Guía de administración del riesgo

Oficina Asesora de Planeación

AÚN+ incluyente e innovadora
PERIODO 20.24

Tabla de Contenido

1 OBJETIVO GENERAL

Fortalecer la comunicación, entendimiento y apropiación de las directrices e instrucciones generales y básicas para la administración de los riesgos en la Universidad del Magdalena.

1.1. OBJETIVOS ESPECÍFICOS

- Establecer la metodología que permita determinar la política, identificación, el análisis y valoración para la adecuada administración de los riesgos.
- Garantizar la estandarización y unidad de criterio para el adecuado manejo de los riesgos que surjan en cada proceso.
- Coadyuvar a la gestión institucional en el contexto estratégico del manejo de los riesgos.
- Fomentar entre los funcionarios el enfoque basado en riesgos encaminado a identificar, analizar su contexto y administrar los riesgos.

2 ALCANCE

Esta guía establece la política de administración de riesgos de la Universidad, provee lineamientos metodológicos necesarios para el establecimiento, manejo, tratamiento, seguimiento y actualización de riesgos. La presente guía, de Administración del Riesgo debe ser extensible y aplicable a todos los procesos de la institución.

3 RESPONSABLES Y PARTICIPANTES

Líderes de procesos: responsables de la aplicación metodológica definida en esta guía.
Oficina Asesora de Planeación y Grupo de Gestión de la Calidad: serán los responsables de la actualización de la presente guía y velará por la correcta aplicación de la misma.
Grupo de Control Interno: será responsable de hacerle el seguimiento a la efectividad de los controles, así como las acciones implementadas para evitar la materialización de los riesgos.

4 GENERALIDADES

La presente Guía incluye los lineamientos establecidos en el Manual Operativo del Modelo Integrado de Planeación y Gestión, que incorpora la actualización del Modelo Estándar de Control Interno para el Estado Colombiano MECI, la Guía para la Administración del Riesgo del DAFP en su versión 6, la NTC ISO 31000 Gestión del Riesgo – Principios Directrices e ISO 9001:2015 en su numeral 6.1, emitidas por el ICONTEC, y el Documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano” V2 en su componente Gestión del Riesgo de Corrupción.

4.1 NORMAS DE REFERENCIA NACIONAL

- **Constitución Política Nacional Artículo 209**. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley.
- **Ley 87 de 1993. Artículo 2.** a) Proteger los recursos buscando su adecuada administración ante posibles riesgos que los afectan. f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten y que puedan afectar el logro de los objetivos.
- **Directiva Presidencial 09 de 1999.** Lineamientos para la implementación de la política de lucha contra la corrupción
- **Norma Técnica Colombiana NTC ISO 31000.** Gestión del Riesgo – Principios Directrices. Emitido por el Instituto Colombiano De Normas Técnicas Y Certificación – ICONTEC.
- **Ley 1474 de 2011.** Estatuto Anticorrupción. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Guía para la Administración del Riesgo.** Emitido por el Departamento Administrativo de la Función Pública (versión 6).
- **Decreto 1083 de 2015 –Titulo 21:** Sistema de Control Interno.
- **Decreto1499 de 2017**: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano" V2**. en su componente Gestión del Riesgo de Corrupción.
- **Modelo Integrado de Planeación y Gestión.** MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto1499 de 2017.
- **Anexo 2 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas:** se encuentra dentro de los anexos de la guía para la administración del riesgo v6 y es emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones –MINTIC

4.2 NORMAS DE LA UNIVERSIDAD DEL MAGDALENA

- **Resolución Rectoral 327 de 2003.**Mediante la cual se reglamenta y adopta un sistema para la administración de riesgos de corrupción en la Universidad del Magdalena y se Conforma el Comité de Coordinación de Administración del Riesgo
- **Resolución Rectoral 534 de 2005.**Por medio de la cual se crea el sistema de control interno de la universidad del Magdalena.
- **Acta Rectoral 001 de 2005.** Acta de compromiso para la implementación del MECI
- **Resolución Rectoral 220 de 2008.** Por medio de la cual se conforman los equipos Directivo, Operativo y Evaluador del Diseño e implementación Sistema de Control Interno de la Universidad con base en el Modelo Estándar de Control Interno – MECI.
- **Resolución Rectoral 250 de 2017:** por la cual se adopta el sistema COGUI +: Sistemas de gestión y se dictan otras disposiciones.

- **Resolución Rectoral 374 de 2017:** Por la cual se conforma el Comité de Coordinación del Sistema de Control Interno y se dictan otras disposiciones.
- **Acuerdo Superior N° 23 de 2019.** Por el cual se actualizan las Políticas de Integridad y Buen Gobierno de la Universidad del Magdalena.

4.3 GLOSARIO DE TÉRMINOS

- **Administración de riesgos:** la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos. "Conjunto de elementos de control que, al interrelacionarse, permiten a la Entidad pública gestionar políticas para evaluar aquellos eventos negativos, tanto internos como externos, que pueden afectar o impedir el logro de sus objetivos institucionales, o los eventos positivos, que pueden identificar oportunidades para un mejor cumplimiento de su función y mantener la estabilidad de la entidad." [1]

- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

- **Análisis de Beneficio-Costo:** Una herramienta de la Administración de Riesgos usada para tomar decisiones sobre las técnicas propuestas para la administración de los riesgos, en la cual se valoran y comparan los costos, financieros y económicos, de implementar la medida, contra los beneficios generados por la misma. *Una medida de la Administración del riesgo será aceptada siempre que el beneficio valorado supere al costo.*

- **Acciones:** permite identificar según la calificación del riesgo, el tratamiento que se le va dar a este: Evitar o prevenir, reducir, dispersar, transferir y asumir riesgos.

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Causa:** Son los medios, circunstancias y agentes que generan los riesgos.

- **Causa Inmediata**: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz**: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

[1]Manual Operativo del Modelo Integrado de Planeación y Gestión – Dimensión 7

- **Control:** Medida que permite reducir o mitigar un riesgo.

- **Control Automático:** Utilizan herramientas tecnológicas como sistemas de información o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros.

- **Control Manual:** Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros

- **Costo:** Se entiende por costo las erogaciones, directas e indirectas en que incurre la institución en la prestación de un servicio o manejo de un riesgo.

- **Consecuencia**: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Gestión del Riesgo**: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Entorno.** Todos los Factores que rodean e influyen en la vida y desarrollo de la institución. Los Factores del entorno se clasifican en internos (controlables) y externos (no controlables)

- **Evento:** Incidente o situación, que ocurre en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

- **Factores de riesgo:** Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- **Frecuencia:** Medida de ocurrencia de un evento o efectos expresado como la cantidad de veces que ha ocurrido un evento o efecto en un tiempo dado.

- **Impacto:** Consecuencias que puede ocasionar a la institución la materialización del riesgo.

- **Indicador**: Es un criterio de medición y de evaluación cuantitativa o cualitativa. Es la valoración de una o más variables que informa sobre una situación o tendencia y soporta la toma de decisiones.

- **Integridad:** Propiedad de exactitud y completitud.
- **Monitoreo:** comprobar, supervisar, observar críticamente, o registrar el progreso de una actividad, acción o sistema en forma sistemática para identificar cambios.

- **Mapa de riesgo**: documento con la información resultante de la gestión del riesgo.

- **Nivel del riesgo**: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Plan de contingencia:** Plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la institución.

- **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

- **Plan Anticorrupción y de Atención al Ciudadano**: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

- **Responsables:** Son las personas encargadas de adelantar las acciones para gestionar el riesgo.

- **Riesgo de Gestión:** Posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el de los objetivos de la institución o del proceso.

- **Riesgo de Corrupción:** Posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de la Universidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo Fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

- **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su posibilidad de ocurrencia o impacto.

- **Riesgo Residual:** Es el riesgo que queda cuando las técnicas de la administración del riesgo han sido aplicadas.

- **Riesgo de Seguridad de la Información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguimiento:** Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la planeación futura.

- **Sistema:** Conjunto de cosas o partes coordinadas, ordenadamente relacionadas entre sí, que contribuyen a un determinado objetivo.

- **Tolerancia del riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Vulnerabilidad**: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5 INTRODUCCION

Para el Estado Colombiano, el Decreto 1083 de 2015 establece en el artículo 2.2.21.5.4 que todas las entidades de la Administración Pública deben contar con una política de Administración de Riesgos tendiente a darle un manejo adecuado a los riesgos, con el fin de lograr de la manera más eficiente el cumplimiento de sus objetivos y estar preparados para enfrentar cualquier contingencia que se pueda presentar.

El Sistema de Control Interno, se articuló al Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión –MIPG (Dimensión 7), a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades. El Control Interno es transversal a la gestión y desempeño de las entidades y se implementa a través del Modelo Estándar de Control Interno – MECI.

La actualización del Modelo Estándar de Control Interno para el Estado Colombiano – MECI, se efectuó a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5 de la Ley 87 de 1993.

La presente guía incorpora la metodología establecida por la función pública para la identificación, análisis, valoración y evaluación del riesgo, así como el establecimiento de controles.

La Universidad del Magdalena define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos -MIPG, así como los del Modelo Estándar de Control Interno, los lineamientos de la Guía para la administración del riesgo de DAFP en su versión 6 (2022), la cual articula los riesgos de gestión, corrupción, fiscales y de seguridad de la información.

6 MARCO CONCEPTUAL[2]

Teniendo en cuenta que la Universidad cuenta con modelo de gestión integral, consideró estas normas en el presente marco conceptual.

La Norma ISO 9001:2015 en su numeral 6.1 Acciones para abordar los riesgos y las oportunidades, establece que se debe hacer una planificación del Sistema de Gestión de la Calidad, la organización debe considerar las cuestiones referidas en el apartado 4.1, los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades, que la organización debe planificar las acciones para abordar estos riesgos y oportunidades, las

[2]Tomado del Departamento Administrativo de la Función Pública

cuales deben ser proporcionales al impacto potencial en la conformidad de los productos y los servicios; y en su nota 1, indica que, las opciones para afrontar los riesgos pueden incluir: evitar riesgos, asumir riesgos para perseguir una oportunidad, eliminar la fuente de riesgo, cambiar la probabilidad o las consecuencias, compartir el riesgo o mantener riesgos mediante decisiones informadas.

El Documento Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano MECI, establece que las entidades para dar cumplimiento al componente de Administración de riesgos, cuentan con algunas herramientas, entre las cuales se pueden destacar La Cartilla "Guía para la Administración del Riesgo" propuesta por el DAFP y La norma NTC ISO 31000, y que deben tener en cuenta dentro de la administración del riesgo el cumplimiento del artículo 73 de la Ley 1474 de 2011.

En este sentido la Secretaria de Transparencia de la presidencia de la Republica, junto con el DAFP, diseñó el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano” el cual da pautas metodológicas y establece que para la construcción del mapa de riesgos de corrupción se debe remitir al documento Guía para la gestión de riesgos de corrupción, dado por el DAFP.

La estructura del modelo estándar de control interno MECI del DAFP, es dada por módulos y un eje transversal. Por lo tanto, el componente de Administración del Riesgo, al ser un componente del Módulo de Control de Planeación y Gestión, se sirve de la planeación (misión, visión, objetivos, metas, factores críticos de éxito), del campo de aplicación (procesos, proyectos, sistemas de información), del Componente Direccionamiento Estratégico y todos sus elementos. Y su mirada sistémica contribuye a que la entidad no sólo garantice la gestión institucional y el logro de los objetivos, sino que fortalece el ejercicio del Control Interno en las entidades de la Administración Pública.

