacto para Riesgos Estratégicos

Los riesgos estratégicos pueden generar consecuencias significativas en la gestión y sostenibilidad de la entidad, afectando su reputación, recursos financieros y el cumplimiento de su misión institucional. Para evaluar su impacto, se establecen niveles de afectación con base en variables como la pérdida económica y el daño reputacional, permitiendo una gestión efectiva y oportuna de los riesgos identificados.

Valor	Nivel	Pérdida Económica	Reputación/Imagen
1	Insignificante	< 0.002 % del presupuesto (funcionamiento + inversión) Afectación entre ≤ 40 SMMLV.	Afectación mínima en un área.
2	Menor	0.002 % - 0.01 % del presupuesto (funcionamiento + inversión) Afectación entre 40-200 SMMLV.	Afectación interna con impacto en grupos de interés.
5	Moderado	0.01 % - 0.05 % del presupuesto (funcionamiento + inversión) Afectación entre 200-1000 SMMLV.	Imagen afectada con impacto en objetivos estratégicos.
10	Mayor	0.05 % - 0.1 % del presupuesto (funcionamiento + inversión) Afectación entre 1000-2000 SMMLV.	Imagen afectada con impacto mediático regional.
20	Catastrófico	> 0.1 % del presupuesto (funcionamiento + inversión) Afectación > 2000 SMMLV.	Crisis de reputación con impacto nacional/internacional.

Parámetros de Impacto para Riesgos en 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.

Valor	Nivel	Costo	Tiempo	Alcance	Calidad
1	Insignificante	Variación < 1 %.	Retraso ≤ 1 mes.	Afectación mínima (≤ 1 % del avance).	Impacto imperceptible.
2	Menor	Variación 1 %-5 %.	Retraso de 1-2 meses.	Afectación leve (1 %-5 % del avance).	Ajustes menores.

5	Moderado	Variación 5 %-10 %.	Retraso de 2-4 meses.	Afectación media (5 %-10 % del avance).	Ajustes significativos.
10	Mayor	Variación 10 %-20 %.	Retraso de 4-6 meses.	Afectación mayor (10 %-20 % del avance).	Entregables inaceptables, ajustes mayores.
20	Catastrófico	Variación > 20 %.	Retraso > 6 meses.	Afectación severa (> 20 % del avance).	Proyecto inviable, ajustes críticos.

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.

Valor	Nivel	Imagen	Legal	Objetivos Ambientales	Ambiente	Económico
1	Insignificante	Afecta solo al SGA.	Sin incumplimientos legales.	No afecta objetivos ambientales.	Impacto interno.	Pérdida ≤ 1 % del presupuesto del SGA.
2	Menor	Afecta la sede.	No aplica.	No aplica.	No aplica.	Pérdida 1 %-3 % del presupuesto del SGA.
5	Moderado	Afecta la Alta Dirección de la sede.	No aplica.	No aplica.	No aplica.	Pérdida 3 %-5 % del presupuesto del SGA.
10	Mayor	Afecta la sede a nivel general.	Sanciones de autoridad ambiental.	No aplica.	Impacto en comunidades vecinas.	Pérdida 5 %-10 % del presupuesto del SGA.
20	Catastrófico	Impacto en todas las sedes de la universidad.	Suspensión de actividades por la autoridad ambiental.	Afectación a objetivos del SGA.	Impacto ambiental municipal/regional.	Pérdida ≥ 10 % del presupuesto del SGA.

2.4.3.3. Nivel de Riesgo Inherente, Nivel de Aceptabilidad y Mapa de Calor

El nivel de riesgo inherente, también conocido como riesgo puro, representa la valoración del riesgo antes de la aplicación de controles o medidas de mitigación. Su cálculo es fundamental para determinar la magnitud de los riesgos identificados y priorizados en el proceso de análisis del riesgo.

Existen dos métodos para obtener el nivel de riesgo inherente:

- **Cálculo matemático:** Multiplicando los valores asignados a los niveles de probabilidad e impacto, según la siguiente fórmula:

Nivel de Riesgo Inherente = Valor del Nivel de Probabilidad × Valor del Nivel de Impacto

- **Mapa de Calor:** Cruzando los valores de probabilidad e impacto en la matriz de riesgo (Mapa de Calor), lo que permite visualizar gráficamente la severidad del riesgo.

El valor del riesgo inherente surge de la interacción entre dos variables clave:

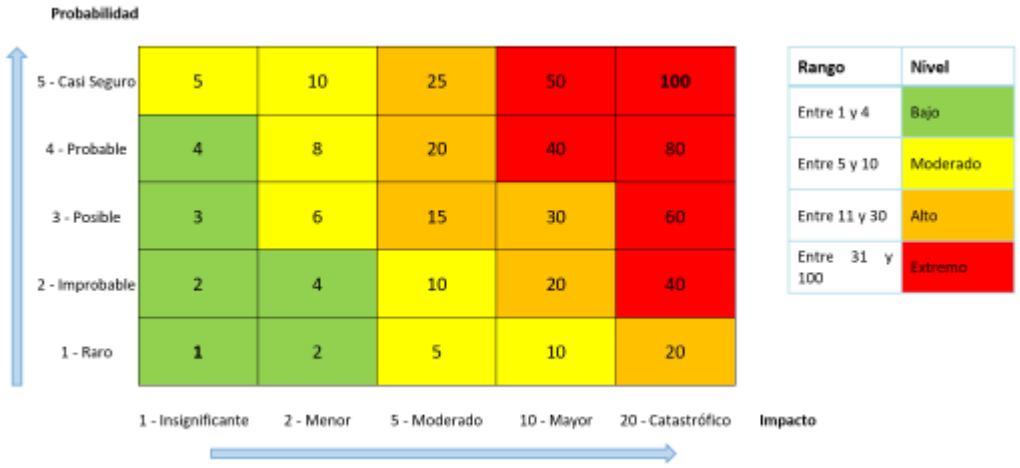
- **Probabilidad**: Representa la frecuencia o posibilidad de ocurrencia de un evento adverso.
- **Impacto**: Indica la magnitud de las consecuencias que tendría dicho evento sobre los objetivos institucionales.

Cuanto mayor sea la probabilidad y el impacto, más alto será el nivel de riesgo. Esta relación se expresa gráficamente en el Mapa de Calor, facilitando la clasificación y priorización de riesgos.

Independientemente del método utilizado, cada riesgo debe ser registrado con su valoración inherente en el Mapa de Calor correspondiente para facilitar su análisis y tratamiento.

Mapa de Calor

La UMNG ha definido dos Mapas de Calor para la valoración del nivel de riesgo inherente, según la tipología del riesgo:



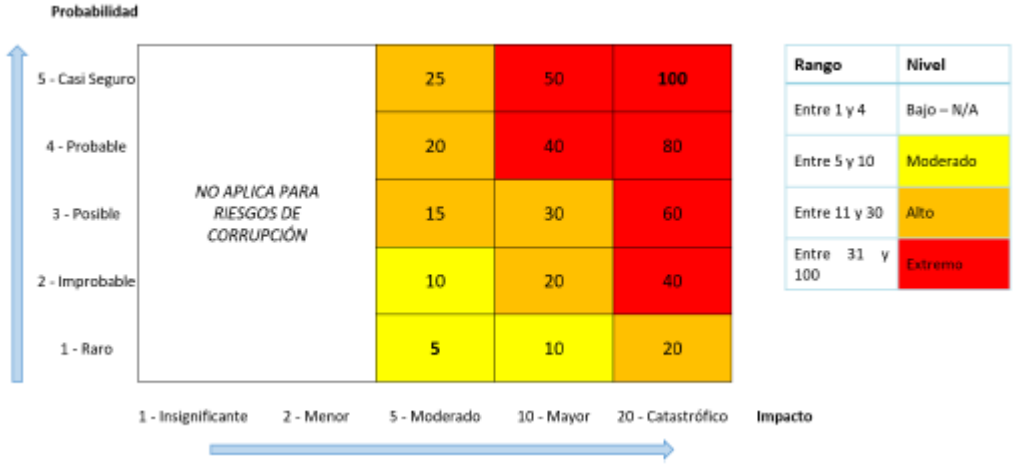
Este mapa contempla cinco niveles de probabilidad y cinco niveles de impacto, permitiendo clasificar los riesgos en niveles bajo, moderado, alto o extremo. Se utiliza para riesgos estratégicos, operativos, financieros, ambientales, de salud y otros que no estén relacionados con corrupción.

Mapa de Calor para Riesgos de Corrupción

Dado que, según la metodología de la Secretaría de Transparencia, los riesgos de corrupción no

pueden clasificarse con impactos "insignificantes" o "menores", el análisis se restringe a los niveles de impacto: moderado, mayor y catastrófico, y niveles de probabilidad de 1 (raro) a 5 (casi seguro). Por ello, se emplea un Mapa de Calor ajustado para esta tipología, en el cual solo se visualizan las combinaciones válidas.

Este enfoque diferenciado asegura que los riesgos de corrupción se analicen con criterios de severidad más altos, priorizando su control, reporte y mitigación efectiva.



- El nivel de riesgo inherente debe establecerse para todos los riesgos identificados en la etapa de "Identificación del Riesgo". Se calcula multiplicando el valor del nivel de probabilidad por el valor del nivel de impacto, o bien, ubicando estos valores en el Mapa de Calor.

- El nivel de riesgo inherente se determina sin considerar la existencia de mecanismos de control, reflejando el riesgo en su estado puro.

- Todos los riesgos identificados y priorizados, junto con su redacción, nivel de probabilidad, impacto y riesgo inherente, deben ser correctamente ubicados en el Mapa de Calor para su visualización y análisis.

- Las acciones y opciones de tratamiento de cada riesgo se definen en la etapa de "Tratamiento del Riesgo" (numeral 2.4.5), una vez se haya determinado el nivel de riesgo residual, el cual sirve como referencia para seleccionar la estrategia de mitigación más adecuada.

2.4.3.4. Análisis preliminar (riesgo inherente)

El análisis preliminar tiene como propósito determinar los niveles de severidad del riesgo a través de la combinación entre la **probabilidad de ocurrencia** y el **impacto potencial**, antes de implementar medidas de control. Esta combinación permite clasificar el riesgo dentro de las **zonas de severidad** definidas en la matriz de calor institucional, las cuales orientan la priorización en la gestión de riesgos.

Ejemplo (continuación):

Proceso: gestión de recursos

Objetivo: adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

Evaluación del riesgo inherente

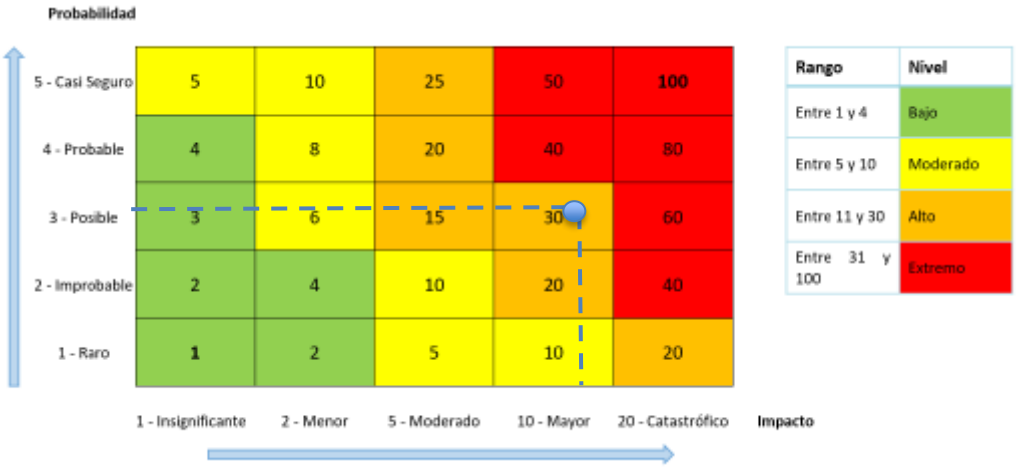
Probabilidad inherente:

- **Valor:** 3
- **Nivel:** Posible
- **Justificación:** El evento se ha presentado al menos una vez en los últimos dos años.

Impacto inherente:

- **Valor:** 10
- **Nivel:** Mayor
- **Justificación:**
    - La pérdida económica proyectada supera el 0.05 % y hasta el 0.1 % del presupuesto total (funcionamiento + inversión).
    - La afectación estimada oscila entre 1.000 y 2.000 SMMLV.
    - Desde el punto de vista reputacional, se prevé una afectación institucional con repercusión mediática a nivel regional.

Al ubicar la combinación de los valores asignados a probabilidad (3) e impacto (10) en la matriz de calor, el riesgo se localiza en el cuadrante 30, correspondiente a una zona de alta severidad. Este resultado evidencia la necesidad de definir e implementar controles específicos orientados a la mitigación del riesgo identificado.



Nivel de Aceptabilidad

El nivel de aceptabilidad permite clasificar la gravedad del riesgo, tanto en su estado inherente como en su estado residual (tras la implementación de controles). Se obtiene al ubicar el cruce de probabilidad e impacto en el Mapa de Calor o mediante la clasificación de la multiplicación de ambos valores:

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

			- Otras acciones obligatorias
			- Definir los KRI's
			- Reportar a la instancia correspondiente

Cada nivel de riesgo requiere diferentes estrategias de tratamiento, las cuales deben definirse en la etapa de Valoración del Riesgo, asegurando que la gestión de riesgos sea efectiva y acorde con la exposición que representa para la institución.