Ilustración 1. Administración del Riesgo como componente del módulo de Planeación y Gestión

El enfoque dado por la Guía de Administración de Riesgos (que da respuesta al MECI), está estructurado de la siguiente manera:

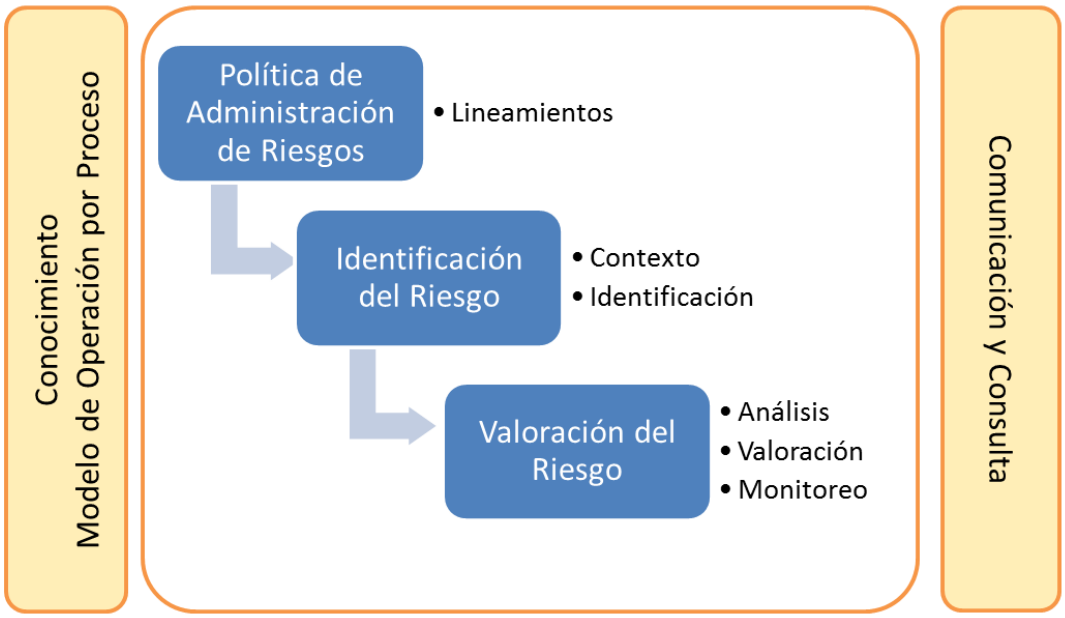


Ilustración 2. Enfoque dado por la Guía de Administración de Riesgos (que da respuesta al MECI)

El enfoque dado por la NTC ISO 31000 está estructurado según la siguiente figura[3].

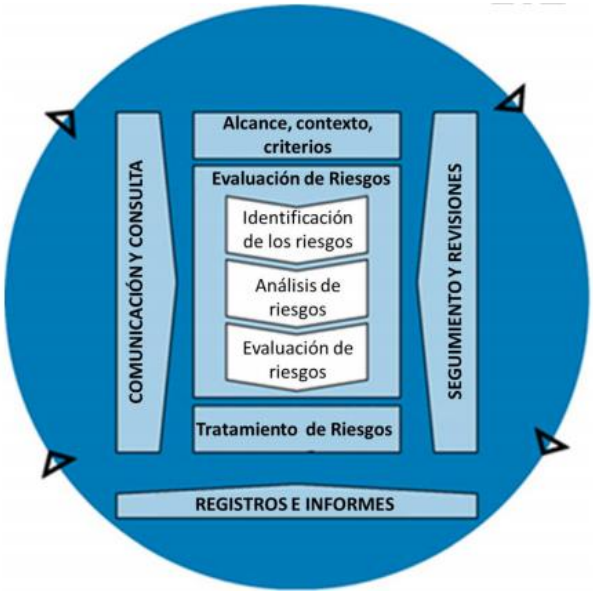


Ilustración 3. Enfoque dado por la NTC ISO 31000

[3] Tomado de la Norma ISO 31000 de la Gestión del Riesgo

El enfoque dado por la Guía para la Gestión de Riesgos de Corrupción (que da respuesta al artículo 73 de la Ley 1474 de 2011), esta estructura de la siguiente manera:

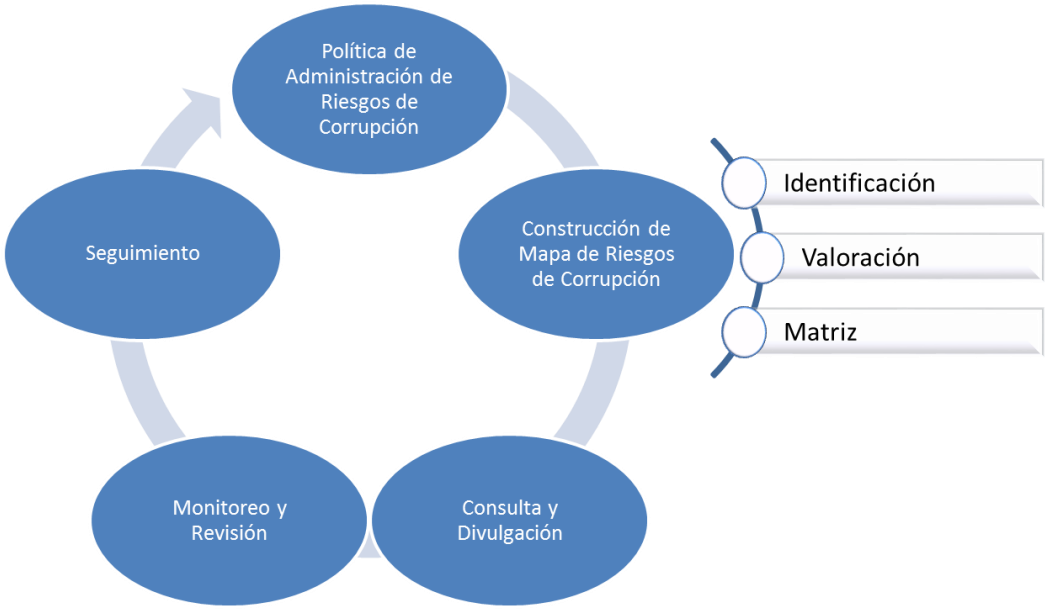


Ilustración 4. Enfoque dado por la Guía para la Gestión de Riesgos de Corrupción

Teniendo en cuenta que los enfoques presentados por cada una de las normas, documentos y guías se complementan, a continuación, se presenta la metodología de administración de riesgos de la Universidad.

7 CONTEXTO ESTRATÉGICO

Contribuye al control de la Universidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que se actúe en dirección contraria a los propósitos institucionales.

De acuerdo con la norma NTC ISO 31000, la organización debiera analizar y comprender su contexto interno y externo cuando diseñe el marco de referencia para administrar/gestionar sus riesgos.

El análisis del contexto externo de las organizaciones puede incluir, pero no limitarse a:

- los factores sociales, culturales, políticos, legales, reglamentarios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local;
- los impulsores clave y las tendencias que afectan a los objetivos de la organización;
- las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas;
- las relaciones contractuales y los compromisos;
- la complejidad de las redes y dependencias.

El análisis del contexto interno de las organizaciones puede incluir, pero no limitarse a:

- la visión, la misión y los valores;
- la gobernanza, la estructura de las organizaciones, los roles y la rendición de cuentas;
- las estrategias, los objetivos y las políticas;
- la cultura de las organizaciones;
- las normas, las directrices y los modelos adoptados por las organizaciones;
- las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías);
- los datos, los sistemas de información y los flujos de información;
- las relaciones con partes interesadas internas, teniendo en cuenta sus percepciones y valores;
- las relaciones contractuales y los compromisos; — las interdependencias e interconexiones.

Para los Mapas de Riesgos por Proceso se recomienda tener claro la Caracterización del Proceso, así como tener claros los objetivos, las estrategias, y el alcance.

Con este elemento de Contexto Estratégico se busca que la Universidad obtenga los siguientes resultados:

- Establecer la normativa interna y externa (Nacional y/o Internacional) que le aplique.
- Identificar el contexto externo que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la universidad.
- Identificar el contexto interno y de proceso que pueden ocasionar la presencia de riesgos con base en el análisis de los componentes Ambiente de Control, Direccionamiento Estratégico y demás estudios que sobre la cultura organizacional y el clima laboral se hayan adelantado en la universidad.
- Aportar información que facilite y enriquezca las demás etapas de la Administración del Riesgo.

7.1 RIESGOS DE GESTIÓN

Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de la Universidad[4].

Contexto Externo, Se determinan las características o aspectos esenciales del entorno en el cual opera la Universidad.
Contexto Interno, son propios de la Universidad. Se determinan las características o aspectos esenciales del ambiente en el cual la institución busca alcanzar sus objetivos.

Contexto del Proceso, Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. *Como herramienta básica para el análisis del contexto del*

[4] Manual Operativo del Modelo Integrado de Planeación y Gestión – Dimensión 7

proceso se sugiere utilizar las caracterizaciones de los mismos, donde es posible contar con este panorama.

Tabla 1. Contexto Estratégico Riesgos de Gestión

Contexto EXTERNO	Contexto INTERNO	Contexto del PROCESO
AMENAZAS	DEBILIDADES	DEBILIDADES
ECONÓMICOS Y FINANCIEROS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.	**FINANCIEROS**: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.
MEDIOAMBIENTALES Y CAMBIO CLIMÁTICO: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**PERSONAL:** Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional	**INTERACCIONES CON OTROS PROCESOS:** Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes
POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación.	**PROCESOS:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento	**TRANSVERSALIDAD:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la universidad
SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público	**TECNOLOGÍA:** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información	**PROCEDIMIENTOS ASOCIADOS:** Pertinencia en los procedimientos que desarrollan los procesos
TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	**ESTRATÉGICOS:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo	**RESPONSABLES DEL PROCESO:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso
LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).	**COMUNICACIÓN INTERNA:** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones	**COMUNICACIÓN ENTRE LOS PROCESOS:** Efectividad en los flujos de información determinados en la interacción de los procesos.
		ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

7.2 RIESGOS DE CORRUPCIÓN

Se busca de manera general "identificar un conjunto sistemático de situaciones que, por sus características, pueden originar prácticas corruptas", asociándolas a cada uno de los procesos y procedimientos de la respectiva entidad[5].

[5] Documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"

Para ello la Universidad ha definido teniendo en cuenta diferentes fuentes de información las Amenazas (Externos) y Debilidades (Internos).

Tabla 2. Contexto Estratégico Riesgos de Corrupción

Contexto EXTERNO	AMENAZAS	• Cambios regulatorios y técnicos • Apatía de los grupos de interés • Recortes presupuestales • Desconocimiento de los usuarios en el manejo del sistema de tramites • Gran demanda de información personalizada por la ciudadanía • Presiones por parte de personas, gremios o entidades externas
Contexto INTERNO	DEBILIDADES	• Ausencia cultura de ética y buen gobierno • Cambios en la alta dirección • Falta de control al poder • Discrecionalidad en la toma de decisiones • Alta rotación del personal • Desmotivación de funcionarios • Falta cualificación del personal • Concentración de conocimiento • No distribución de acuerdo competencias • Omisión de procedimientos • Falta de planeación y coherencia procesos • Baja automatización de seguimiento • Deficiente gestión documental • Asimetrías de la información

7.3 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Hace referencia a las vulnerabilidades y amenazas que se encuentran en el entorno digital de la organización e incluye aspectos relacionados con el ambiente físico, digital y las personas[6].

Para este tipo de riesgo más que la identificación del contexto, se requiere una identificación del grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Activo		• Software • Hardware • Información

7.4 RIESGOS FISCALES

Hace referencia al daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.[7]

[6] Guía para la administración del riesgo y el diseño de controles en entidades públicas.
[7] Guía para la administración del riesgo y el diseño de controles en entidades públicas V6.

Para este tipo de riesgos se debe tener especial cuidado en no confundir con el daño fiscal, por lo tanto, la definición debe estar enfocada a la probabilidad o posibilidad de que ocurra un evento que pueda afectar negativamente a los recursos, bienes y/o intereses patrimoniales de la universidad.

La Guía para la administración del riesgo y el diseño de controles en entidades públicas, resume lo anterior de la siguiente manera:

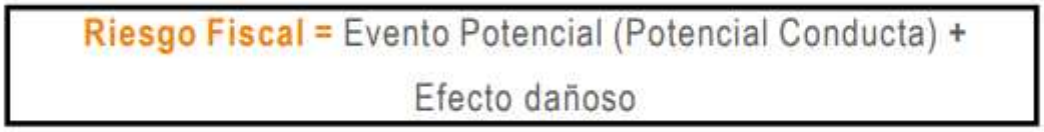


Ilustración 5. Riesgo fiscal - DAFP

8 METODOLOGIA PARA LA ADMINISTRACIÓN DE RIESGOS[8]

La administración del riesgo parte de una política institucional definida y respaldada por la dirección que se compromete a manejar el tema dentro de la Universidad. Con el fin de asegurar dicho manejo, es importante establecer el entorno de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos.

La metodología para la Administración del Riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la Universidad, el conocimiento de la misma desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo que son: política de administración del riesgo, identificación de riesgos y valoración de riesgos y finalmente de la definición e implantación de estrategias de comunicación transversales a toda la institución para que su efectividad pueda ser evidenciada.

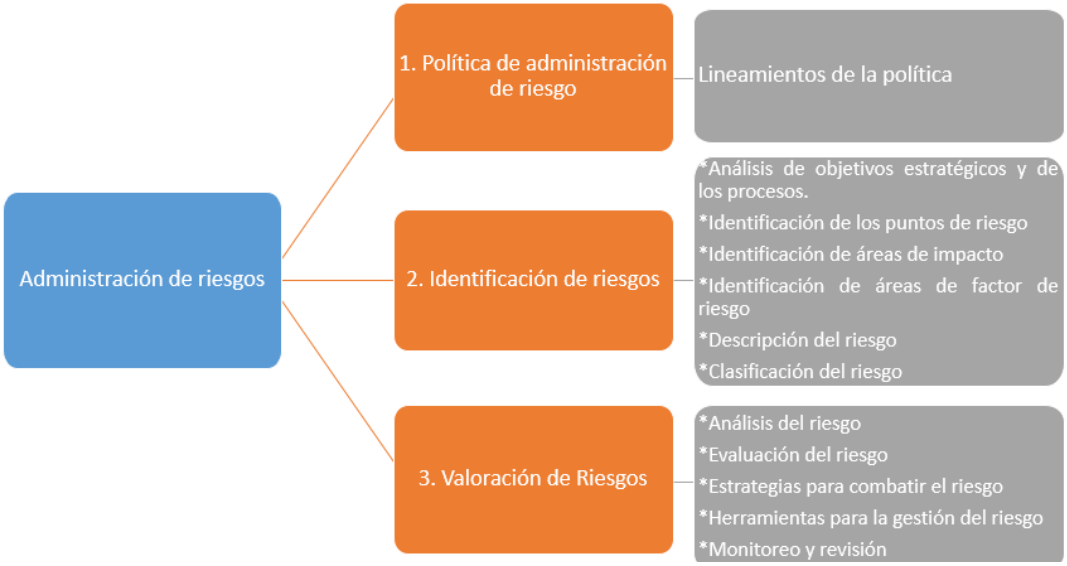


Ilustración 6. Metodología Administración del Riesgo

[8]Guía para la administración del riesgo y el diseño de controles en entidades públicas V6.

8.1 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La política señala qué debe hacerse para efectuar el control y su seguimiento, basándose en los planes y los objetivos institucionales o por procesos.

Ilustración 7. Política Administración del Riesgo

8.1.1 Definición

La política contenida en esta Guía de Administración del Riesgo permitirá identificar las opciones para tratar y manejar los riesgos, basados en el análisis y la valoración de los mismos, convirtiéndose en una herramienta fundamental con mirada sistémica que contribuye a que la Universidad no sólo garantice la gestión institucional y el logro de los objetivos, sino que fortalece el ejercicio del Control Interno.
La política definida en este documento transmite la posición de la Alta Dirección y establece la guía de acción necesaria para todos los servidores de la Universidad.

- **OBJETIVO.** Establecer los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de toda naturaleza a los que se enfrenta la Universidad.

  Objetivos Específicos

  - Orientar la toma de decisiones respecto al tratamiento de los riesgos.
  - Facilitar el cumplimiento de los objetivos institucionales y evitar lesiones al interés de la Universidad para la obtención de un beneficio particular.
  - Brindar una herramienta que facilite a la Universidad una adecuada administración de los riesgos.
  - Facilitar la aplicación de la metodología de administración de los riesgos en los procesos de la Universidad.

- **ALCANCE**

  La política de administración del riesgo contribuye al control interno de la Universidad, fomentando la cultura del autocontrol al interior de los procesos, la cual debe ser

aplicada por todos los líderes y funcionarios de la Institución, de acuerdo con las responsabilidades definidas en el presente documento. El desarrollo de la política de administración del riesgo implica tomar el contexto estratégico que es la base para la identificación del riesgo para cada proceso, determinar las posibles causas internas y externas, establecer los efectos de los riesgos, definir, calificar y evaluar los riesgos, definir y evaluar los controles, establecer respuesta a los riesgos, consolidar la información en una matriz que permita visualizar la relación de dichos riesgos con los procesos institucionales, realizar evaluación y seguimiento a acciones, y mantener y actualizar los mapas.

- **ROLES Y RESPONSABILIDADES**

Alta y Media Dirección

- Estimular la cultura de la identificación y prevención del riesgo
- Definir las políticas para la gestión de los riesgos identificados y valorados
- Definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios.
- Así mismo, debe designar a un directivo de primer nivel (debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del MECI y el Sistema de Gestión de la Calidad) que asesore y apoye todo el proceso de diseño e implementación del Componente.

Jefe y Equipo de Oficina Asesora de Planeación

- Responsable de la adecuada ejecución de este componente.
- Implementar y/o mantener las políticas para Administrar los riesgos
- Capacitar a los servidores de la entidad en la construcción y/o mantenimiento del mapa de riesgos por proceso.
- Construir y/o mantener el mapa de riesgo institucional.

Jefe y Equipo de Oficina Control Interno

- Evaluar la ejecución de las acciones de mejora llevadas a cabo por los procesos y con base en dicha evaluación, realizar recomendaciones preventivas y/o correctivas a los líderes de los procesos.
- Verificar que en la entidad se implementen políticas para la Administración del Riesgo y que estas sean mecanismos reales.

Líderes o Responsables de los Procesos

- Identificar, Analizar y Valorar los riesgos
- Elaborar el mapa de riesgo
- Identificar las acciones necesarias para administrar el riesgo
- Establecer cronograma y ejecutar las acciones definidas en el mapa de riesgo
- Evaluar, validar, ajustar y actualizar periódicamente el mapa de riesgo.

8.1.2 Divulgación

- **COMUNICACIÓN Y CONSULTA**

Su socialización se realizará en cumplimiento del procedimiento GC-P01 Procedimiento para el control de documentos y registros, en el cual se especifica la publicación de documentos en el portal diseñado para tal fin.
Para conocimiento y consulta, mediante correo electrónico se comunicará a todos los procesos la actualización y/o mejora de la presente guía, en la cual se especifican las políticas para administrar los riesgos.

- **DESARROLLO**

Para su ejecución y monitoreo, se apoyará en el documento DP-G02 Guía de Administración del Riesgo, el procedimiento DP-P03 Procedimiento para la Administración del Riesgo, y el instructivo DP-I02 Instructivo Creación de Mapas de Riesgos.

- **MANTENIMIENTO**

Sabiendo que hay situaciones que ocurren al interior de la Universidad y de su entorno que pueden llevar a variar algunas circunstancias presentes al momento de construir la Política, se llevará acabo revisión anual con el fin de que se actualice de ser necesario con respecto a los cambios surtidos, esto teniendo en cuenta que no toda revisión a la política de administración del riesgo implica cambios en la misma, ya que se puede llegar a la conclusión de que ésta se encuentra actualizada, y que las variaciones en el interior de la Universidad y en su entorno no afectan las directrices dadas para el manejo del riesgo. Sin embargo, es importe que se realice una revisión con el fin de asegurar su oportuna actualización.

La revisión, mantenimiento y actualización de los mapas de riesgos tanto por procesos como el institucional debe realizarse al menos una vez al año, o dentro del mismo año cada vez que las condiciones internas o externas cambien. Hace parte del mantenimiento los monitoreos a la ejecución de las acciones establecidas para administrar los riesgos, los cuales deben hacerse cuatrimestralmente.

8.2 IDENTIFICACIÓN DE RIESGOS

El propósito de la identificación de riesgos es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.[9]

El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del análisis del Contexto Estratégico y debe partir de la claridad de los objetivos estratégicos de la Universidad para la obtención de resultados. Es importante centrarse en los riesgos más significativos para la Universidad relacionados con los objetivos de los procesos, programas y/o proyectos, y los objetivos institucionales. Es allí donde, al igual que todos los servidores, adopta un papel proactivo en el sentido de visualizar en sus

[9] NTC ISO31000

contextos estratégicos y misionales los factores o causas que pueden afectar el curso institucional

8.2.1 Riesgos de gestión

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.[10]

Fases para la identificación de riesgos de gestión:

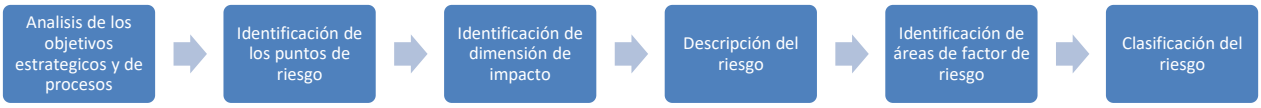
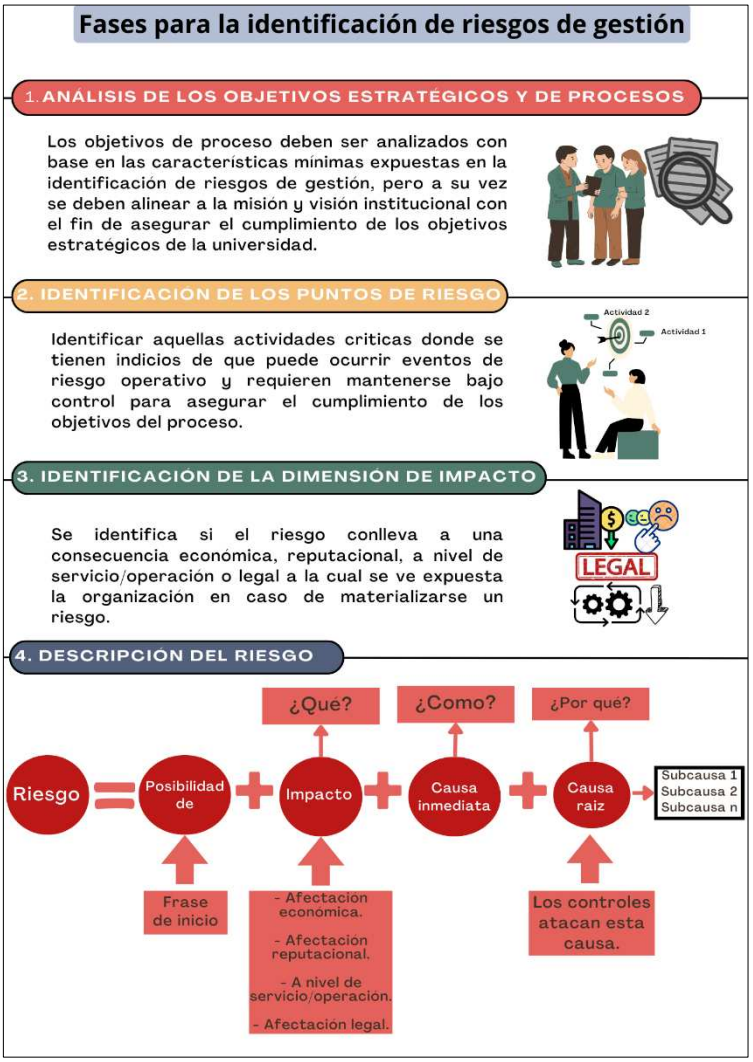