2.4.4. Tratamiento de los Riesgos

El tratamiento de los riesgos es una fase esencial dentro del proceso de gestión, ya que permite definir e implementar medidas para minimizar su impacto y reducir su probabilidad de ocurrencia. A partir del análisis y la valoración de los riesgos, se establece que no todos poseen el mismo nivel de criticidad y exposición. Por ello, es fundamental priorizar su gestión, asignando recursos de manera eficiente y asegurando que los controles existentes sean adecuados.

Para abordar esta gestión, se han definido dos acciones clave:

- Definición de la medida de tratamiento: Determinar la estrategia más adecuada para gestionar el riesgo, considerando su impacto y probabilidad.
- Establecimiento de planes de acción: Diseñar e implementar medidas concretas que permitan reducir la exposición al riesgo o mitigar sus efectos en caso de materialización.

2.4.4.1. Definición de la Medida de Tratamiento.

Una vez evaluados los riesgos, se deben establecer las medidas más apropiadas para su tratamiento. La selección de estas estrategias debe realizarse con base en el contexto institucional, el tipo y magnitud del riesgo, así como los recursos disponibles para su implementación. Asimismo, se debe tener en cuenta el principio de costo-beneficio, asegurando que el esfuerzo y los recursos invertidos en su mitigación sean justificados en función de las pérdidas potenciales que podrían derivarse de su materialización.

Dado que la gestión del riesgo es un proceso dinámico, el tratamiento debe ser continuo y ajustable según los cambios en el entorno, la evolución de los procesos, la disponibilidad de nueva información y los resultados de monitoreo. La efectividad de cada medida de tratamiento debe ser revisada periódicamente para asegurar su vigencia y eficacia, y ajustada cuando se identifiquen desviaciones o nuevas amenazas.

Las estrategias de tratamiento incluyen las siguientes acciones:

- **Reducir el riesgo:** Implementación de controles, acciones preventivas y medidas correctivas para disminuir la probabilidad de ocurrencia o el impacto del riesgo.
- **Transferir o compartir el riesgo:** Desplazar la responsabilidad del riesgo total o parcialmente mediante mecanismos como seguros, contratos, convenios de colaboración o acuerdos con terceros.
- **Aceptar el riesgo:** Asumir el riesgo cuando su impacto es mínimo o cuando la

implementación de controles no es viable o no se justifica económicamente. Esta decisión debe estar documentada y alineada con el nivel de tolerancia definido por la institución.

- **Evitar el riesgo:** Eliminar la causa del riesgo mediante la suspensión, rediseño o reemplazo de la actividad, proceso o práctica que genera la exposición al riesgo.

2.4.4.2. Niveles de Aceptabilidad y Medidas de Tratamiento

Los riesgos identificados y analizados deben ubicarse en un Mapa de Calor, que permite clasificar su nivel de aceptabilidad en función de la combinación entre su impacto y su probabilidad de ocurrencia. Esta valoración se realiza utilizando una matriz de riesgo cualitativa basada en una escala numérica del 1 al 100, producto de multiplicar los valores asignados a los niveles de probabilidad (de 1 a 5) por los niveles de impacto (de 1 a 20). Esta escala ha sido definida por la Universidad Militar Nueva Granada en el marco del Modelo Integral de Gestión del Riesgo (MIGR), y está alineada con metodologías reconocidas como la Guía para la Administración del Riesgo del DAFP (2022) y la norma ISO 31000:2018.

La interpretación de los puntajes obtenidos se agrupa en los siguientes rangos:

- **Bajo (1-4 puntos):** Los riesgos en este nivel son considerados aceptables con los controles actuales. No requieren medidas adicionales más allá de su monitoreo regular para verificar que su nivel de exposición no se incremente.

- **Moderado (5-10 puntos):** Representan riesgos tolerables, pero cercanos al límite de la capacidad de aceptación definida por la UMNG. Se recomienda reforzar los controles existentes o implementar medidas adicionales si se evidencia una tendencia al alza en su evolución.

- **Alto (11-30 puntos):** Son riesgos significativos que superan la capacidad de aceptación de la institución. Requieren medidas de mitigación prioritarias, así como un seguimiento estricto y frecuente. Su gestión debe ser reportada a los niveles directivos correspondientes.

- **Extremo (31-100 puntos):** Corresponden a riesgos inaceptables por su alto potencial de impacto negativo. Exigen acciones inmediatas y correctivas, que pueden incluir la reestructuración de procesos, la implementación de controles robustos o incluso la suspensión temporal o definitiva de las actividades que generan el riesgo.

Cada nivel de aceptabilidad se vincula con diferentes estrategias de tratamiento, las cuales deben definirse considerando el contexto institucional, la criticidad del riesgo y la disponibilidad de recursos. Estas decisiones deben documentarse debidamente y estar sujetas a revisión periódica como parte del ciclo de mejora continua de la gestión del riesgo.

2.4.4.3. Identificación y Evaluación de Controles

Los controles son mecanismos implementados para modificar los riesgos, ya sea reduciendo su

probabilidad de ocurrencia o mitigando sus impactos una vez materializados. Su adecuada identificación, evaluación e integración son claves para garantizar una gestión eficaz del riesgo en la Universidad Militar Nueva Granada (UMNG).

Para su identificación, se deben considerar atributos clave como la eficiencia, eficacia, oportunidad, operatividad, viabilidad técnica, apego jurídico y su relación costo-beneficio. Además, su efectividad real debe evaluarse continuamente, no solo su existencia formal, como parte del ciclo de mejora continua institucional.

Los controles pueden agruparse en tres categorías principales:

1. Controles Administrativos

Actúan sobre la organización y el cumplimiento de normas, procedimientos y responsabilidades. Ejemplos:

- Aplicación de procedimientos operativos, manuales, guías e instructivos institucionales.
- Establecimiento de la segregación de funciones.
- Verificación sistemática de firmas y autorizaciones requeridas.
- Revisión y aprobación de decisiones por niveles jerárquicos superiores.
- Monitoreo del cumplimiento de cronogramas y planes de trabajo.
- Elaboración, análisis y seguimiento de informes de gestión.
- Ejecución de auditorías internas o externas.

2. Controles Tecnológicos

Enfocados en proteger la infraestructura digital y garantizar la seguridad de la información. Ejemplos:

- Uso de mecanismos de control de acceso físicos (lectores biométricos) y digitales (autenticación por perfiles).
- Activación de alertas generadas por sistemas de información como mecanismos preventivos.
- Realización de copias de seguridad (backup) o respaldos de información.
- Implementación de niveles jerárquicos de autorización en plataformas digitales.

3. Controles Operativos

Dirigidos a la ejecución de actividades críticas en los procesos misionales, administrativos o de apoyo. Ejemplos:

- Programas de capacitación y entrenamiento.
- Listas de verificación (checklists) para actividades clave.
- Mantenimiento preventivo y correctivo de equipos o infraestructura.
- Análisis de indicadores de desempeño o control.
- Autoevaluaciones para identificar brechas o debilidades.

- Confrontación y conciliación de información para detectar errores.
- Planes de contingencia ante escenarios críticos.

Adicionalmente, se destaca la importancia de integrar estos controles en la cultura organizacional de la UMNG. Esto se logra mediante procesos de sensibilización, capacitación y apropiación por parte del personal, promoviendo un enfoque proactivo en la prevención y mitigación de riesgos.

La actualización periódica de los controles es indispensable, considerando los cambios en el entorno, en la estructura institucional, los avances tecnológicos y las lecciones aprendidas. Por tanto, los controles deben formar parte de un sistema vivo que evoluciona junto con los procesos y objetivos de la universidad.

2.4.4.4. 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 a continuación:

Evaluación del Riesgo Residual

Luego de implementar controles, se obtiene el nivel de riesgo residual, es decir, el riesgo que persiste tras aplicar las medidas correctivas. Este se compara con los niveles de tolerancia definidos por la institución para determinar si se requiere una acción adicional o si el riesgo puede ser aceptado.

En casos donde los controles no sean suficientes, se debe considerar la escalabilidad del riesgo a niveles superiores dentro de la institución. El riesgo debe ser escalado al Comité de Gestión y Desempeño o al Equipo Técnico de Identificación y Respuesta (ETIR), quienes evaluarán alternativas adicionales de tratamiento o medidas estratégicas de mitigación o cuando se cumpla al menos uno de los siguientes criterios:

1. Persistencia del riesgo después de aplicar controles y medidas correctivas, sin reducción significativa del nivel de riesgo residual.
2. Impacto residual clasificado como “Extremo”, incluso tras implementar controles efectivos.
3. Ausencia de controles viables debido a limitaciones técnicas, legales o estructurales.
4. Necesidad de intervención estratégica o recursos extraordinarios para su mitigación (cambio normativo, reestructuración, inversión adicional).
5. Afectación a procesos críticos o estratégicos de la Universidad (académicos, financieros, administrativos, misionales).
6. Recomendación de auditoría o entes de control externo que sugieran su revisión a nivel superior.

Característica	Descripción
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.

Identificación de Controles – Atributos Informativos

La correcta identificación de controles de probabilidad e impacto es fundamental para la gestión de riesgos, ya que permite minimizar tanto la ocurrencia como las consecuencias de los eventos adversos. Para ello, cada riesgo debe contar con al menos dos o tres controles: uno orientado a mitigar el impacto y uno o dos dirigidos a reducir la probabilidad de ocurrencia, ya sea actuando sobre la causa inmediata o sobre la causa raíz.

Es posible que, en algunos casos, el mismo mecanismo de control pueda aplicarse tanto a la causa inmediata como a la causa raíz. Sin embargo, existen ciertos riesgos en los que no es factible implementar controles de probabilidad o de impacto. Por ejemplo, en los riesgos asociados a fenómenos naturales como terremotos o erupciones volcánicas, no se pueden prevenir las causas mediante controles de probabilidad. De igual forma, en los riesgos de corrupción, la reglamentación del Departamento Administrativo de la Función Pública (DAFP) establece que no se pueden asignar controles de impacto.

Cuando no sea posible establecer un control de probabilidad o impacto para un riesgo específico, se

debe justificar claramente la razón e informar al responsable de la segunda línea de defensa de la tipología correspondiente. Esta instancia evaluará el caso y determinará la acción a seguir, que podría incluir su monitoreo, escalamiento al Comité de Gestión y Desempeño para su evaluación y asesoramiento.

Luego de identificar los posibles controles de un riesgo, se debe establecer para cada control los atributos informativos que se muestran a continuación:

Atributo	Descripción	Ejemplo UMNG
Código	Identificador único que permite diferenciar el control de un riesgo de cualquier otro control.	345
Nombre	Nombre asignado al control; se sugiere en su redacción que este tenga implícita una acción acompañada de un sustantivo.	Respaldo periódico de bases de datos institucionales
Responsable	Funcionario, dependencia, procesos, sistema, tecnología o área encargada de su implementación.	Coordinador de Seguridad de la Información
Objetivo (¿Qué hace?)	Establece para qué se realiza la actividad del control.	Garantizar la integridad y disponibilidad de la información institucional.
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. A través del sistema de respaldo, se genera una copia de seguridad. 2. La copia es probada en un entorno de pruebas. 3. La copia se almacena en el servidor seguro de la UMNG. Desviaciones: 1. Si la copia falla, se repite el procedimiento. 2. Si persiste el error, se reporta a 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.	01/03/2024
Variable que reduce	Variable 'Probabilidad' (causa inmediata y/o raíz) o 'Impacto' que se espera combatir con el control.	Impacto: Pérdida de información crítica.
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.	Sí, definido en la Política de Respaldo de Información de la UMNG, código UMG.SEG.004.
Tipo de evidencia	Define cuál es el soporte de la ejecución del control que permita validar en algún momento la eficacia de su implementación.	Archivo de respaldo almacenado en servidor seguro y registro en el sistema de gestión de información.

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.

2.4.4.5. Escritura de los controles

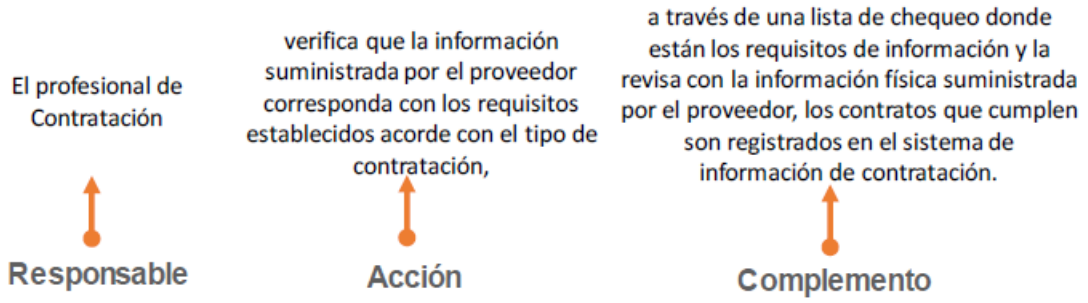
Para garantizar una redacción clara, coherente y útil en el análisis y valoración de los controles, se recomienda adoptar una estructura estandarizada que permita identificar los elementos esenciales de cada control y su funcionalidad en la gestión del riesgo.
La estructura propuesta incluye los siguientes componentes:

- **Responsable de ejecución del control:** Corresponde al cargo del servidor público que ejecuta directamente la acción del control. En el caso de controles automáticos, se especifica el sistema o herramienta tecnológica que realiza la actividad.

- **Acción:** Hace referencia al verbo que describe la actividad concreta realizada como parte del control. Esta acción debe ser precisa y orientada a evidenciar el tipo de intervención que se aplica sobre el riesgo.

- **Complemento:** Detalla el objeto o propósito del control, incluyendo el mecanismo, documento, sistema o procedimiento mediante el cual se ejecuta. Este componente permite identificar con claridad el alcance del control implementado.

En la siguiente figura se presenta un ejemplo ilustrativo que aplica esta estructura de manera completa, facilitando su análisis en etapas posteriores del proceso de gestión de riesgos, tales como la evaluación de efectividad, la identificación de brechas y la priorización de acciones correctivas.



Tipología de controles en el ciclo de los procesos

La identificación precisa del tipo de control implementado en una organización es fundamental para determinar su alcance, momento de aplicación y nivel de efectividad frente a los riesgos identificados.

Esta clasificación se logra analizando el ciclo del proceso en el cual se inserta el control, lo cual permite establecer su tipología con mayor exactitud.

Con base en el ciclo de los procesos, se reconocen tres fases globales que determinan el tipo de control aplicado:

- **Entradas:** Recursos, insumos o condiciones iniciales requeridas para el inicio del proceso.

- **Interrelaciones:** Actividades o acciones intermedias que transforman las entradas en productos o servicios.

- **Salidas:** Productos, resultados o servicios entregados por el proceso.

Tipologías de control según el momento de activación

- **Control preventivo:** Se activa en la fase de entrada del proceso. Su propósito es evitar la ocurrencia del riesgo mediante la implementación de condiciones que aseguren el resultado esperado. Ataca la causa y la probabilidad de ocurrencia del riesgo.

- **Control detectivo:** Se activa durante la ejecución del proceso. Su función es identificar la materialización del riesgo o desviaciones antes de que afecten el resultado final, permitiendo corregir y volver a los controles preventivos. Ataca la probabilidad de ocurrencia.

- **Control correctivo:** Se activa en la fase de salida, cuando el riesgo ya se ha materializado. Su objetivo es mitigar los impactos generados y restaurar la operación del proceso. Ataca el impacto del riesgo.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

2.4.4.6. Análisis y valoración de controles: atributos para su calificación

Con el fin de determinar la efectividad de los controles implementados para mitigar los riesgos institucionales, se establece una metodología de análisis basada en atributos. Esta evaluación permite asignar un puntaje que refleja el grado de eficiencia, formalización y aplicabilidad del control.

A. Atributos para valorar la eficiencia del control

Los atributos de eficiencia se califican con peso específico y determinan el movimiento en la matriz de calor:

Característica	Descripción	Peso
Tipo de control		
Preventivo	Va hacia las causas del riesgo y busca asegurar el resultado final esperado.	25%
Detectivo	Detecta la materialización del riesgo y permite activar mecanismos correctivos. Puede generar reprocesos.	15%
Correctivo	Mitiga el impacto una vez se ha materializado el riesgo. Suele tener costos asociados.	10%
Implementación		

Automático	El control se ejecuta sin intervención humana, mediante sistemas o aplicativos.	25%
Manual	El control lo ejecuta una persona, lo cual implica riesgo de error humano.	15%

B. Atributos informativos (sin peso en la calificación)

Estos atributos permiten caracterizar el entorno operativo del control:

- **Documentación:** Indica si el control está o no documentado en manuales, procedimientos, flujogramas, etc.
- **Frecuencia:** Se refiere a la periodicidad del control (continua o aleatoria).
- **Evidencia:** Establece si el control deja un registro verificable de su ejecución.

Nota: *Los atributos informativos no afectan la calificación, pero son fundamentales para el análisis integral del control.*

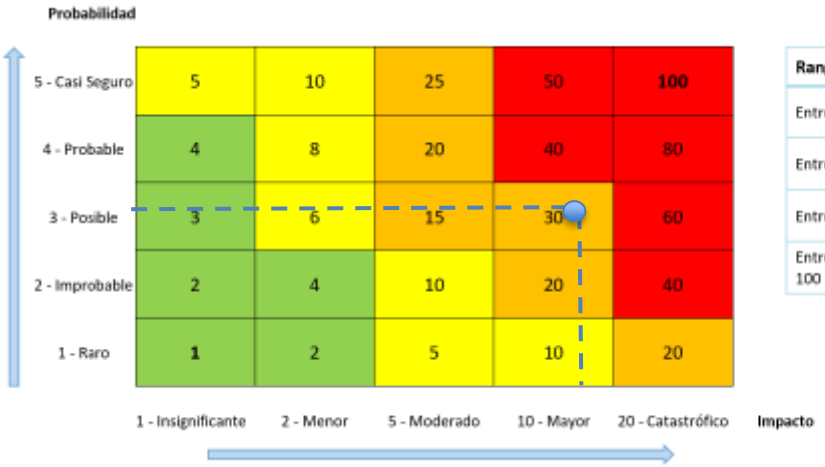
Ejemplo aplicado (continuación del caso anterior)

Proceso: Gestión de recursos

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la institución para su funcionamiento continuo.

Riesgo identificado: Posibilidad de pérdida económica por multa o sanción del ente regulador debido a adquisición de bienes sin cumplimiento de requisitos normativos.

- **Probabilidad inherente:** 3 (Posible)
- **Impacto inherente:** 10 (Mayor)
- **Zona de riesgo inherente:** 30 (Alta)



Al ubicar la combinación de los valores asignados a probabilidad (3) e impacto (10) en la matriz de calor, el riesgo se localiza en el cuadrante 30, correspondiente a una zona de alta severidad. Este resultado evidencia la necesidad de definir e implementar controles específicos orientados a la mitigación del riesgo identificado.

Ejemplo de Controles identificados y valoración

Control 1: El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Característica	Descripción	Peso	Evaluación
Tipo de control			
Preventivo	Va hacia las causas del riesgo y busca asegurar el resultado final esperado.	25%	25%
Detectivo	Detecta la materialización del riesgo y permite activar mecanismos correctivos. Puede generar reprocesos.	15%	-
Correctivo	Mitiga el impacto una vez se ha materializado el riesgo. Suele tener costos asociados.	10%	-

Implementación			
Automático	El control se ejecuta sin intervención humana, mediante sistemas o aplicativos.	25%	-
Manual	El control lo ejecuta una persona, lo cual implica riesgo de error humano.	15%	15%
Total valoración control 1			**40%**

Control 2: El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Característica	Descripción	Peso	Evaluación
Tipo de control			
Preventivo	Va hacia las causas del riesgo y busca asegurar el resultado final esperado.	25%	-
Detectivo	Detecta la materialización del riesgo y permite activar mecanismos correctivos. Puede generar reprocesos.	15%	15%
Correctivo	Mitiga el impacto una vez se ha materializado el riesgo. Suele tener costos asociados.	10%	-
Implementación			
Automático	El control se ejecuta sin intervención humana, mediante sistemas o aplicativos.	25%	-
Manual	El control lo ejecuta una persona, lo cual implica riesgo de error humano.	15%	15%
Total valoración control 2			**30%**

Aplicación de controles:

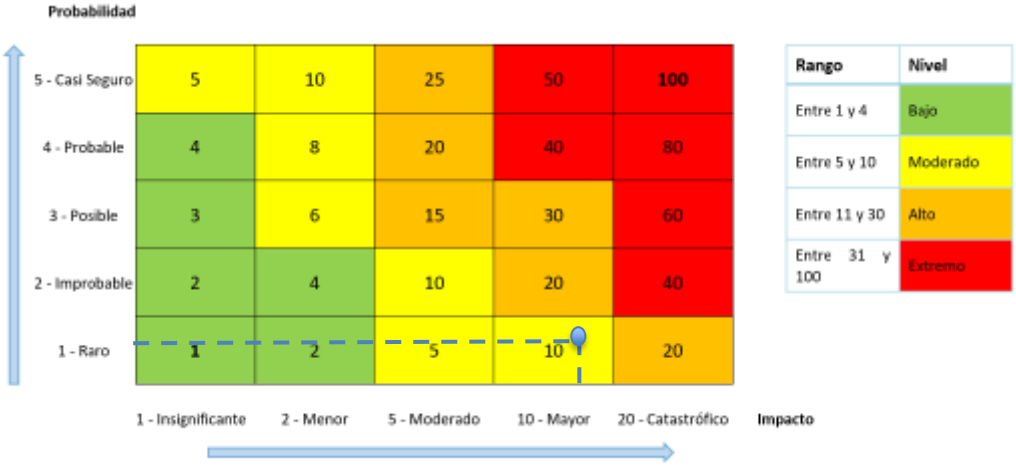
- **Control 1 (Preventivo):** 40%
- **Reducción =** 3 (nivel de probabilidad definido en el cálculo de riesgo inherente) x 40% (evaluación del control) = 1.2 → 3 - 1.2 = 1.8 Nivel de Probabilidad

- **Control 2 (Detectivo):** 30%
- **Reducción** = 1.8 x 30% = 0.54 → 1.8 - 0.54 = 1.26

Probabilidad residual ajustada: 1.26 = 1 (Se redondea a la escala anterior).

Valor residual final = 1 x 10 = 10 Impacto (Riesgo Moderado)

Nota: Si no se aplican controles correctivos, el impacto inherente permanece igual. El control impacta principalmente la probabilidad.



2.4.4.7. Otros mecanismos de evaluación para medir la efectividad de los controles

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 siguiente tabla.

Atributo	Descripción	Peso (%)	Ejemplo

Naturaleza del control (25 %) (momento en el que actúa)	Preventivo	Se acciona antes de que ocurra el evento de riesgo	25	Correctivo (15%)
	Detectivo	Se activa durante la ejecución detectando el riesgo y corrigiendo deficiencias	20	
	Correctivo	Se acciona después de que el riesgo se ha materializado, generando costos adicionales	15	
Nivel de automatización (10 %)	Automático	Ejecutado automáticamente sin intervención humana	10	Automático (10%)
	Semiautomático	Requiere uso de TIC y talento humano	7	
	Manual	Ejecutado manualmente por personas, susceptible a errores	5	
Cobertura (25 %)	Total	Aplica a todos los eventos sin distinción	25	Parcial (15%)
	Parcial	Aplica a una parte considerable de los eventos	15	
	Nula	Aplica a una pequeña porción o a ninguno de los eventos	0	
Nivel de periodicidad de ejecución (15 %)	Óptimo	Se ejecuta con la misma periodicidad que la actividad de riesgo	15	Bueno (10%)
	Bueno	Se ejecuta la mayoría de las veces	10	
	Malo	Se ejecuta con escasa periodicidad	5	
Madurez del control (25 %)	Definido, documentado, implementado, socializado y seguimiento	Cuenta con información documentada, aplicado en procesos y con seguimiento	25	Madurez del control (25 %)
	Definido, documentado, implementado y socializado	Cuenta con información documentada y aplicado en procesos	20	
	Definido, documentado, implementado	Cuenta con documentación y forma parte del proceso	15	
	Definido y documentado	Cuenta con documentación	10	
	Definido	Opera de manera informal	5	
Máximo % de eficiencia	100%	Máximo % de eficiencia	75% - Medio	

Nivel	Rango	Descripción	Disminución (en los niveles de probabilidad e 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.

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; se debe evaluar periódicamente. La eficacia se obtiene por autoevaluación a cargo de los integrantes de la primera o segunda línea de defensa o por auditorías e informes de seguimiento realizados por la Oficina de Control Interno de Gestión. Los atributos de eficacia para determinarla se exponen a continuación:

Atributo		Descripción	Peso	Ejemplo
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 nula o escasamente 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/o 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%	
Máxima 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:

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

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.

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.

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).

Indicadores clave de riesgo

Los Indicadores Clave de Riesgo (KRI's, por sus siglas en inglés Key Risk Indicators) son métricas específicas diseñadas para monitorear los cambios relevantes en el comportamiento de los riesgos. Funcionan como alertas tempranas que permiten identificar variaciones significativas en la probabilidad de ocurrencia de una causa (raíz o inmediata) o en el nivel de severidad de un impacto, facilitando así la toma oportuna de decisiones preventivas o correctivas.

Los KRI's se comportan como sensores que advierten cuando un riesgo empieza a desviarse de su comportamiento esperado. Por ello, es fundamental definir con claridad su nombre, propósito, frecuencia de medición y rangos de alerta.

Atributo	Descripción
Nombre	Denominación del indicador. Debe ser claro, conciso y estar enfocado en medir una causa (inmediata o raíz) o un impacto asociado al riesgo.
Descripción o fórmula	Detalle del uso del indicador o fórmula para calcular su valor. Este atributo es opcional, pero recomendable para asegurar trazabilidad y repetibilidad.
Frecuencia de medición	Periodicidad con la que se debe obtener el valor del indicador. Puede ser diaria, semanal, mensual, trimestral, semestral, anual u ocasional.
Estados de alerta	Rango de valores que permiten identificar el nivel de riesgo asociado al indicador:
	- **Bueno (sin alerta):** El riesgo está bajo control y dentro de límites aceptables.