Ilustración 8. Identificación del Riesgo de gestión



[10] Guía para la administración del riesgo y el diseño de controles en entidades públicas

Impacto: las consecuencias que puede ocasionar al proceso la materialización del riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

5. IDENTIFICACIÓN DE ÁREAS DE FACTOR DE RIESGO

A continuación, se presenta un listado con ejemplos de factores de riesgos que se pueden presentar en la universidad:

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos, Errores de grabación, autorización, Errores en cálculos para pagos internos y externos, Falta de capacitación, temas relacionados con el personal.
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto activos, Posibles comportamientos no éticos de los empleados, Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos, Caída de aplicaciones, Caída de redes, Errores en programas.
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes, Incendios, Inundaciones, Daños a activos fijos.
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad, Asalto a la oficina, Atentados, vandalismo, orden público.

6. CLASIFICACIÓN DEL RIESGO

Clasificación	Descripción
Ejecución y administración de procesos.	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Teniendo en cuenta los factores y la clasificación del riesgo a continuación se evidencia su interrelación:

Ilustración 9. Relación entre factores de riesgo y clasificación del riesgo

8.2.2 Riesgos de seguridad de la información

Hace referencia a la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información[11]

Para este tipo de riesgo más que la identificación del contexto, se requiere una identificación del grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

[11] Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de seguridad de la información.

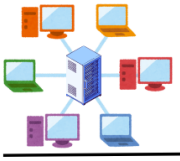
¿QUÉ SON LOS ACTIVOS?

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, se refiere a todos los elementos que necesitan ser protegidos en un entorno digital.

Algunos ejemplos comunes de activos de seguridad digital incluyen:

DATOS:

- Información personal, financiera o confidencial.
- Archivos digitales importantes como documentos, imágenes, videos, etc.



SISTEMAS Y APLICACIONES:

- Servidores, computadoras, redes, sistemas operativos.
- Aplicaciones web, móviles, de escritorio, etc.

IDENTIDADES DIGITALES:

- Cuentas de usuario, contraseñas, credenciales de acceso.
- Certificados digitales, firmas electrónicas.

REPUTACIÓN Y MARCA:

- Presencia en línea de una organización o individuo.
- Imagen y confianza digital.

INFRAESTRUCTURA:

- Equipos de red, centrales de datos, sistemas de respaldo.
- Conexiones de internet, energía eléctrica.

Estos activos digitales deben ser protegidos de amenazas como accesos no autorizados, robo de información, daños, interrupciones del servicio, entre otros.

Ilustración 10. Activos y tipos de activos

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información: **"confidencialidad, Integridad o disponibilidad"**. Por tanto, siempre van a tener la misma estructura en su identificación:

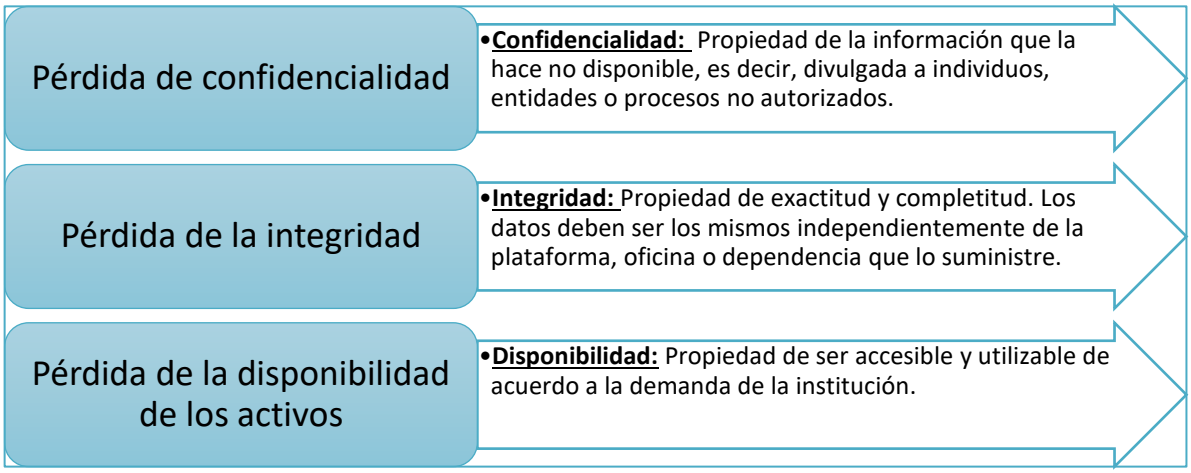


Ilustración 11. Identificación riesgos digitales

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Tabla 3. Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplo de vulnerabilidades	Ejemplo de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información en la institución.

8.2.3 Riesgos fiscales

Hace referencia al efecto de la incertidumbre sobre los objetivos de una organización relacionados con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.

Metodología para la identificación de riesgos fiscales
A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación del riesgo fiscal:

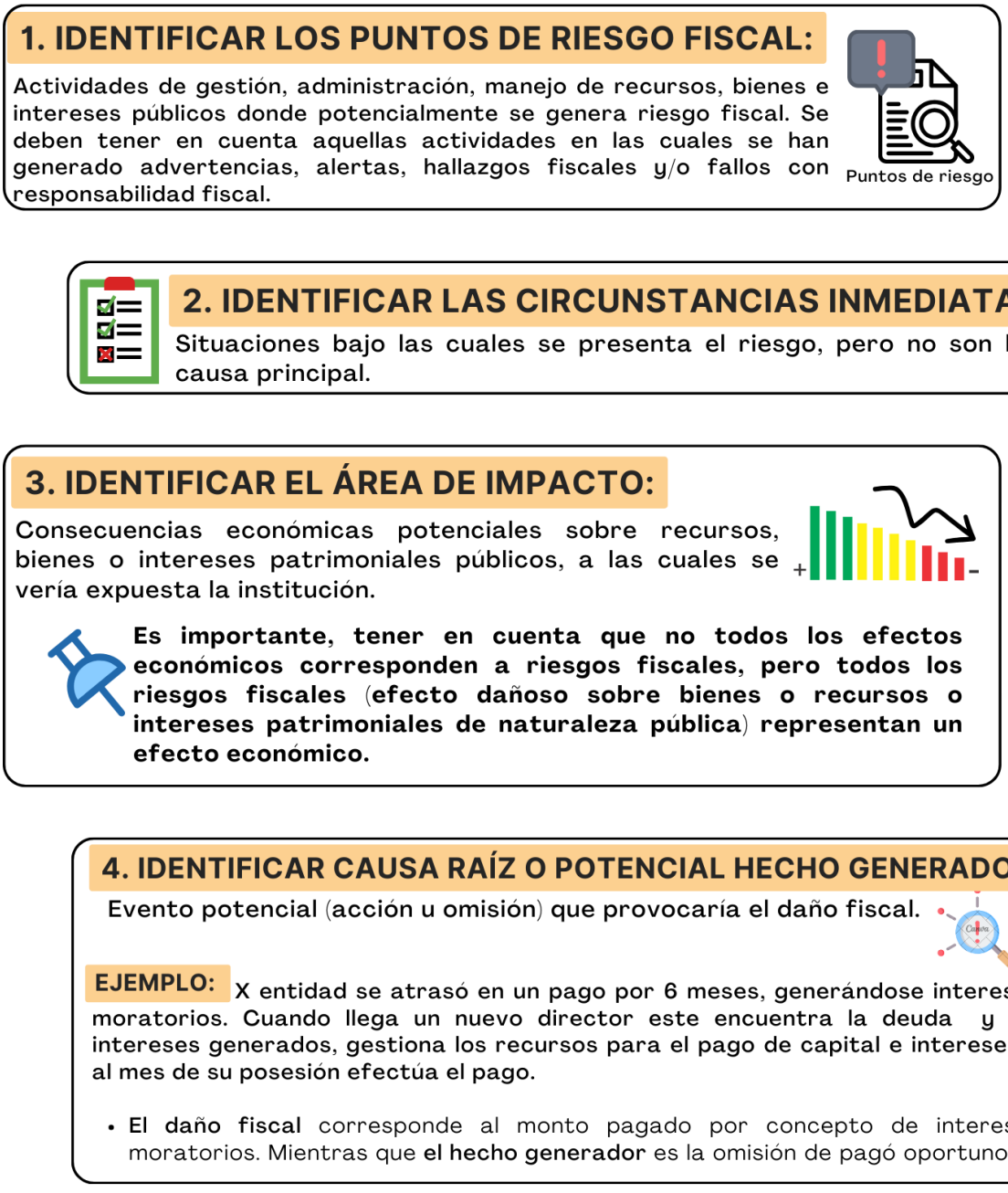


Ilustración 12. Metodología para la identificación de riesgos fiscales

Para la redacción del riesgo fiscal se sigue la estructura definida en el ítem ***8.2.1 Riesgos de gestión*** apartado "***Fases para la identificación de riesgos de gestión***" de la presente guía; teniendo en cuenta:

- **Iniciar con la oración:** Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
- **Impacto:** Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
- **Circunstancia inmediata:** Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- **Causa Raíz:** Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

EJEMPLO

Proceso: Contratación

Objetivo: Adquirir oportunamente los bienes, obras y servicios requeridos por la entidad para su operación.

Alcance: Desde la identificación de las necesidades hasta la liquidación de los contratos.

Riesgo Fiscal: Posibilidad de efectos dañosos sobre recursos públicos (área de impacto), por pago de mayores valores en la contratación de obras (circunstancia inmediata), a causa de la elaboración deficiente de los estudios previos y análisis del sector que soportan el valor estimado del contrato (causa raíz).

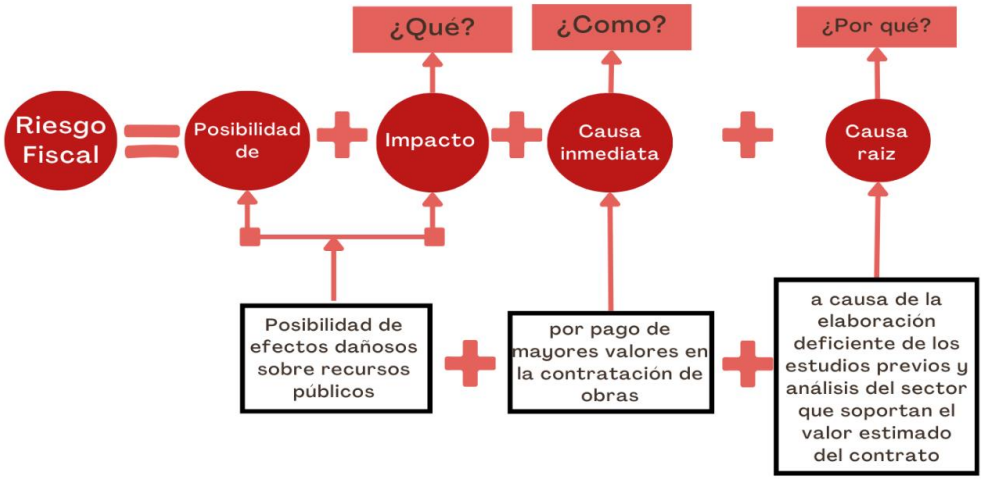


Ilustración 13. Ejemplo de riesgo fiscal

8.2.4 Riesgos de Corrupción

Se busca de manera general "identificar un conjunto sistemático de situaciones que, por sus características, pueden originar prácticas corruptas", asociándolas a cada uno de los procesos y procedimientos de la respectiva entidad[12].

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

Es necesario que en la descripción del riesgo concurran los componentes de su definición: **acción u omisión** + **uso del poder** + **desviación de la gestión de lo público** + **el beneficio particular**.

Con el fin de facilitar la identificación de riesgos de corrupción y de evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se utilizará la Matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición. Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción.

Los riesgos de corrupción se establecen sobre ***procesos***. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

8.3 VALORACIÓN DEL RIESGO

En esta etapa se busca establecer la calificación y evaluación del riesgo, a través de un análisis inicial de la posibilidad de ocurrencia de este y el impacto, que es considerado como riesgo inherente, y posteriormente una calificación final que es el resultado de la identifican y evaluación de controles, considerado riesgo residual.

Para la valoración del riesgo se aplicarán las siguientes fases.

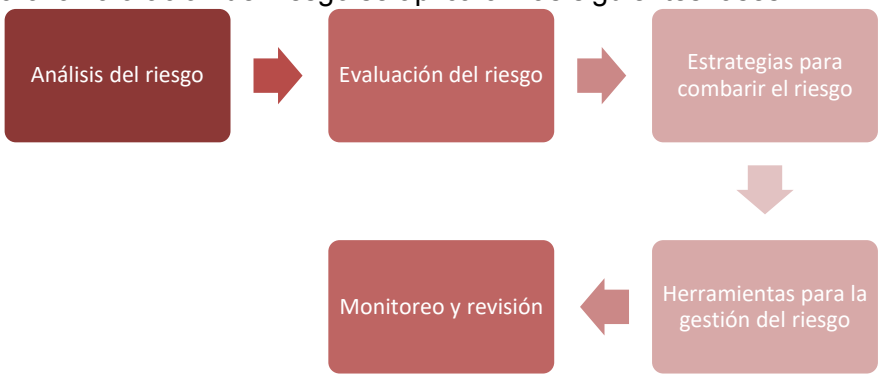


Ilustración 14. Fases para la valoración del riesgo

[12] Documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano"

- ***Valoración del Riesgo***

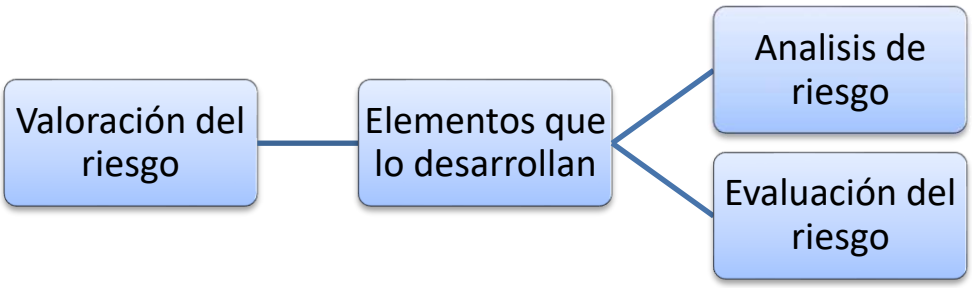


Ilustración 15. Estructura para el desarrollo de la valoración del riesgo

El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos, y busca establecer la Posibilidad de ocurrencia del mismo y su Impacto, con el fin de estimar la zona de riesgo inicial **RIESGO INHERENTE**; este aspecto puede orientar la clasificación del riesgo con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar[13].

Entendiéndose por *posibilidad de ocurrencia del Riesgo*, la oportunidad de que un incidente o evento suceda. Y como *Impacto*, el efecto o consecuencias que puede ocasionar a la Universidad la materialización del riesgo.

8.3.1 Análisis del riesgo

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

8.3.1.1 Riesgos de gestión y riesgos de seguridad de la información

La *Calificación del Riesgo:* deben calificar cada riesgo identificado, a través del análisis cualitativo y/o cuantitativo que le haga a la posibilidad de ocurrencia del riesgo y el impacto de éste.

- ***Determinar la probabilidad***

Entendiendo probabilidad como la posibilidad de ocurrencia del riesgo, para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Como referente, a continuación, se muestra una tabla donde se relaciona la probabilidad frente al riesgo de acuerdo a la frecuencia con la cual se realice la actividad

[13] Manual Operativo del Modelo Integrado de Planeación y Gestión – Dimensión 7

Tabla 4. Relación de la frecuencia con la probabilidad

Frecuencia de la actividad	Probabilidad frente al riesgo
1 vez al año	Muy baja
Semestral, Trimestral, Bimensual	Baja
Mensual	Media
Semanal	Alta
Diaria	Muy alta

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la Tabla 5 se establecen los criterios para definir el nivel de probabilidad.

Tabla 5. Criterios para definir el nivel de probabilidad

Descriptor-frecuencia	Frecuencia de la actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año máximo 5000 veces al año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Una vez establecida la frecuencia de la actividad se debe seleccionar el descriptor correspondiente a dicha frecuencia.

- **Determinar el impacto**

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

En la Tabla 6 se establecen los criterios para definir el nivel de impacto.

Tabla 6. Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la universidad

Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la universidad internamente, de conocimiento general nivel interno, de alta dirección y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la universidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la universidad con efecto publicitario sostenido a nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la universidad a nivel nacional, con efecto publicitario sostenido a nivel país.

NOTA: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.
Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles

8.3.1.2 Riesgos de corrupción

- La *Calificación del Riesgo:* busca determinar el grado en el cual se puede materializar un evento.

La ***Posibilidad*** hace referencia a la oportunidad de que algo suceda, medido o determinado de manera objetiva (basado en datos y hechos históricos) o subjetiva (bajo criterios de experiencia o experticia de quien analiza), utilizando términos generales o matemáticos (como la probabilidad numérica) o la frecuencia en un periodo de tiempo determinado[14].

Nivel-Descriptor	Descripción	Frecuencia
5 – Casi Certeza	**Se espera** que ocurra en la mayoría de las circunstancias	+ de 1 vez al año
4 – Probable	**Probablemente** ocurrirá en la mayoría de circunstancias	1 vez ultimo año
3 – Posible	**Podría** ocurrir en algún momento.	1 vez últimos 2 años
2 – Improbable	**Pudo** ocurrir en algún momento.	1 vez últimos 5 años
1 – Raro	**Puede** ocurrir solo en circunstancias Excepcionales.	No en la historia reciente

Ilustración 16. Matriz de calificación posibilidad riesgos de corrupción

*El **Impacto***, tratándose de riesgos de corrupción el impacto siempre será negativo; en este orden de ideas, no aplica la descripción de riesgos insignificante o menores.

[14] ICONTEC. Norma Técnica Colombiana NTC31000.

Nivel-Descriptor	Descripción (si el hecho se llegara a presentar)
5 – Catastrófico	Tendría **desastrosas** consecuencias o efectos sobre la Institución
4 – Mayor	Tendría **altas** consecuencias o efectos sobre la Institución
3 – Moderado	Tendría **medianas** consecuencias o efectos sobre la Institución

Ilustración 17. Matriz calificación impacto riesgos de corrupción

Para determinar el impacto se pueden utilizar los siguientes criterios descritos en la Ilustración 18**¡Error! No se encuentra el origen de la referencia.** que representan los temas en que suelen impactar la ocurrencia de los riesgos:

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) 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.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Nivel de impacto MAYOR

Ilustración 18. Criterios para calificar el impacto

Nota: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

Con el Elemento Análisis de Riesgos se espera que la Universidad obtenga los siguientes resultados:

- Establecer la posibilidad de ocurrencia de los riesgos inherentes, que pueden disminuir la capacidad de la Universidad, para cumplir su propósito.
- Medir el impacto, las consecuencias del riesgo inherente sobre las personas, los recursos, los objetivos institucionales o el desarrollo de los procesos.
- Establecer criterios de calificación y evaluación de los riesgos inherentes que permiten tomar decisiones pertinentes sobre su tratamiento.

8.3.2 Evaluación del Riesgo

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Riesgos antes y después de controles[15]

Es importante considerar que los controles estén bien definidos, para asegurar que efectivamente mitigan las causas que hacen que el riesgo se materialice.

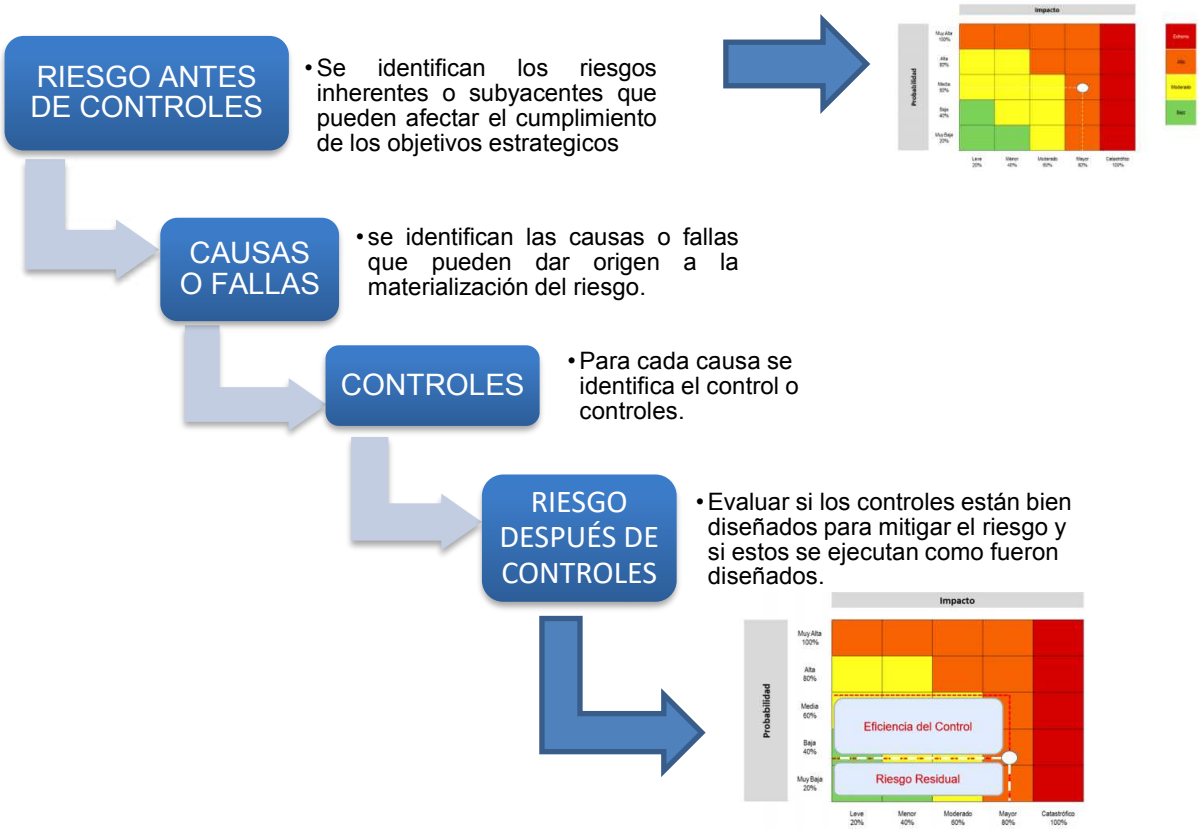


Ilustración 19. Riesgos antes y después de controles

[15] Guía para la administración del riesgo y el diseño de controles en entidades públicas

Para tener en cuenta al momento de crear un control:

- Para cada causa debe existir un control
- Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón)
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica
- Para los riesgos de gestión la causa raíz es la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

8.3.2.1 Riesgos de gestión y riesgos de seguridad de la información

Análisis preliminar (riesgo inherente):

Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la Universidad al riesgo, ubicándolo en una zona de severidad, Bajo, Moderado, Alto o Extremo y fijar las prioridades de las acciones requeridas para su tratamiento.