	- **Regular (en alerta):** Requiere revisión y monitoreo. Puede ameritar acciones para reducir el riesgo.
	- **Malo (alerta crítica):** El riesgo ha superado los límites tolerables y exige acciones correctivas inmediatas.
Resultado del indicador	Valor obtenido tras aplicar la fórmula o medición, según la frecuencia definida. Este valor debe compararse con los estados de alerta para activar medidas.

Notas Finales

- Los KRI's deben definirse y monitorearse obligatoriamente en los riesgos residuales clasificados como "Alto" o "Extremo".

- Cuando se seleccione como opción de tratamiento la acción "Reducir", deberá formularse un plan de mejoramiento obligatorio para los riesgos "Extremos" y "Altos", y de manera opcional para los "Moderados".

- En caso de que un riesgo se materialice, deberá establecerse un plan de mejoramiento sin excepción.

- Cuando no sea posible definir un plan de mejoramiento para un riesgo significativo —ya sea potencial o materializado—, este deberá ser escalado al Equipo Técnico de Identificación y Respuesta (ETIR). Este equipo está conformado por los directores de la Oficina Asesora de Planeación Estratégica, la Oficina de Control Interno de Gestión y la División de Gestión de Calidad, junto con un profesional designado por cada una de estas dependencias, quienes acompañan y asesoran los procesos de gestión del riesgo en sus respectivas líneas de defensa.

- El ETIR será el encargado de analizar el caso, determinar la viabilidad de su tratamiento y definir el curso de acción correspondiente. En situaciones donde no sea posible aplicar ningún tipo de tratamiento, el ETIR deberá gestionar y asegurar la trazabilidad, el soporte técnico y el cumplimiento de los principios del Sistema Integrado de Gestión de la UMNG.

Ejemplo de Indicadores Clave de Riesgo (KRI's) para riesgo residual significativo - Proceso de Contratación

Riesgo	Nivel de Riesgo Residual y Tratamiento	Indicador Clave de Riesgo (KRI)	Meta	Frecuencia de Medición	Resultado del Indicador	Estado "Bueno" (sin alerta)	Estado "Regular" (en alerta)	Estado "Malo" (crítico)	Acciones por Realizar
Retrasos en la formalización de contratos que afectan el desarrollo de actividades misionales y operativas.	20 – Alto. Reducir	Número de procesos contractuales que superan el plazo legal establecido para su formalización	3	Trimestral	4	≤ 3	entre 4 y 6	>6	Requiere intervención del área jurídica y revisión del flujo del proceso de contratación
	20 – Alto. Reducir	Porcentaje de procesos contractuales que inician ejecución sin legalización formal	4%	Trimestral	12%	≤ 5%	6% - 10%	>10%	Activar auditoría interna o revisión interna urgente del procedimiento administrativo
	20 – Alto. Reducir	Valor total contratado sin legalización (en pesos colombianos)	$ 20.000.000	Trimestral	$ 36.000.000	≤ $20.000.000	$20.000.001 - $50.000.000	>$50.000.000	Escalar a Secretaría General y establecer correctivos inmediatos; riesgo financier

									o-institucional crítico

2.4.4.5. Seguimiento y revisión

El seguimiento y la revisión constituyen una fase esencial del ciclo de gestión integral del riesgo institucional, al permitir valorar la evolución del perfil de riesgo, la efectividad real de los controles implementados y el cumplimiento de los planes de mejoramiento definidos. Este proceso garantiza que los riesgos —en su condición inherente y residual— se mantengan dentro de los niveles de tolerancia definidos por la Universidad Militar Nueva Granada (UMNG).

Desde la perspectiva del Modelo de las Líneas de Defensa, el seguimiento y revisión se estructura de la siguiente manera:

Primera Línea de Defensa – Líderes de Proceso y Proyectos

- Ejecutan y supervisan de forma directa los controles operativos en el día a día.

- Documentan la implementación de los controles, monitorean su funcionamiento y consolidan la información de riesgos y planes de mejoramiento en la plataforma institucional.
- Son responsables del análisis de desviaciones, generación de alertas tempranas y activación de medidas correctivas inmediatas.
- Evalúan si los controles continúan siendo pertinentes para mitigar el riesgo residual.

Segunda Línea de Defensa – Oficina Asesora de Planeación Estratégica y División de Gestión de Calidad

- **Oficina Asesora de Planeación Estratégica (OFIPLA):**
    - Revisa el perfil del riesgo inherente y residual para cada proceso, con base en los lineamientos metodológicos del Modelo Integral de Gestión del Riesgo (MIGR).
    - Realiza seguimiento cuatrimestral al cumplimiento de los controles y planes de mejoramiento de riesgos estratégicos e institucionales.
    - Consolida la información de riesgos por tipología y elabora informes técnicos que permiten su análisis transversal.
    - Acompaña al Equipo Técnico de Identificación y Respuesta (ETIR) en el escalamiento y gestión de riesgos críticos.

- **División de Gestión de Calidad:**
    - Verifica que los controles definidos por los líderes de proceso estén debidamente documentados, actualizados y alineados con los estándares del Sistema Integrado de Gestión (SIG).
    - Evalúa la efectividad de los controles mediante auditorías internas, revisiones de seguimiento y validaciones de cumplimiento normativo.
    - Acompaña técnicamente a los procesos para fortalecer la cultura de autocontrol y mejora continua.

Tercera Línea de Defensa – Oficina de Control Interno de Gestión

- Audita de manera independiente la calidad del seguimiento realizado por la primera y segunda línea.
- Evalúa la confiabilidad de los reportes sobre la gestión del riesgo y verifica la trazabilidad de los planes de mejoramiento implementados.
- Identifica brechas sistémicas en la gestión del riesgo y recomienda acciones correctivas estratégicas.
- Supervisa la alineación del sistema de control interno con el marco institucional y normativo.

Los resultados del proceso de seguimiento pueden incluir, entre otros:

- Informes periódicos (semestrales o anuales) sobre la evolución del mapa de riesgos institucional.
- Evaluaciones sobre la eficacia y eficiencia de los controles implementados.
- Análisis del grado de cumplimiento de los planes de mejoramiento.

- Identificación de variaciones significativas en el perfil de riesgos que requieran ajustes o rediseño de estrategias.
- Escalamiento de riesgos críticos al Comité de Gestión y Desempeño o al Equipo Técnico de Identificación y Respuesta (ETIR), conforme al marco de gobernanza institucional.

2.4.5.1. Periodicidad del seguimiento a los riesgos Institucionales

Categoría de Riesgo	Frecuencia de Seguimiento	Justificación
Riesgos Fiscales	**Trimestral**	Implican el uso de recursos públicos y pueden derivar en hallazgos fiscales, sanciones o detrimento patrimonial. Requieren seguimiento regular para garantizar la correcta ejecución presupuestal, la legalidad en el gasto y la oportuna gestión de alertas por parte de los órganos de control.
Riesgos Estratégicos	**Semestral**	Impactan la misión, visión y objetivos institucionales a largo plazo. Su evolución no suele ser inmediata, pero requiere ajustes estratégicos periódicos.
Riesgos Operativos	**Mensual**	Pueden afectar la ejecución diaria de los procesos internos, requiriendo ajustes constantes en los controles y medidas correctivas.
Riesgos Financieros y Contables	**Mensual**	La gestión de recursos y estabilidad financiera debe evaluarse con regularidad para prevenir desviaciones que afecten la sostenibilidad de la entidad.
Riesgos de Corrupción	**Trimestral**	Su vigilancia debe ser constante para detectar posibles vulnerabilidades, pero la naturaleza de estos riesgos exige revisiones formales con una periodicidad alineada a las auditorías internas.
Riesgos Ambientales	**Semestral**	Los impactos ambientales suelen manifestarse en el mediano y largo plazo, pero requieren seguimiento periódico para mitigar afectaciones institucionales y cumplimiento normativo.

Riesgos de Seguridad y Salud en el Trabajo	**Diario (crítico) / Mensual (general)**	Los incidentes pueden presentarse en cualquier momento. Los riesgos críticos requieren monitoreo constante, mientras que otros aspectos pueden revisarse mensualmente.
Riesgos Antrópicos	**Diario (crítico) / Trimestral (preventivo)**	En caso de amenazas inminentes, se debe hacer monitoreo diario. Para planificación y prevención, es adecuado un seguimiento trimestral.
Riesgos de Seguridad de la Información	**Diario (sistemas críticos) / Mensual (evaluación general)**	La ciberseguridad exige un monitoreo constante de amenazas y vulnerabilidades, complementado con auditorías mensuales de la infraestructura tecnológica.
Riesgos de Daño Antijurídico	**Trimestral**	La materialización de estos riesgos puede generar sanciones o litigios prolongados, por lo que deben revisarse periódicamente y con enfoque preventivo.
Riesgos de Proyectos de Investigación e Innovación	**Trimestral**	Los proyectos de investigación tienen ciclos definidos, por lo que su seguimiento periódico permite anticipar riesgos que puedan afectar sus resultados.
Riesgos de Plan de Desarrollo	**Semestral**	Afectan la planeación a largo plazo y su evaluación debe coincidir con las revisiones institucionales del plan estratégico.
Riesgos de Plan de Rectoral	**Trimestral**	Afectan la planeación a largo plazo y su evaluación debe coincidir con las revisiones institucionales del plan estratégico.

En el caso específico de los riesgos de corrupción, el monitoreo y la revisión deben realizarse tres veces al año, conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP. Este proceso debe ser liderado por la Oficina Asesora de Planeación Estratégica en colaboración con los equipos de trabajo en todos los niveles jerárquicos, con el objetivo de consolidar la información recopilada y evaluar el grado de aplicabilidad y alcance de las actividades definidas en el mapa de riesgos. Esto incluye la verificación del estado de implementación de los controles y la ejecución de los planes de acción asociados.

Para demostrar el cumplimiento de los compromisos adquiridos en la gestión de riesgos, la Universidad Militar Nueva Granada implementará un sistema de auditoría interna que permita validar la correcta administración de riesgos conforme a la normativa institucional y los lineamientos nacionales. En el caso específico de los riesgos estratégicos y de corrupción, y de acuerdo con lo establecido en el Plan Anual de Auditorías y Seguimientos, la Oficina de Control Interno de Gestión realizará seguimientos cuatrimestrales en los meses de enero, mayo y septiembre, en concordancia

con lo dispuesto por la Secretaría de Transparencia, la Presidencia de la República y el Departamento Administrativo de la Función Pública.

De acuerdo con la frecuencia establecida por la Guía DAFP, la Oficina de Control Interno debe realizar la revisión y seguimiento de los mapas de riesgos de corrupción y estratégicos institucionales de acuerdo con las siguientes fechas:

Seguimiento	Fechas de corte	Fecha de Presentación	Observaciones
Primer seguimiento	31 de diciembre	Enero	Publicar dentro de los primeros diez (10) del mes siguiente.
Segundo seguimiento	30 de abril	Mayo	
Tercer seguimiento	31 de agosto	Septiembre	

El informe de seguimiento por parte de la Oficina de Control Interno Gestión se deberá publicar en la página web de la Universidad y de fácil acceso para la comunidad neogranadina.

La Oficina Asesora de Planeación Estratégica encargada de liderar y monitorear los riesgos institucionales identificados por los líderes de procesos, realizará los seguimientos de manera cuatrimestral (Marzo, Julio y Noviembre).

Además, la Oficina Asesora de Planeación Estratégica junto con la División de Gestión de Calidad definirán el mecanismo a seguir para que cada líder de proceso revise y valide la pertinencia de sus riesgos, los controles aplicados, las variables de medición y las evidencias que sustentan el adecuado seguimiento y control de los riesgos. Estas evidencias deben reflejar la fiabilidad de las variables de medición y el objeto del riesgo y del control.

2.4.5.2. Seguimiento de Riesgos Materializados

El seguimiento de los riesgos materializados se realiza con base en un esquema estructurado que abarca desde la identificación y reporte del evento hasta la ejecución de medidas correctivas y preventivas. Este proceso integra a todos los actores institucionales conforme al Modelo de las Tres Líneas de Defensa, asegurando una respuesta articulada, oportuna y eficaz.

Las etapas clave del proceso de gestión de riesgos materializados son las siguientes:

- **Registro del evento:** Consiste en el diligenciamiento del riesgo materializado en las herramientas institucionales establecidas, como el sistema KAWAK (numeral 3.5.1).
- **Análisis del evento:** Implica la evaluación de las causas inmediatas y raíz del evento, así como su impacto sobre los procesos, servicios o resultados institucionales. Este análisis debe estar soportado con evidencia objetiva y métricas que permitan medir la severidad del impacto.
- **Formulación del Plan de Acción (PA):** Se define un conjunto de medidas correctivas y preventivas para mitigar el impacto y prevenir la recurrencia del evento. Estas acciones deben estar documentadas, tener responsables asignados y contar con plazos definidos para su implementación. Su registro también se gestiona a través del aplicativo KAWAK.
- **Seguimiento del PA:** Se monitorea el avance y efectividad de las acciones implementadas. Los resultados del seguimiento deben ser documentados, con evidencia verificable, y comunicados tanto a los niveles operativos como a los estratégicos de la Universidad.