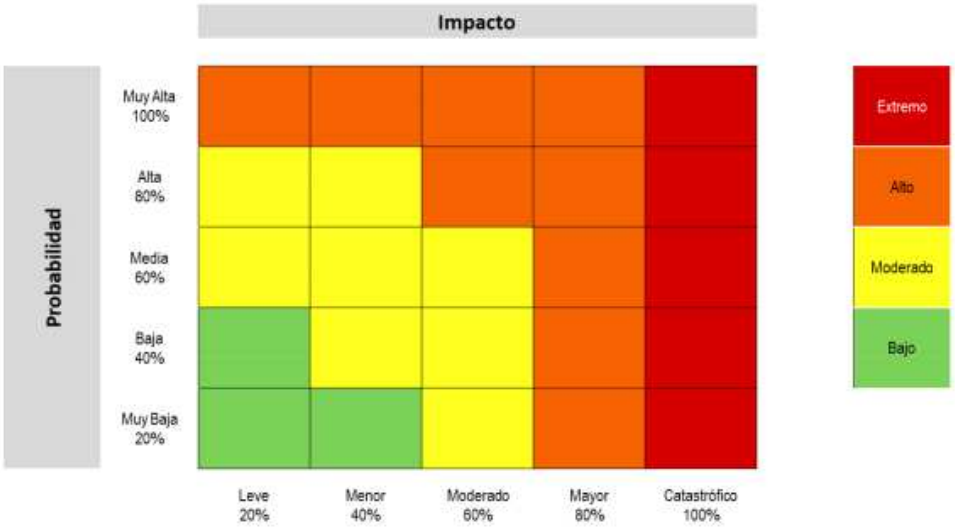


Ilustración 20. Matriz de calor (niveles de severidad del riesgo)

***Valoración de controles*:**

Definiendo control como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control:

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. En la Ilustración 21 se consideran 3 fases globales del ciclo de un proceso.

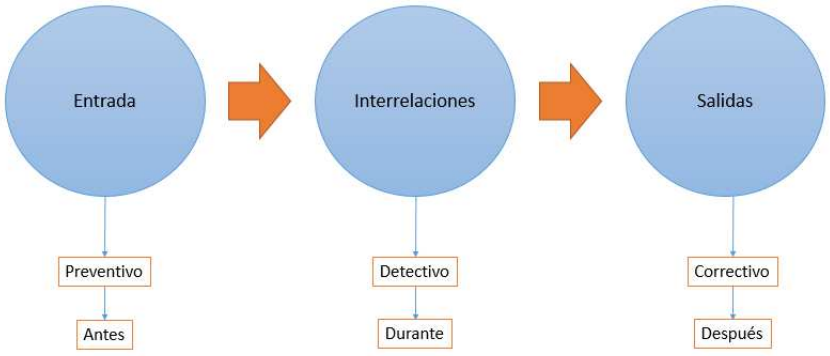


Ilustración 21. Ciclo del proceso y tipología de controles

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

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.

Análisis y evaluación de los controles – Atributos:

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la Tabla 7 se puede observar la descripción y peso asociados a cada uno así:

Tabla 7. Atributos de para el diseño del control

Característica			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad. Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

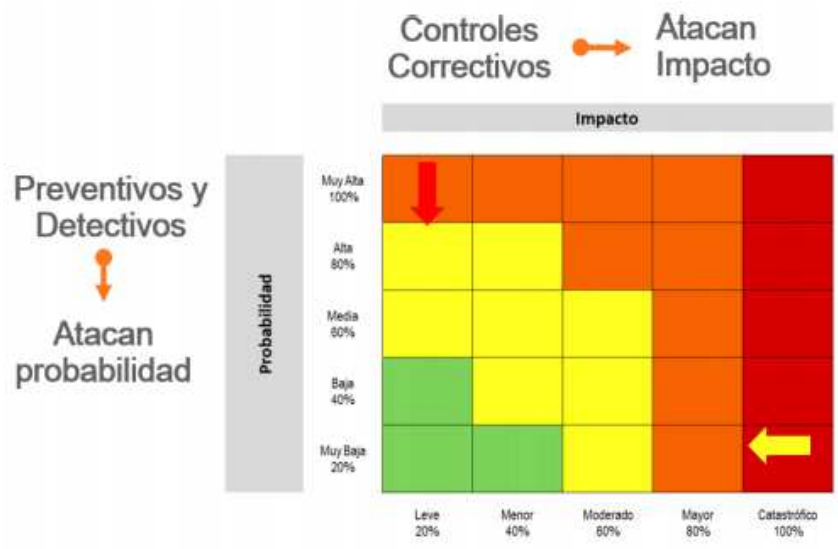


Ilustración 22. Movimiento en la matriz de calor acorde con el tipo de control

Nivel de riesgo (riesgo residual):

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Para mayor claridad, a continuación, se describe la formula y se observan los cálculos requeridos para la aplicación de los controles de acuerdo a los datos descritos.

$$Riesgo\ Residual = R.Inherente - (R.I * control)$$

R. Inherente tiene dos valores uno de probabilidad y otro de impacto, se utiliza de acuerdo a la tipología del control

Ejemplo:
Datos
Probabilidad inherente= 60%
Impacto= 80%
Valoración control 1= preventivo 40%
Valoración control 2= detectivo 30%

Tabla 8. Aplicación de controles para establecer riesgo residual

Riesgo	Datos relacionados con la probabilidad de impacto inherente		Datos valoración de controles		Calculo
Posibilidad de pérdida económica por	Probabilidad inherente	60%	Valoración del control 1 preventivo	40%	60%-(60%*40%)= 36%

multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos	Valor de la probabilidad para aplicar el segundo control	36%	Valoración del control 2 detectivo	30%	36%-(36%*30%)=25.2%
	Probabilidad residual	25.2%			
	No se tienen controles para aplicar al impacto	NA	NA	NA	NA
	Impacto residual	80%			

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.Ilustración 23 se observa el movimiento en la matriz de calor.

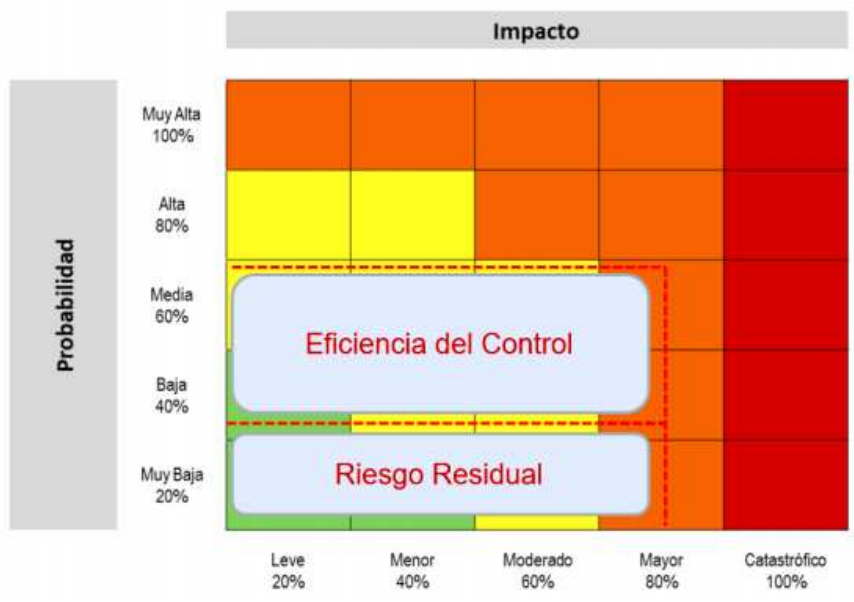


Ilustración 23. Movimiento en la matriz de calor con el ejemplo propuesto

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

8.3.2.2 Riesgos de corrupción

La Evaluación del Riesgo permite establecer el grado de exposición de la Universidad al riesgo, ubicándolo en una zona de riesgo, de acuerdo a la probabilidad e impacto determinado.

Matriz de Calificación, Evaluación y Respuesta a los Riesgos

		Impacto		
		3 Moderado	4 Mayor	5 Catastrófico
Posibilidad	1 – Raro	Z.R Baja	Z.R. Moderada	Z.R Alta
	2 – Improbable	Z.R. Moderada	Z.R. Moderada	Z.R Alta
	3 – Posible	Z.R Alta	Z.R Alta	Z.R. Extrema
	4 – Probable	Z.R Alta	Z.R. Extrema	Z.R. Extrema
	5 – Casi Certeza	Z.R. Extrema	Z.R. Extrema	Z.R. Extrema

Z.R.: Zona de Riesgo

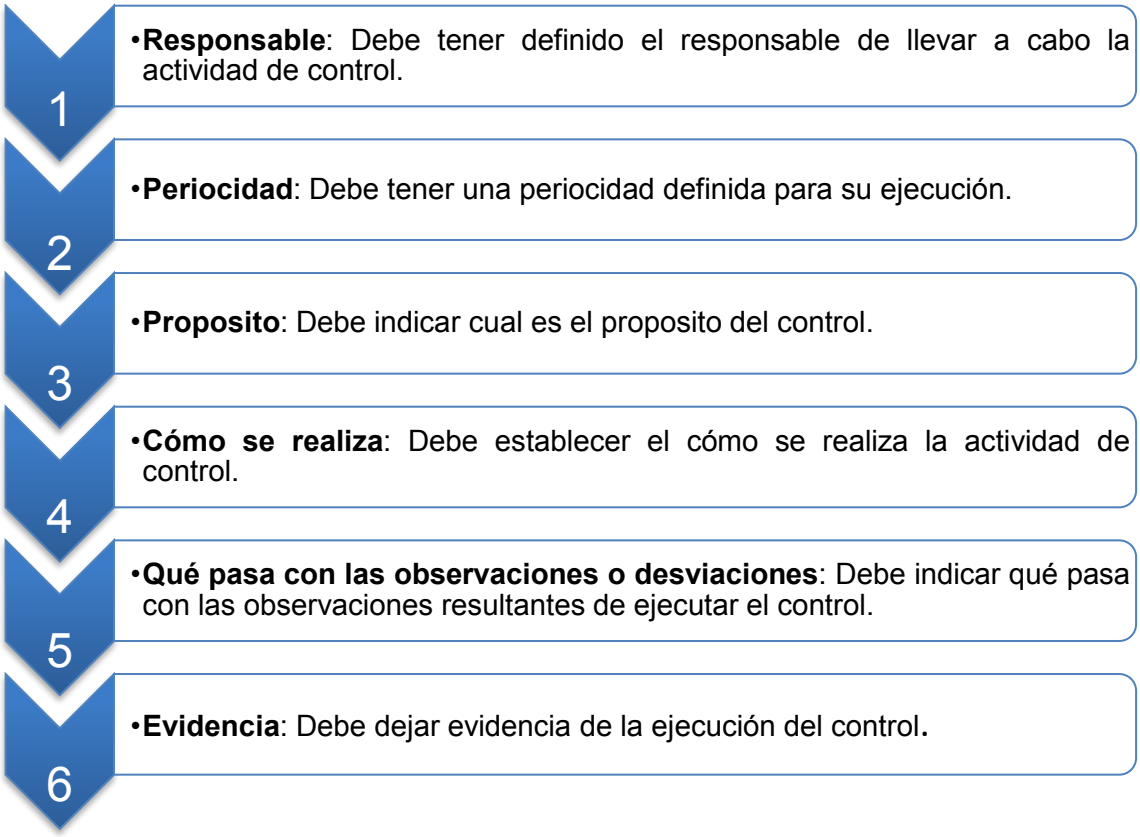
Ilustración 24. Matriz de Calificación, Evaluación y Respuesta a los Riesgos de corrupción

En la evaluación se busca confrontar los resultados del análisis del riesgo inicial **RIESGO INHERENTE**, frente a los controles establecidos, con el fin de determinar la zona de riesgo final **RIESGO RESIDUAL**. Para ello se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones[16].

***Valoración de los controles - Diseño de controles*[17]**

Para asegurar la mitigación adecuada del riesgo, se deben considerar las siguientes variables a la hora de definir el control.

[16] Manual Operativo del Modelo Integrado de Planeación y Gestión – Dimensión 7
[17] Guía para la administración del riesgo y el diseño de controles en entidades públicas V4



Valoración de los controles[18]

La valoración de los controles para la mitigación de los riesgos, se fundamenta en dos premisas:

- ***El control está bien diseñado para mitigar el riesgo***
- ***El control se ejecuta como fue diseñado y de manera consistente***

Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

El análisis y evaluación de los controles para la mitigación de los riesgos, se realiza de acuerdo con las seis (6) variables establecidas:

[18] Guía para la administración del riesgo y el diseño de controles en entidades públicas V4.

Tabla 9. Análisis y evaluación de los controles para la mitigación de los riesgos

Criterio de evaluación	Aspecto a evaluar en el diseño del control	Opciones de respuestas	Peso en la evaluación del diseño del control
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del Control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permite mitigar el riesgo?	Confiable	15
		No confiable	10
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y se resuelven oportunamente	15
		No se investigan y se resuelven oportunamente	0
6. Evidencia de la ejecución del control.	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0

Resultado de la evaluación del diseño del control

Para que un control se evalué como bien diseñado, se deben cumplir todas las variables de la Tabla 10 y se determinada en tres rangos de acuerdo a la calificación que se obtenga de sumar los puntos asignados a cada variable:

Tabla 10. Criterios de evaluación del diseño del control

Rango de calificación del diseño	Resultado – Peso en la evaluación del Diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Resultado de la evaluación de la ejecución del control

Se evalúa la ejecución del control, dado que no basta solo con que el control este bien diseñado, si no que se debe ejecutar de manera consistente, con el fin de que el riesgo se pueda mitigar. Para evaluarlo se lleva a cabo una actividad de confirmación y se califica de acuerdo a la siguiente Tabla 11***¡Error! No se encuentra el origen de la referencia.***:

Tabla 11. Criterios de evaluación ejecución del control

Rango de calificación del diseño	Resultado – Peso en la evaluación del Diseño del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable
Moderado	El control se ejecuta algunas veces por parte del responsable
Débil	El control no se ejecuta por parte del responsable

Análisis y evaluación de los controles para la mitigación de los riesgos

La calificación de riesgos inherentes y residuales se realiza al riesgo y no a cada causa, por lo que hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto si ayudan al tratamiento de los riesgos, considerando el diseño, ejecución individual y promedio de los controles.

La calificación de la solidez de cada control, asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

Tabla 12. Análisis y Evaluación de los controles para la mitigación de los riesgos

Peso individual del diseño	"El control se ejecuta de manera consistente por los responsables (Ejecución)"	Evaluación Individual de Cada Control Fuerte: 100 Moderado: 50 Débil: 0	Peso en la evaluación del diseño del control SI/NO
fuerte calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Evaluación del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

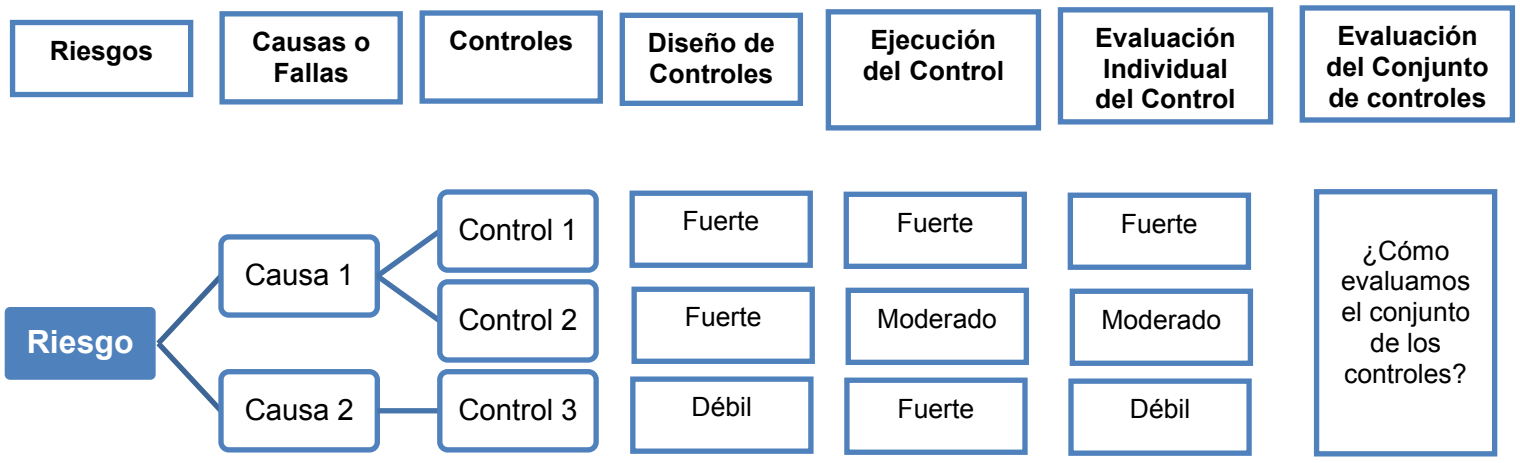


Ilustración 25. Evaluación del conjunto de controles para la adecuada mitigación del riesgo

Tabla 13. Criterios de evaluación del conjunto de controles

Rango de calificación del diseño	Resultado – Peso en la evaluación del Diseño del control
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

La evaluación del conjunto de controles, se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

Disminución de Probabilidad

Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento

El desplazamiento de un riesgo inherente en su probabilidad para el cálculo del riesgo residual, se realizará de acuerdo con la siguiente tabla:

Tabla 14. Disminución de probabilidad

Evaluación del conjunto de los controles	Controles Ayudan a disminuir la probabilidad	# Columnas en la matriz de riesgo que de desplaza en el eje de la probabilidad
fuerte	directamente	2
fuerte	directamente	2
fuerte	directamente	2
fuerte	no disminuye	0
moderado	directamente	1
moderado	directamente	1
moderado	directamente	1
moderado	no disminuye	0
fuerte	directamente	2

Luego de determinar la eficiencia de los controles se debe escoger la zona de riesgo (riesgo residual)

Matriz de Calificación, Evaluación y Respuesta a los Riesgos

		Impacto		
		3 Moderado	4 Mayor	5 Catastrófico
Posibilidad	1 – Raro	Z.R Baja	Z.R. Moderada	Z.R Alta
	2 – Improbable	Z.R. Moderada	Z.R. Moderada	Z.R Alta
	3 – Posible	Z.R Alta	Z.R Alta	Z.R. Extrema
	4 – Probable	Z.R Alta	Z.R. Extrema	Z.R. Extrema
	5 – Casi Certeza	Z.R. Extrema	Z.R. Extrema	Z.R. Extrema

Z.R.: Zona de Riesgo

Ilustración 26. Matriz de Calificación, Evaluación y Respuesta a los Riesgos de corrupción

 Si la evaluación del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

Con este elemento se busca que la Universidad obtenga los siguientes resultados:

- Identificar los controles existentes para los riesgos identificados y analizados.
- Priorizar los riesgos residuales de acuerdo con los resultados obtenidos de confrontar la evaluación del riesgo con los controles existentes.
- Elaborar el mapa de riesgo por proceso, teniendo en cuanta los criterios dados en el elemento Políticas de Administración del Riesgo.

8.3.3 Estrategias para combatir el riesgo

Para todos los tipos de riesgos, las acciones quedan enmarcadas dentro de unas opciones de respuesta, las cuales son recomendaciones de orientación estratégica del plan de acción a seguir, en el control efectivo del riesgo dentro del proceso. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo

Estas posibles acciones a tomar según Calificación del Riesgo son:

- **Reducir el Riesgo:** medidas orientadas a disminuir tanto la posibilidad (medidas de prevención), como el impacto (medidas de protección o correctivas), mediante la optimización de procedimientos y la implementación de controles.
  Luego de realizar el análisis y considerar que el nivel de riesgo es alto se determina tratarlo mediante transferencia o mitigación del mismo
  - **Transferir**: después de realizar un análisis se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de contratos de seguros. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. También es posible transferir el riego a otro u otros procesos dentro de la misma institución.
  - **Mitigar**: después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo, no necesariamente es un control adicional.

- **Aceptar el Riesgo:** después de realizar un análisis y considerar los niveles de riesgos se determina aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen, conociendo los efectos de su posible materialización.

- **Evitar la Posibilidad:** después de realizar un análisis y considerar que el nivel del riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, iii) evidencia o registro e iv) indicador.

En caso de **riesgo residual**, dado por reducción del riesgo, el responsable del proceso o representante legal puede aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.

Para escoger la opción de manejo que va a tratar el riesgo, también tiene que tener en cuenta que:

- *Riesgo* en Zonas Moderadas o Altas, se debe realizar un análisis del costo beneficio, costo de la implementación de la acción contra el beneficio de la misma.

- Siempre que el riesgo sea calificado con Zona de Riesgo Extrema e Impacto Alto se debe eliminar la actividad que genera el riesgo en la medida que sea posible y se deben diseñar planes de contingencia, para protegerse en caso de su ocurrencia.

- **ACCIONES.** Es la aplicación concreta de la opción de manejo establecida. Y la puede basar en las acciones sugeridas o recomendadas en el formato.

Algunas de las acciones tienden a reducir o controlar la *Posibilidad (Causas)* y otras el *impacto (Consecuencias)*[19].

Las acciones que decida implementar deben:

- Ser Factibles y Efectivas, tales como: definición de estándares, optimización de procesos y procedimientos y cambios físicos, entre otros.

- Tener Viabilidad Jurídica: Velar por que los controles que se van a implantar no vayan en contra de la normatividad vigente.

- Tener Viabilidad Técnica e Institucional: Establecer claramente si la Universidad está en capacidad de implantar y sostener a largo plazo nuevas tecnologías u otros mecanismos necesarios para ejecutar el control.