La gestión de riesgos materializados debe realizarse de manera inmediata tras su detección, complementándose con revisiones periódicas que permitan evaluar la efectividad de las acciones tomadas.

Contribución por Líneas de Defensa:

- **Primera Línea de Defensa (Líderes de proceso):** Son los primeros responsables en reportar el evento y activar el análisis inmediato del riesgo materializado. Ejecutan las acciones definidas en el Plan de Acción, hacen seguimiento directo y documentan su cumplimiento en las plataformas oficiales.

- **Segunda Línea de Defensa (Oficina Asesora de Planeación Estratégica y División de Gestión de Calidad):**

    - *OFIPLA:* Acompaña técnicamente la formulación del plan de acción y verifica su coherencia con la tipología de riesgo y su criticidad. Realiza seguimiento cuatrimestral a riesgos materializados de impacto institucional.
    - *DGC:* Evalúa la documentación y trazabilidad del control posterior al evento, asegurando su incorporación al SIG. Realiza auditorías de validación sobre la ejecución del plan de acción.

- **Tercera Línea de Defensa (Oficina de Control Interno de Gestión):** Supervisa de forma independiente que los riesgos materializados hayan sido gestionados conforme a la normativa, validando el cierre efectivo de los planes de acción, así como la existencia de mejoras sistémicas cuando sea necesario.

2.4.5.3. Evaluación de Controles

Para garantizar la eficiencia y eficacia de los controles implementados, se deben realizar evaluaciones periódicas que permitan verificar su impacto en la reducción de riesgos. Estas evaluaciones deben considerar tanto el diseño del control (eficiencia) como su efectividad en la ejecución (eficacia), asegurando un aseguramiento razonable sobre la mitigación del riesgo.

Los criterios de evaluación de los controles incluyen:

- **Eficiencia:** Diseño adecuado del control en relación con el riesgo identificado. Por ejemplo, un control eficiente sería un sistema automatizado que impide errores en la liquidación de pagos antes de que estos se materialicen.

- **Eficacia:** Resultados obtenidos a partir de la ejecución del control en un período determinado. Un ejemplo sería verificar que, tras la implementación del control, se ha reducido significativamente la frecuencia de errores detectados en auditorías.

- **Periodicidad:** Frecuencia con la que se aplica y revisa el control. Aunque la evaluación general debe realizarse al menos una vez al año, ciertos controles críticos (como los asociados a seguridad de la información o corrupción) pueden requerir revisiones trimestrales o incluso continuas.

- **Cobertura:** Evalúa qué áreas, funciones o procesos están protegidos por el control, así como si existen brechas en su aplicación. Una cobertura adecuada implica que el control aplica transversalmente a todos los subprocesos expuestos al riesgo.

El seguimiento y evaluación de los controles es responsabilidad compartida entre:

- **Primera Línea de Defensa:** Encargada de ejecutar, monitorear y documentar los controles en el día a día.
- **Segunda Línea de Defensa (Oficina Asesora de Planeación Estratégica y División de Gestión de Calidad):** Acompañan metodológicamente y consolidan los resultados de la evaluación de los controles.
- **Tercera Línea de Defensa (Oficina de Control Interno de Gestión):** Valida de forma independiente que los controles evaluados realmente mitiguen los riesgos, y que los informes reflejen fielmente la situación observada.

Cada tipología de riesgo puede definir herramientas específicas para este propósito, tales como:

- Auditorías internas o externas.
- Revisión de controles en Kawak.
- Cuestionarios de autoevaluación de controles.

Estas herramientas permiten estandarizar la recolección de información, facilitar la trazabilidad del proceso evaluativo y mejorar la toma de decisiones frente a la gestión de riesgos institucionales.

2.4.5.4. Registro e Informe de la Gestión de Riesgos

El registro y documentación de la información de gestión de riesgos es clave para asegurar la trazabilidad, disponibilidad y confiabilidad de los datos. Para ello, se establecen tres momentos fundamentales:

- **Identificación y estructuración de la información a registrar:** Se debe asegurar la estandarización mediante formatos institucionales definidos en el marco metodológico de la UMNG, basados en referentes como la NTC ISO 31000:2018 y los lineamientos del Departamento Administrativo de la Función Pública (DAFP). Entre los formatos más utilizados se encuentran las fichas de riesgos, matrices de valoración y registros de controles.
- **Centralización de la información:** La universidad cuenta con una plataforma digital de gestión de riesgos (KAWAK) como sistema centralizado para la identificación, análisis, evaluación y monitoreo de riesgos. Esta herramienta permite el almacenamiento organizado de la información y su trazabilidad a lo largo del ciclo de vida del riesgo.
- **Elaboración de informes de gestión:** Se elaboran distintos tipos de informes según el nivel de gestión:

- *Informes estratégicos:* Dirigidos a la alta dirección, Comité Institucional de Gestión y Desempeño, Consejo Académico o Consejo Superior. Incluyen análisis del perfil de riesgo institucional, evolución de los riesgos críticos, estado de los controles y recomendaciones estratégicas.
- *Informes operativos:* Dirigidos a líderes de proceso y responsables de riesgos. Contienen seguimiento detallado de los planes de acción, actualización de controles y alertas de riesgo con base en los KRI.

Periodicidad y Responsables del Registro:

- El registro de riesgos debe realizarse de forma continua y actualizada, especialmente al identificar nuevos eventos, modificar condiciones del riesgo o actualizar controles.
- La responsabilidad del registro recae en la primera línea de defensa: líderes de proceso, coordinadores y responsables de proyectos.
- La segunda línea (Oficina Asesora de Planeación Estratégica y División de Gestión de Calidad) verifica la completitud, consistencia y vigencia de la información registrada.

Acceso y Seguridad de la Información:

La información de riesgos se gestiona bajo las políticas institucionales de seguridad de la información y protección de datos personales. Se establecen niveles de acceso según la clasificación de la información:

- **Pública:** Información general sobre riesgos institucionales.
- **De acceso restringido:** Información técnica y operativa sujeta a autorización.
- **Confidencial:** Información crítica o sensible relacionada con riesgos estratégicos, financieros, de corrupción u otros de alto impacto.

Indicadores Clave (KPIs) en los Informes:

Los informes deben incluir KPIs que reflejen el estado y evolución del riesgo, tales como:

- Número de riesgos identificados por tipología.
- Porcentaje de riesgos evaluados y con controles activos.
- Número de planes de acción ejecutados vs. programados.
- Nivel de cumplimiento en la mitigación de riesgos críticos.
- Resultados de los Indicadores Clave de Riesgo (KRI).

Los informes de gestión de riesgos deben alinearse con:

- La NTC ISO 31000:2018 – Gestión del Riesgo.
- La Guía para la Administración del Riesgo del DAFP (versión 6, 2022).
- Las disposiciones del Modelo Estándar de Control Interno (MECI).
- Los requerimientos de auditoría interna y entes de control externo.

Este enfoque asegura una gestión documentada, accesible y útil para la toma de decisiones en todos los niveles de la Universidad Militar Nueva Granada, fortaleciendo la cultura de gestión de riesgos y la mejora continua institucional.

3. Registro en la Plataforma KAWAK

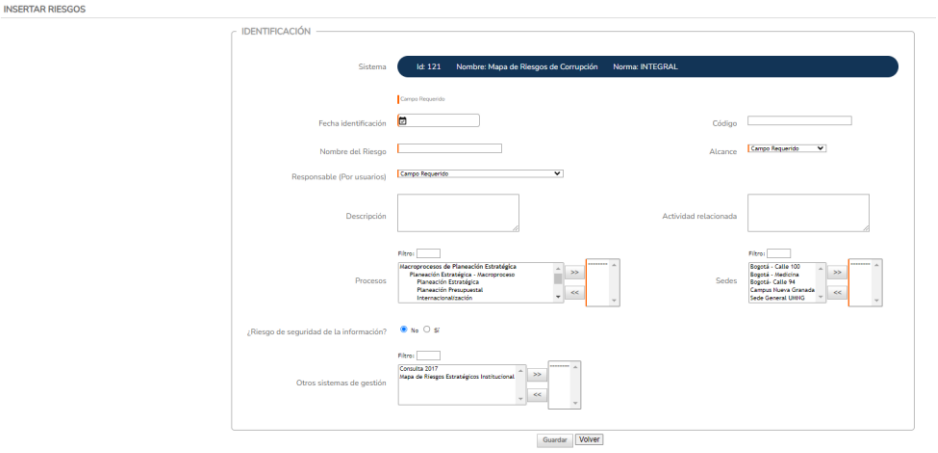
En el proceso de levantamiento o actualización de los procesos y procedimientos institucionales liderado por la División de Gestión de Calidad, cada líder de proceso debe revisar y validar los riesgos y controles asociados a su gestión, asegurando que la información registrada en la plataforma KAWAK esté actualizada, sea pertinente y responda tanto a las necesidades del proceso como a los lineamientos institucionales.

Es importante tener en cuenta que los riesgos asignados a un área o proceso pueden corresponder a distintas tipologías (riesgos operativos, de corrupción, de sistemas de gestión de la información, fiscales o estratégicos), de acuerdo con su naturaleza y con el mapeo realizado por la Oficina Asesora de Planeación Estratégica (OFIPLA). Este mapeo permite identificar los actores responsables de la gestión, monitoreo y control de cada riesgo, y garantiza su adecuada mitigación y disponibilidad para la toma de decisiones institucionales.

La configuración de los riesgos en la plataforma KAWAK está a cargo de la Oficina Asesora de Planeación Estratégica (OFIPLA). Su actualización será responsabilidad del profesional designado por esta oficina, quien acompañará el proceso con base en los insumos suministrados por la División de Gestión de Calidad y la Oficina de Control Interno de Gestión.

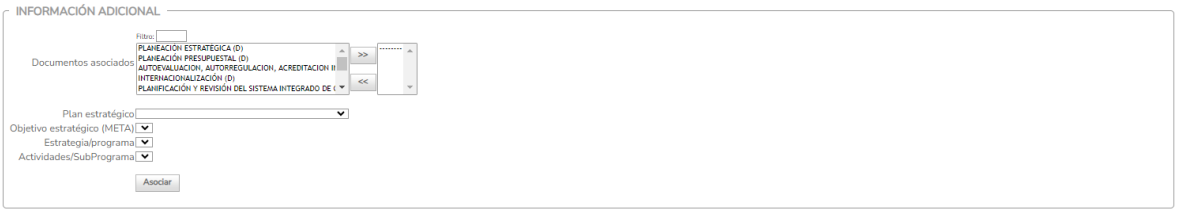
Los permisos de edición de los riesgos y controles estarán exclusivamente bajo la administración de la OFIPLA. Por su parte, el acceso al módulo de riesgos de KAWAK será asignado por la División de Gestión de Calidad a los profesionales técnicos que hayan sido formalmente designados para esta función. La visualización de los riesgos y controles será habilitada por la OFIPLA una vez el líder de proceso reporte oficialmente el nombre del profesional técnico responsable del seguimiento de los controles asociados a su proceso o área.

Se asignará un usuario de consulta a la Oficina de Control Interno de Gestión, con el fin de que esta dependencia pueda realizar de forma autónoma el seguimiento a los riesgos y controles de la Universidad, y generar los reportes cuatrimestrales requeridos por el Comité de Evaluación del Control Interno (CECI) y el Departamento Administrativo de la Función Pública (DAFP).

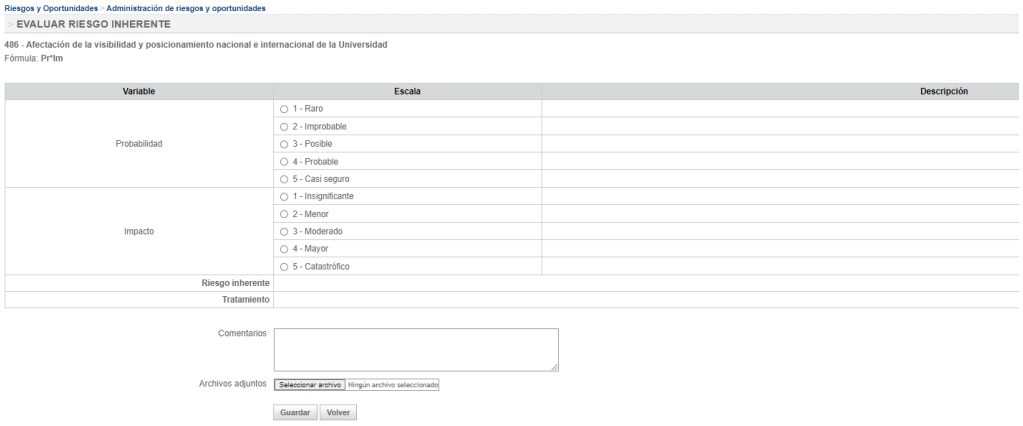


Por parte de la División de Calidad cuando se esté caracterizado el riesgo junto con los líderes de proceso, se proporcionará la siguiente Información a la OFIPLA para la debida configuración del riesgo en la plataforma Kawak:

- Se identifican los documentos que existan asociados al riesgo identificado
- Seleccionar el plan estratégico
- Identificar el objetivo estratégico con el cual se asocia el riesgo identificado



La configuración y gestión del proceso de riesgos institucional se realiza a través del módulo de administración de riesgos en la plataforma KAWAK por parte de la Oficina Asesora de Planeación Estrategica (OFIPLA). Para evaluar un riesgo, se debe ingresar a la pestaña **EVALUAR**, como se muestra a continuación, donde se establece el nivel de impacto y probabilidad de ocurrencia del riesgo, de acuerdo con los parámetros definidos en el presente procedimiento.



3.1. Permisos

Cada líder de proceso debe definir, dentro de su equipo de trabajo, quién o quiénes serán los responsables de atender la gestión, seguimiento y reporte de los riesgos asignados a su proceso o procedimiento. Esta asignación debe contemplar la capacidad técnica y el conocimiento del proceso, garantizando una gestión oportuna y efectiva de los riesgos en la plataforma KAWAK.

En caso de cambios en el personal asignado a esta función, el líder del proceso deberá informar de manera inmediata a la Oficina Asesora de Planeación Estratégica, mediante correo electrónico institucional, indicando:

- El nombre completo de la persona que dejará de ejercer la responsabilidad.
- El nombre completo y cargo de quien asumirá el rol de profesional o técnico de riesgos para el proceso, riesgo o control respectivo.
- Esta notificación permitirá actualizar los permisos en la plataforma KAWAK, específicamente en lo relacionado con los usuarios autorizados para editar, visualizar o asignar controles a los riesgos y planes de tratamiento definidos.

Este manual garantiza la trazabilidad, continuidad y consistencia en la gestión de riesgos institucionales, evitando vacíos de responsabilidad que puedan afectar el control y mitigación de eventos críticos.

3.2. Implementación de Controles

En la opción **Implementar Controles** de la plataforma KAWAK se describen las medidas que se han definido o implementado para mitigar las causas y/o consecuencias de los riesgos identificados. Estos controles pueden estar orientados a disminuir la probabilidad de ocurrencia o a reducir el impacto del riesgo.

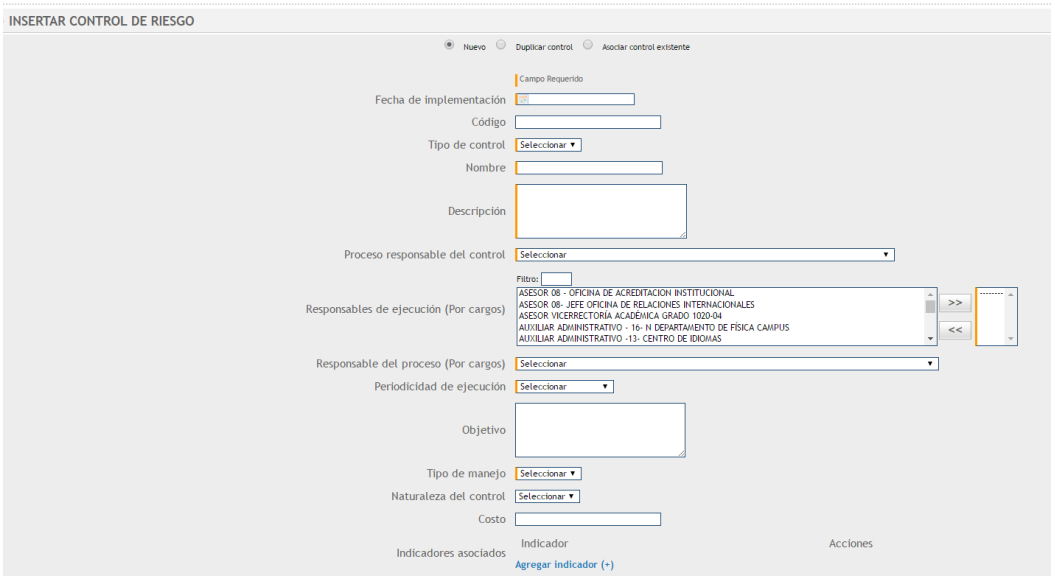
Una vez realizada la valoración del riesgo, es fundamental identificar, registrar y documentar los controles existentes en la plataforma KAWAK, evaluando su cumplimiento y efectividad con base en criterios establecidos.

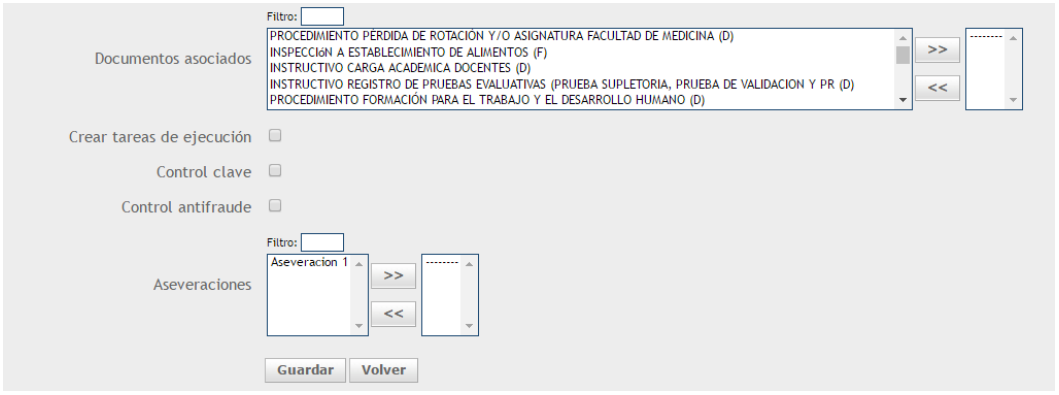
De acuerdo con la metodología definida por la Universidad, se deben diligenciar los siguientes campos para cada control:

- Nombre del control
- Descripción del control
- Tipo de control
- Proceso responsable
- Responsables de ejecución
- Periodicidad de ejecución
- Objetivo del control
- Tipo de manejo
- Naturaleza del control
- Costo estimado o asociado

- Indicadores y documentos asociados
- Responsable de la ejecución

Calificación del control: esta valoración debe realizarse con base en cinco variables previamente definidas en la metodología institucional, las cuales deben estar debidamente soportadas con documentación verificable.





3.3. Evaluación del Riesgo

La evaluación del riesgo es el proceso mediante el cual se contrastan los resultados del análisis del riesgo con los controles implementados, con el fin de establecer prioridades en su gestión y definir políticas adecuadas para su manejo. Para ello, es fundamental contar con un conocimiento claro de los puntos de control existentes en los distintos procesos, proyectos, dependencias y sistemas de gestión institucional.

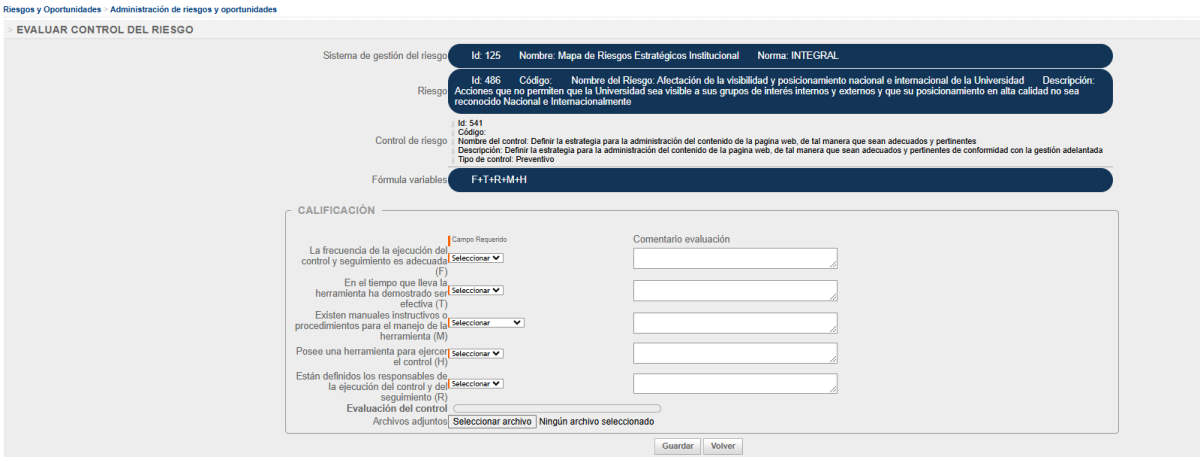
Cada control es evaluado con base en sus atributos de diseño y eficacia, lo que permite determinar si realmente contribuye a la mitigación del riesgo. Es importante considerar que:

- Un mismo riesgo puede tener múltiples causas y, por lo tanto, requerir diversos controles.
- La evaluación debe analizar cómo los controles desplazan el riesgo desde la zona inherente (riesgo sin mitigación) hasta la zona residual (riesgo luego de aplicar controles).
- Para que un control sea efectivo, debe cumplir con todas las variables de diseño y demostrar su impacto real en la reducción de la probabilidad o impacto del riesgo.

En la evaluación de los controles de riesgos, los responsables de los procesos deben realizar un análisis exhaustivo de las actividades desarrolladas para la mitigación del riesgo y adjuntar evidencia suficiente del control realizado.

En la plataforma KAWAK, los responsables de los procesos deben realizar una evaluación detallada de los controles, asegurando que:

1. Se analicen las actividades implementadas para la mitigación del riesgo.
2. Se deben cargar y garantizar que el reporte cargado en la plataforma corresponda al documento previamente concertado con el líder de proceso y que esté debidamente descrito para cada control definido y como respaldo que acredita la ejecución del control.
3. Se califique el control según las variables establecidas.
4. Se incluyan comentarios y justificaciones en cada ítem requerido.



3.4. Desplazamiento del Riesgo de la Zona Inherencia a la Zona Residual

El **riesgo residual** corresponde al nivel de riesgo que persiste una vez han sido implementados los controles definidos para mitigar un evento. Este parte de la premisa de que ningún riesgo puede ser completamente eliminado, a menos que desaparezca el activo expuesto. Por ello, la gestión del riesgo busca generar un grado razonable de confianza en el cumplimiento de los objetivos institucionales, llevando los riesgos a niveles aceptables para la Universidad.

La aplicación de controles —cuya eficacia y eficiencia deben haber sido previamente evaluadas— permite disminuir los niveles de **impacto** y **probabilidad** asociados al riesgo. Esto genera un

desplazamiento en el Mapa de Calor, trasladando el riesgo desde su zona de **inherencia** (riesgo puro) hacia su nueva ubicación en la zona de **riesgo residual**, donde se refleja el efecto de las acciones de mitigación.

Es importante tener en cuenta que los controles actúan de forma **acumulativa**, es decir:

- El primer control se aplica sobre el nivel original del riesgo (valor inherente).
- El segundo control se aplica sobre el nivel resultante luego de aplicar el primero, y así sucesivamente.
- Este desplazamiento se calcula en el eje de **probabilidad** o en el de **impacto**, dependiendo del tipo de variable que el control esté diseñado para reducir.

El resultado final será el nuevo nivel del riesgo (residual), el cual debe ubicarse en el Mapa de Calor y evaluarse frente a los criterios de aceptabilidad institucional definidos por la UMNG. Este nivel servirá como base para decidir si se acepta el riesgo o si deben diseñarse nuevas medidas de tratamiento.

3.4.1. Plan de tratamiento

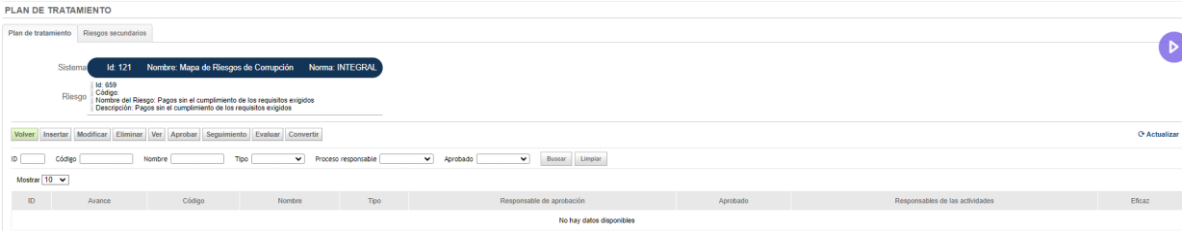
a. Tratamiento del riesgo Configurados.

De acuerdo con la autoevaluación por la **primera línea de defensa** (líderes del Proceso), y con el fin de lograr la mitigación de los diferentes riesgos;(Riesgos Estratégicos, corrupción y Seguridad Digital), conforme a la política de administración del riesgo establecida en la UMNG, los dueños de los procesos tendrán en cuenta la importancia de cada riesgo identificado, frente a la **probabilidad e impacto** de este y la relación **costo-beneficio**, siendo estas medidas de control fundamental en el tratamiento de los riesgos, con el fin de evitar, reducir que el riesgo se materialice. La inobservancia a estos criterios generaría situaciones adversas al cumplimiento de los objetivos en cada proceso en la UMNG.

Se tiene definido que los riesgos que se encuentran en zonas de calificación moderada, alta y extrema requieren tratamiento con el objetivo de llevarlos a zona de calificación baja, mientras que los que se encuentran en zona baja deben ser monitoreados y controlados para evitar que se materialicen en el futuro.

Al establecer los controles de riesgo, se define el plan de tratamiento con lo cual la metodología le permite al usuario tener un seguimiento más detallado de la evolución y seguimiento al riesgo identificado. El sistema gestiona el ID e identifica:

- Fecha de creación
- Fecha de última modificación
- Nombre del plan
- Responsable
- Responsable de aprobar el plan
- Calificación
- Origen y estado



En la gestión de riesgos se contemplan tres tipos de planes de acción:

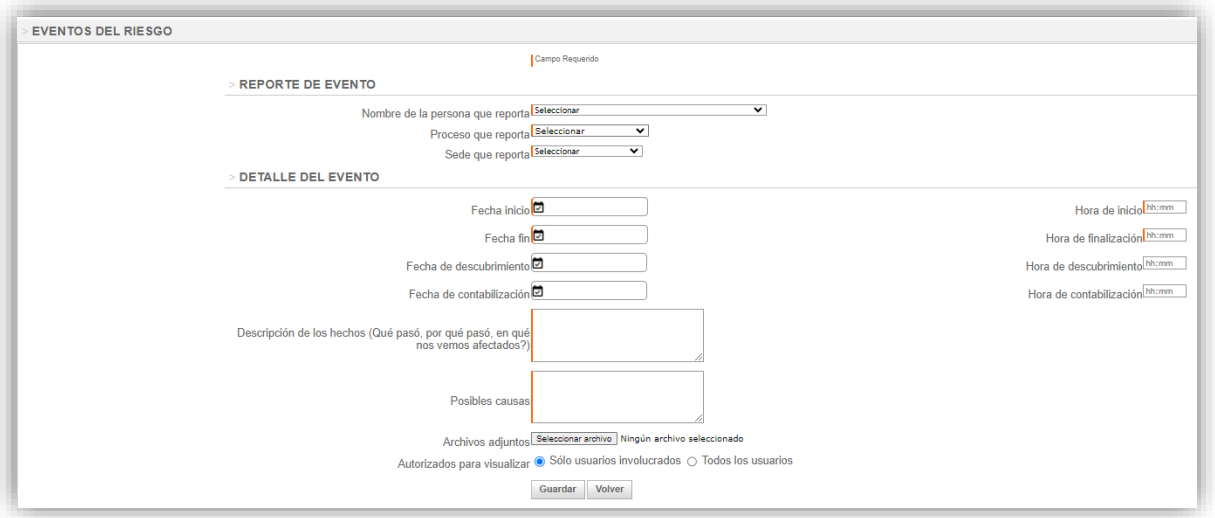
Plan de tratamiento: Corresponde al conjunto de acciones que no modifican directamente un control existente, sino que se ejecutan durante un periodo determinado con el fin de fortalecer la gestión del riesgo. El resultado de un plan de tratamiento durante una vigencia determinada será la generación de un nuevo control —ya sea de probabilidad o de impacto— que podrá aplicarse en vigencias futuras, con el objetivo de modificar la valoración del riesgo residual.

Plan de mejora (oportunidad de mejora): Al igual que los planes de tratamiento, consiste en un conjunto de actividades que se ejecutan en un periodo determinado. Sin embargo, su finalidad no es crear un nuevo control, sino fortalecer o perfeccionar un control ya existente, mejorando su eficiencia, eficacia o alcance dentro del proceso de gestión del riesgo.

3.4.2. Gestión de eventos del riesgo

El módulo de gestión de eventos tiene como finalidad, evidenciar la ocurrencia de los riesgos (riesgos materializados), con el fin de establecer los controles adecuados para evitar la continuidad de su materialización.

La metodología establecida incluye: Un análisis detallado de los eventos ocurridos, la definición del tipo de evento, la perdida en el proceso o procesos, la definición de las posibles causas, la identificación de los controles que fallaron, la documentación de las acciones inmediatas, la cuantía de la pérdida y los archivos que soportan la novedad.

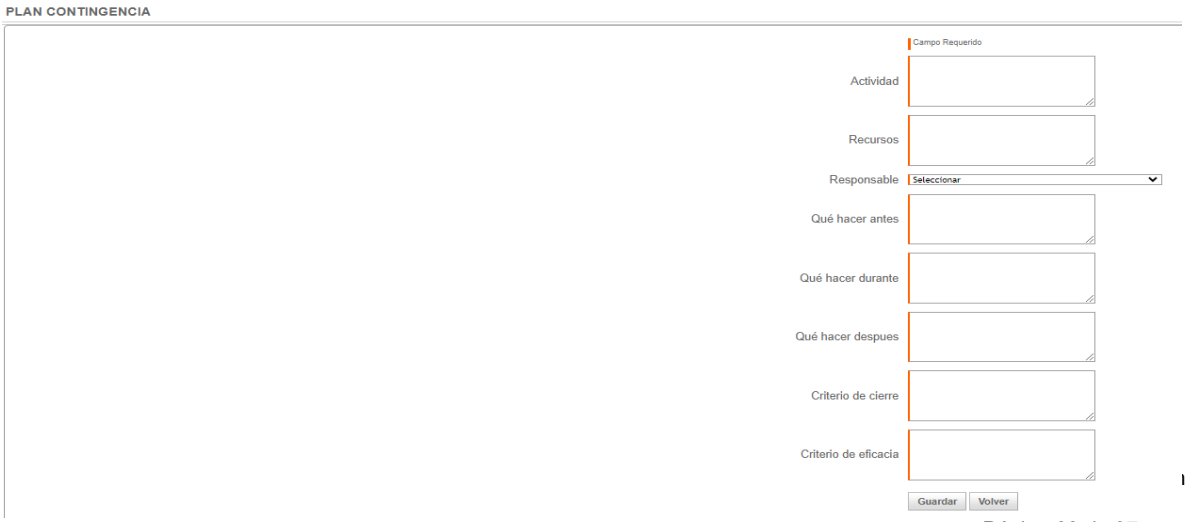


Plan de acción o de contingencia: Utilizado cuando se materializa un riesgo.

El Plan de contingencia identifica las acciones a ejecutar en caso de materialización del riesgo este plan le permite al líder del proceso definir las actividades requeridas para gestionar el riesgo.

Que solicita la metodología:

- Definición de la actividad
- Recursos
- Responsable
- ¿Qué hacer antes?
- ¿Qué hacer durante?
- ¿Qué hacer después?
- Criterio de cierre
- Criterio de eficacia



4. Comunicación y Consulta

El proceso de gestión del riesgo requiere un flujo continuo, claro y oportuno de información entre todas las partes interesadas. Para ello, la Universidad Militar Nueva Granada (UMNG) implementa estrategias de comunicación y consulta que facilitan la toma de decisiones informadas, basadas en datos confiables, fomentando una cultura organizacional orientada a la prevención y al pensamiento basado en riesgos.

Objetivos del proceso de comunicación:

- Garantizar la identificación precisa de riesgos y su impacto en la institución.
- Evaluar los riesgos de manera transparente, considerando probabilidad e impacto.
- Priorizar los riesgos más críticos para su tratamiento inmediato.
- Involucrar a todas las partes interesadas en la gestión del riesgo.
- Supervisar la efectividad de las medidas de control y su implementación.
- Promover el pensamiento basado en riesgos en todos los niveles organizacionales.

Canales y mecanismos de comunicación institucional:

Página web institucional: Los mapas de riesgos institucionales serán publicados para garantizar acceso a toda la comunidad universitaria. Estarán disponibles en la sección La Universidad, opción Gestión de Riesgos y Oportunidades Institucionales, dentro del apartado Contextualización de Mapas de Riesgos Institucionales por Vigencia.

Plataforma KAWAK: Se mantendrán actualizados los mapas de riesgos institucionales, así como los controles asociados, incorporando mejoras y correcciones derivadas del monitoreo, evaluación, seguimiento y auditorías internas o externas. Los líderes de proceso deben revisar periódicamente esta información para asegurar su vigencia.

Correos institucionales y boletines informativos: Se utilizarán para divulgar alertas, actualizaciones relevantes y recordatorios sobre la gestión del riesgo, especialmente dirigidos a líderes de proceso y profesionales técnicos designados.

Reuniones de seguimiento y control: En los espacios de evaluación interna (comités, reuniones técnicas, mesas de trabajo), se socializarán los principales hallazgos y recomendaciones en torno a riesgos críticos, controles ineficaces o eventos materializados.

Capacitaciones y talleres: Se programarán sesiones formativas periódicas con el fin de fortalecer las competencias de los equipos responsables en gestión de riesgos, controles y planes de acción.

Consulta y retroalimentación:

La UMNG garantizará mecanismos de retroalimentación mediante:

- La habilitación de espacios participativos en reuniones institucionales.
- La recepción de observaciones o sugerencias a través de medios institucionales (correo, formularios internos).
- El análisis y respuesta técnica desde la Oficina Asesora de Planeación Estratégica y la División de Gestión de Calidad a los aportes presentados por líderes de proceso, entes de control o partes interesadas.

Este proceso de comunicación y consulta busca no solo informar, sino también facilitar la participación de todos los actores clave en la construcción, evaluación y mejora continua del modelo de gestión de riesgos institucional.

5. Lineamientos Operativos

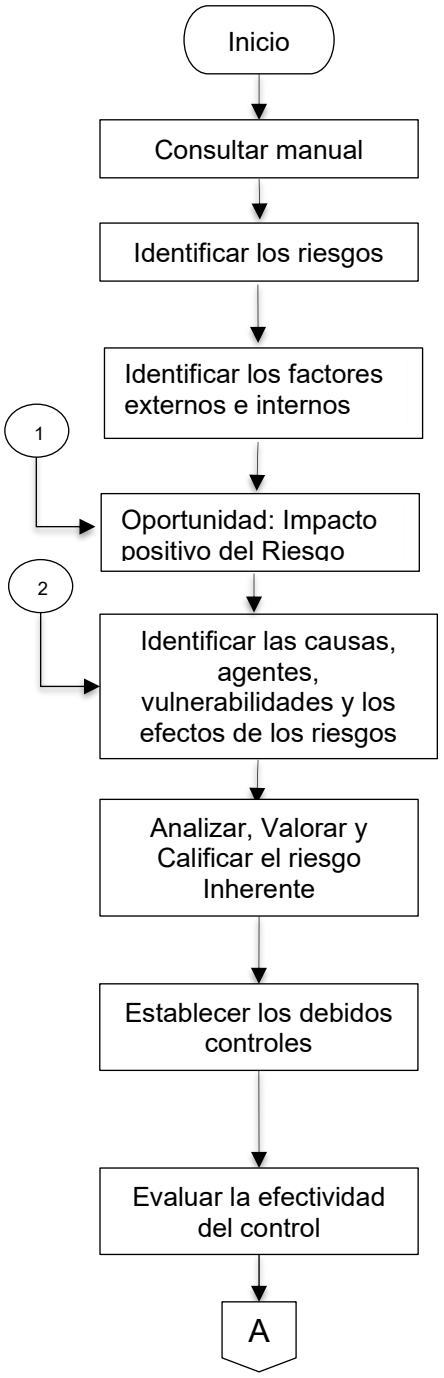
Para garantizar la eficacia en la gestión del riesgo, se establecen los siguientes lineamientos operativos:

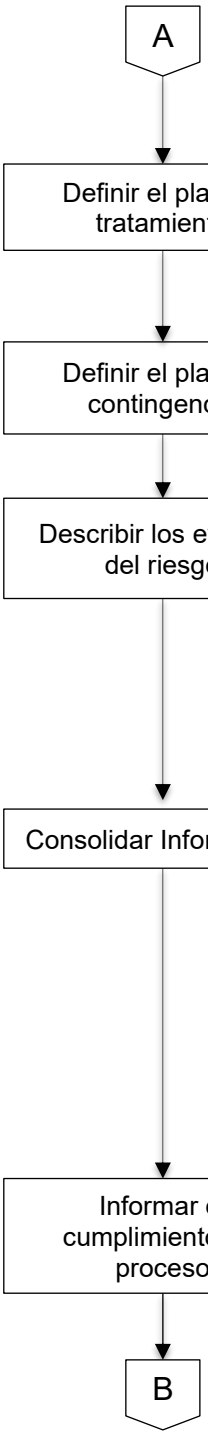
- Monitoreo cuatrimestral de los riesgos estratégicos y de corrupción por parte de la Oficina Asesora de Planeación Estratégica y la Oficina de Control Interno de Gestión.
- La Oficina Asesora de Planeación Estratégica notificará, mediante correo institucional, a todas las unidades académico-administrativas sobre sus responsabilidades en la gestión del riesgo y las fechas clave para el seguimiento de los controles asignados.
- Convocatoria a reuniones de seguimiento en las que los responsables deberán presentar evidencia del seguimiento realizado a los controles implementados, así como su respectiva evaluación.
- Plazo máximo de cinco (5) días hábiles para actualizar la información en la plataforma KAWAK en caso de identificarse incumplimientos en el seguimiento.
- Entrega de informe trimestral de seguimiento a riesgos y controles de procesos y procedimientos, elaborado por la División de Gestión de Calidad, a la Oficina Asesora de Planeación Estratégica, asegurando su alineación con los estándares y procesos institucionales.
- Generación de informes y boletines conjuntos entre la Oficina Asesora de Planeación Estratégica y la División de Gestión de Calidad, sobre el estado de la gestión de los riesgos institucionales.
- Actualización y publicación periódica de los mapas de riesgos institucionales en el micrositio web de la Universidad.

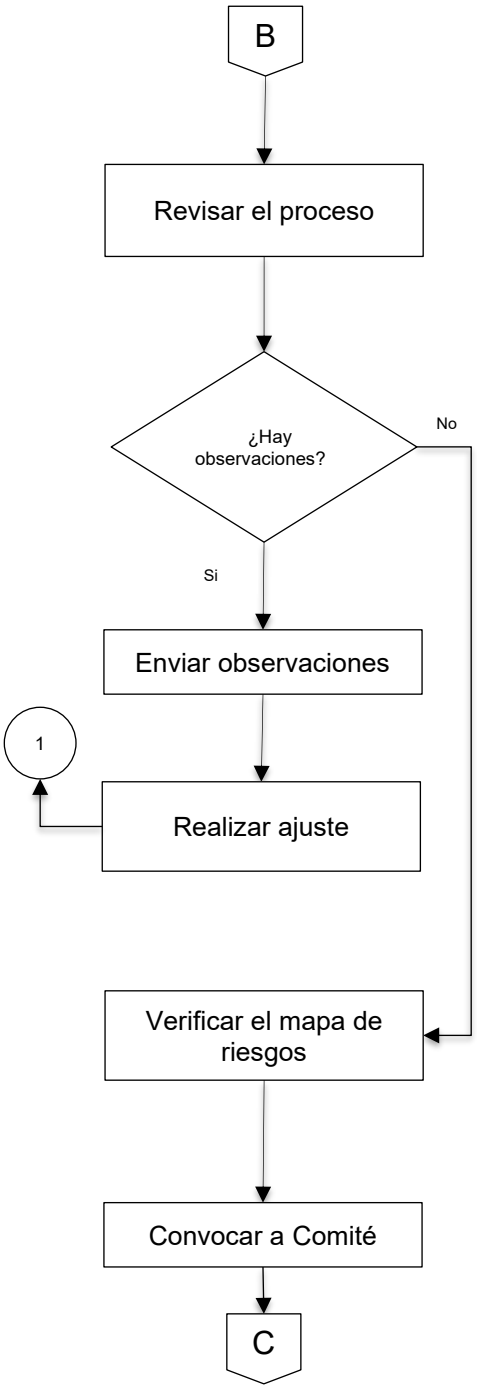
- Realización de auditorías e informes de seguimiento a los riesgos de corrupción y riesgos estratégicos institucionales por parte de la Oficina de Control Interno de Gestión.

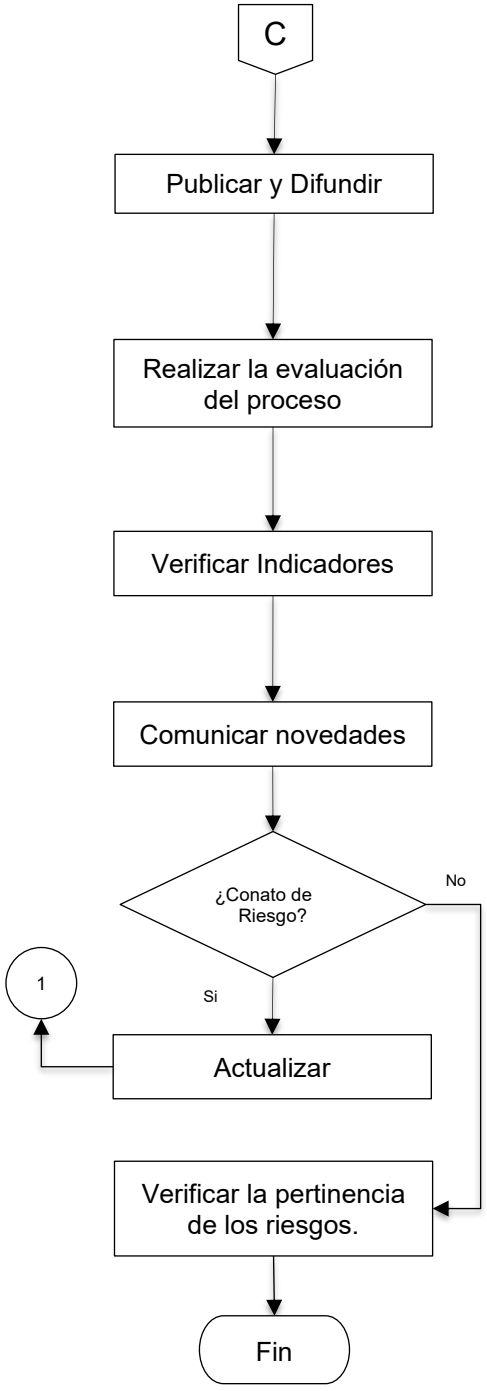
Con este enfoque, la Universidad Militar Nueva Granada refuerza su compromiso con una gestión de riesgos estructurada, transparente y efectiva, que garantice la mejora continua y el cumplimiento de sus objetivos estratégicos.

6. Descripción de Actividades

Actividad	Descripción de la Actividad	Responsable
	1. Consultar el manual para documentar y/o actualizar los aspectos relacionados con los riesgos y oportunidades. 2. Relacionar los riesgos que puedan llegar a afectar el logro de los objetivos institucionales o del proceso. 3. Establecer el contexto estratégico identificando los factores externos e internos. 4. Identificar y definir las causas del riesgo identificado, las vulnerabilidades y los efectos asociados a los riesgos. 5. Analizar y Calificar el riesgo inherente desde los niveles de impacto y probabilidad. 6. Establecer los controles del riesgo 7. Llevar a cabo la validación de la efectividad de los controles de conformidad con los criterios previamente establecidos.	1. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 2. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 3. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 4. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 5. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 6. Líder de proceso, equipo de trabajo y División de Gestión de Calidad 7. Líder de proceso, equipo de trabajo y División de Gestión de Calidad

Actividad	Descripción de la Actividad	Responsable
	8. Definir el plan de tratamiento, formulando acciones que permitan realizar seguimiento al riesgo identificado. 9. Definir el plan de contingencia con el fin de gestionar el riesgo materializado. 10. En caso de materializarse el riesgo se debe definir las posibles causas, la identificación de los controles que fallaron, la documentación de las acciones inmediatas la cuantía de la perdida y los archivos de soporte de la novedad. 11. Consolidar la información en el módulo de configuración del mapa de riesgo en el Sistema KAWAK. 12. Informar a la Oficina Asesora de Planeación Estratégica mediante correo sobre el cumplimiento del proceso.	Líder de proceso y ETIR Líder de proceso y ETIR Líder de proceso y ETIR ETIR y OFIPLA ETIR

Actividad	Descripción de la Actividad	Responsable
	13. Revisar la información diligenciada y analizada del proceso en el módulo de gestión del riesgo en el sistema KAWAK. 14. Enviar al líder del proceso las observaciones. 15. Realizar el ajuste al mapa de riesgos según las observaciones realizadas por la Oficina Asesora de Planeación Estratégica. 16. Verificar en el Sistema KAWAK el mapa de riesgos de cada proceso con el fin de consolidar el mapa de riesgos institucional. 17. Convocar al Comité de Gestión y Desempeño para validar los resultados obtenidos.	Jefe Oficina Asesora de Planeación Estratégica Jefe Oficina Asesora de Planeación Estratégica Líder de proceso, equipo de trabajo y División de Gestión de Calidad Jefe Oficina Asesora de Planeación Estratégica Jefe Oficina Asesora de Planeación Estratégica

Actividad	Descripción de la Actividad	Responsable
	18. Publicar y difundir el mapa de riesgos institucional. 19. Realizar la evaluación del proceso conforme a los tiempos definidos. 20. Verificar los indicadores de cumplimiento del mapa de riesgos del proceso. 21. Comunicar cambios y niveles de cumplimiento sobre los riesgos a la Oficina Asesora de Planeación Estratégica. 22. Actualizar los riesgos. 23. Verificar que los riesgos del proceso no requieran actualización y estén en cumplimiento.	Jefe Oficina Asesora de Planeación Estratégica División de Gestión de Calidad y OFIPLA Líder de proceso, División de Gestión de Calidad y OFIPLA Líder de proceso y División de Gestión de Calidad Líder de proceso, equipo de trabajo y Equipo Técnico Integral de Riesgos (División de Gestión de Calidad y Oficina Asesora de Planeación Estratégica) Jefe Oficina Asesora de Planeación Estratégica

7. Documentos Relacionados

La siguiente lista incluye los principales documentos de referencia utilizados para la formulación y aplicación del presente manual de gestión del riesgo en la Universidad Militar Nueva Granada. Esta relación será ampliada progresivamente, conforme se consolide una cultura organizacional orientada al riesgo.

Documento	Descripción	Versión / Fecha
Mapa de Riesgos Institucional	Registro de los riesgos identificados, valorados y priorizados en la plataforma KAWAK.	Actualización cuatrimestral (última versión visible en KAWAK y página web)
Guía para la Administración del Riesgo y el Diseño de Controles – DAFP	Documento base para la gestión del riesgo en entidades públicas.	Versión 6 – noviembre de 2022
Análisis DOFA por componente estratégico	Instrumento de diagnóstico institucional que identifica factores críticos internos y externos que pueden representar riesgos u oportunidades.	Versión 2024
Normativas internas asociadas al control interno y calidad	Directrices adoptadas en el marco del MECI, el SIG y los sistemas basados en ISO.	Actualización continua según procesos de auditoría y revisión

7.1. Normatividad

Para garantizar una gestión del riesgo coherente con el marco normativo vigente y con las mejores prácticas nacionales e internacionales, se adopta el siguiente conjunto de normas, agrupadas según su naturaleza y aplicabilidad:

1. Normativa Colombiana (Leyes, Decretos y Resoluciones)

- **Ley 87 de 1993:** Establece las normas para el ejercicio del Control Interno en entidades públicas. Es la base legal del Sistema de Control Interno y su relación con la gestión de riesgos.
- **Ley 1474 de 2011 (Anticorrupción):** Modifica la Ley 87 de 1993. Refuerza la prevención y sanción de actos de corrupción, clave en la identificación y tratamiento de riesgos de corrupción.
- **Ley 805 de 2003:** [*Revisar su pertinencia específica en este contexto; si no guarda relación directa con la gestión de riesgos o control interno, podría eliminarse.*]
- **Decreto 1537 de 2001:** Reglamenta la Ley 87 respecto a los elementos técnicos y administrativos del Sistema de Control Interno, orientando su implementación y seguimiento.
- **Decreto 1599 de 2005:** Adopta el Modelo Estándar de Control Interno (MECI), el cual incluye la gestión del riesgo como uno de sus componentes clave.

- **Decreto 1072 de 2015:** Compila las normas sobre el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), que incluye el análisis de riesgos laborales.
- **Resolución 312 de 2019:** Define los estándares mínimos del SG-SST, incluyendo obligaciones sobre la identificación y control de riesgos laborales.
- **Resolución 20223040040595 de 2022:** Adopta la metodología para el diseño, implementación y verificación de los Planes Estratégicos de Seguridad Vial, que requiere la gestión de riesgos en la movilidad institucional.
- **Decreto 1122 de 2024:** Establece lineamientos para la implementación del Programa de Transparencia y Ética Pública (PTEP), el cual articula acciones de gestión del riesgo con enfoque preventivo frente a hechos de corrupción.

2. Normas Internacionales y Técnicas (ISO y NTC)

- **NTC ISO 31000:2018 – Gestión del Riesgo:** Norma central que proporciona directrices para la gestión de riesgos en todo tipo de organizaciones.
- **NTC ISO 31010:2019 – Técnicas de Evaluación del Riesgo:** Complementa la ISO 31000 y presenta herramientas específicas para el análisis y valoración de riesgos.
- **NTC ISO 9001:2015 – Sistema de Gestión de la Calidad:** Incluye el enfoque basado en riesgos como principio de gestión para asegurar la mejora continua.
- **NTC ISO 14001:2015 – Sistema de Gestión Ambiental:** Requiere la identificación y control de riesgos ambientales.
- **NTC ISO 45001:2018 – Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST):** Establece los requisitos para gestionar riesgos laborales y condiciones de seguridad.
- **NTC ISO 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI):** Aplica a la gestión de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información institucional.
- **NTC ISO 21001:2018 – Sistemas de Gestión para Organizaciones Educativas:** Orienta la gestión de riesgos en procesos educativos, con enfoque en la mejora del aprendizaje y el cumplimiento de requisitos de partes interesadas.

3. Guías Técnicas y Lineamientos Institucionales

- **Guía para la Administración de Riesgos (DAFP, 2014):** Documento base para la implementación del componente de riesgo en el MECI.
- **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP, 2022):** Actualización de la guía de 2014. Incluye orientaciones específicas para riesgos de gestión, corrupción y seguridad digital, utilizadas en este manual.
- **Sistema Integrado de Gestión de la UMNG – SIG:** Alineado con los estándares ISO y el MECI, integra la gestión de riesgos en los procesos académicos, administrativos y estratégicos.
- **Acuerdo 13 de 2010:** Estatuto General de la UMNG. Establece el marco organizacional dentro del cual deben implementarse los sistemas de control, seguimiento y gestión de riesgos.