- Poseer un Análisis Costo-Beneficio: Prácticamente todas las respuestas a los riesgos implican algún tipo de costo directo o indirecto que se debe sopesar en relación con el beneficio que genera. Se ha de considerar el costo inicial del diseño e implementación de una respuesta (procesos, personal, tecnología), así como el costo de mantener la respuesta de forma continua[20]. Este caso se puede dar específicamente para aquellos controles nuevos que requieren contrataciones adicionales a los funcionarios que desarrollan los proceso o bien cuando se requiere

[19]Algunas Acciones fueron tomadas del AS/NZS 4360:1999 Estándar Australiano Administración de Riesgos

[20] PRICE WATERHOUSE COOPERS. Administración de Riesgos Corporativos. Técnicas de Aplicación. Colombia. 2005. p. 64

diseñar e implementar sistemas de información o tecnologías específicas para ejecutar el control.

- **INDICADOR DE AVANCE**. El estado de ejecución en que se encuentra la acción: Sin Implementar, En ejecución o No Aplica. El No Aplica se refiere a si en los riesgos de Gestión decidió aceptar el Riesgo, y en los riesgos de Corrupción si decidió No Establecer nuevas acciones.

8.3.4 Herramientas para la gestión del riesgo

8.3.4.1 Consolidación del Mapa de Riesgo

Es una representación final de todo el análisis realizado al Proceso o a la Institución, y contiene a nivel estratégico los mayores riesgos a los cuales se está expuesto, permitiendo conocer las políticas inmediatas de respuesta ante ellos, la aplicación de acciones y sus indicadores[21].

- ***Un Mapa Por cada proceso***. Para facilitar la administración del riesgo.
- ***Un Mapa Institucional.*** El cual se construirá teniendo en cuenta algunos o todos los riesgos identificados por los procesos, dependiendo si son riesgos de gestión o de corrupción.

  Riesgos de GESTIÓN. Se constituirá con los riesgos de gestión cuya Evaluación Final se encuentre en ALTA y EXTREMA de los mapas de riesgos de los procesos estratégicos, misionales y de evaluación, y de aquellos procesos de apoyo sean considerados de importancia Extrema. Dentro de este, se establecerán los riesgos de seguridad digital y fiscales.

  Riesgos de CORRUPCIÓN. Se constituirá con todos los riesgos de corrupción de los mapas de riesgos de los procesos estratégicos, misionales y de evaluación, y de aquellos procesos de apoyo sean considerados de importancia Extrema.

OPCIONES DE MANEJO. Hay que tener en cuenta las opciones de manejo sugeridas, la cual se basa en la *Matriz de Calificación, Evaluación y Respuesta a los Riesgos.* En esta se establece el grado de exposición del proceso al riesgo, según sea Bajo, Moderado, Alto o Extremo**.**

[21] Manual Operativo del Modelo Integrado de Planeación y Gestión – Dimensión 7

8.3.4.1.1 Riesgo de gestión, seguridad de la información y fiscales

Tabla 15. Opciones de manejo riesgos de gestión y seguridad de la información

Probabilidad	Impacto 1	2	3	4	5
5	Z.R Alta Reducir, evitar	Z.R Alta Reducir, evitar	Z.R Alta Reducir, evitar	Z.R Alta Reducir, evitar	Z.R Extrema Reducir, evitar
4	Z.R Moderada Reducir	Z.R Moderada Reducir	Z.R Alta Reducir, evitar	Z.R Alta Reducir, evitar	Z.R Extrema Reducir, evitar
3	Z.R Moderada Reducir	Z.R Moderada Reducir	Z.R Moderada Reducir	Z.R Alta Reducir, evitar	Z.R Extrema Reducir, evitar
2	Z.R Baja Aceptar, reducir	Z.R Moderada Reducir	Z.R Moderada Reducir	Z.R Alta Reducir, evitar	Z.R Extrema Reducir, evitar
1	Z.R Baja Aceptar	Z.R Baja Aceptar, reducir	Z.R Moderada Reducir	Z.R Alta Reducir, evitar	Z.R Extrema Reducir, evitar

8.3.4.1.2 Riesgo de corrupción

Tabla 16. Opciones de manejo riesgos de corrupción

Matriz de Calificación, Evaluación y Respuesta a los Riesgos

	3	4	5
1	**Z.R Baja** Evitar, Reducir	**Z.R. Moderada** Eliminar, Reducir	**Z.R Alta** Eliminar, Reducir, Compartir
2	**Z.R. Moderada** Eliminar, Evitar, Reducir	**Z.R. Moderada** Eliminar, Evitar, Reducir	**Z.R Alta** Eliminar, Evitar, Reducir, Compartir
3	**Z.R Alta** Eliminar, Evitar, Reducir, Compartir	**Z.R Alta** Eliminar, Evitar, Reducir, Compartir	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir
4	**Z.R Alta** Eliminar, Evitar, Reducir, Compartir	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir
5	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir	**Z.R. Extrema** Eliminar, Evitar, Reducir, Compartir

8.3.5 Monitoreo y revisión

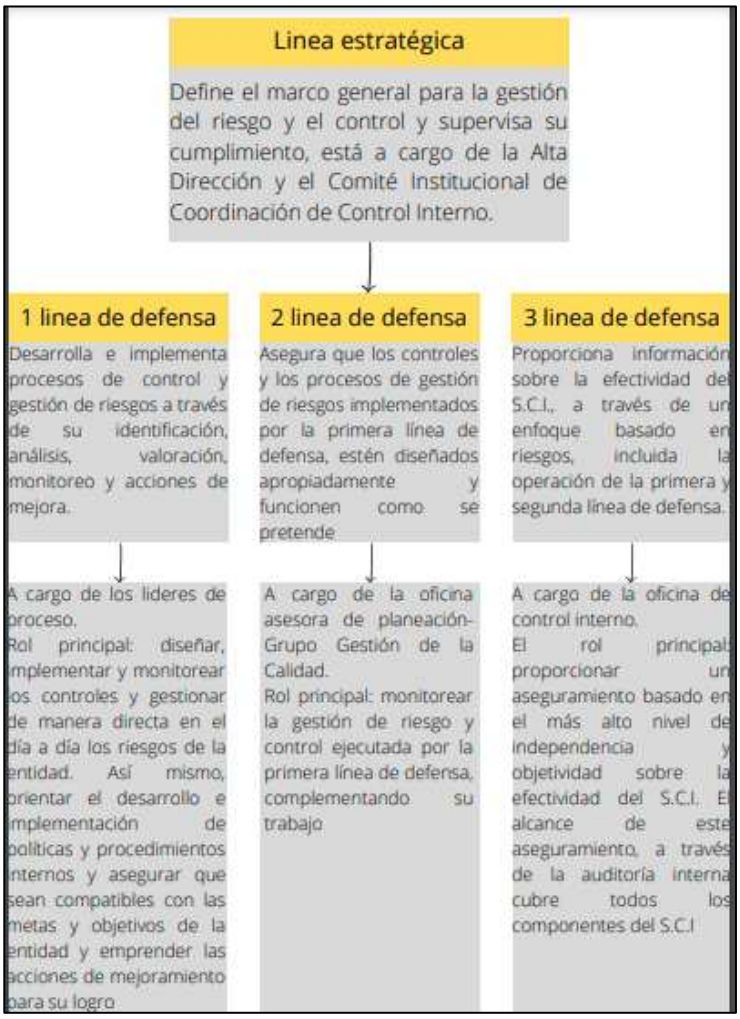


Ilustración 27. Esquema de línea de defensa

El Monitoreo y revisión debe asegurar que las acciones establecidas en los mapas se están llevando a cabo y evaluar la eficiencia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones[22].

Para el ejercicio de la Revisión y Monitoreo es necesario establecer un plan de trabajo o cronograma, al que se le realizaran los monitoreos (Auto monitoreo y Monitoreo de gestión).

- **CRONOGRAMA**. El líder del proceso debe establecer un cronograma de ejecución de las acciones contenidas en la consolidación y cuyo indicador se encuentre SIN IMPLEMENTAR o EN EJECUCIÓN.

[22] Guía para la administración del riesgo y el diseño de controles en entidades públicas V4

Para el desarrollo de las acciones se debe conocer la siguiente información:

- **Producto o Entregable:** Cualquier producto, resultado, o capacidad de prestar un servicio único y verificable que debe producirse para cumplir con la Acción definida. Ejemplo: Resolución (es), Comunicación (es), Sistema de Información, modulo (s), etc.
- **Seguimiento:** Se debe indicar al momento de realizar el seguimiento a las acciones, el avance de las mismas, esto se realiza dando clic en el icono Adicionar seguimiento, aquí se coloca los resultados obtenidos con los indicadores. Una vez terminado los periodos de seguimiento se debe verificar la eficacia. Hay que tener en cuenta que la acción no se puede cerrar en el sistema hasta que se compruebe que el control es eficaz, esta determinación la realiza el Administrador de Riesgos.
- **Fecha de Inicio y de terminación:** Las colocará automáticamente la plataforma cada vez que se realice el seguimiento y se determine la eficacia del sistema.

- **AUTO MONITOREO.** Los Líderes de procesos son los responsables de velar por que las acciones establecidas en el mapa de riesgos de su proceso, se cumplan en los tiempos y términos establecidos en el Cronograma, y deben establecer los avances de las acciones **Cuatrimestralmente**.

- **MONITOREO DE GESTIÓN.** La Oficina de Control Interno mediante el proceso Evaluación Independiente, debe verificar que se cumpla lo consignado en el cronograma de administración de los riesgos, establecido por los líderes de procesos y verificar el estado de avance informado cuatrimestralmente. Es por ello que este monitoreo de gestión se debe realizar en los mismos periodos del auto monitoreo. Este monitoreo se puede realizar en el marco de las auditorias de control interno, seguimientos a planes de mejoramiento, plan anticorrupción, u otras actividades desarrolladas por la oficina. Para aquellas actividades que no cumplieron con el cronograma establecido se dejara constancia en el campo de Observación del formato, del incumplimiento y de la medida que la Oficina recomienda tomar para su cumplimiento

- **INFORME DE RESULTADOS.** La Oficina de Control Interno dentro de su función asesora debe comunicar y presentar luego del seguimiento y evaluación (Monitoreo de Gestión) sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas[23].

[23] Guía para la administración del riesgo y el diseño de controles en entidades públicas V4

9 REGISTRO DE MODIFICACIONES

Versión	Fecha	Ítem modificado	Descripción
01	30/04/2009	Código del proceso	Cambia la codificación DE-G01 del proceso de Direccionamiento Estratégico a EI-G03 del proceso de Evaluación Independiente.
		Roles y Responsabilidades	Se quita la responsabilidad al jefe de la oficina asesora de planeación.
02	07/05/2010	4.4 Metodología	Se actualizó tenieno en cuenta los últimos lineamientos dados por el DAFP a través de su Guia de Administración del Riesgo de Noviembre de 2009.
03	06/05/2011	1. Objetivo General 2. Alcance	Se hizó referencia a la Guia del DAFP edición 4 del año 2011 Se le establecio la numeración 1.1 para los objetivos especificos. Se hicieron correcciones de redaccion.
		3 Generalidades	Se incluyo el item de Responsables, el cual se convirtio en el numeral 3. Cambio a Numeral 4. El titulo normas de referencia fue reemplazado por:Normas de referencia nacional y normas de referencia universidad del magdalena En normas de referencia nacional se incluyendo las de Guia del DAFP edición 4, la armonización entre el MECI y la NTCGP1000:2009 y lo establecido en la NTC ISO 31000 Se realizaron correcciones de redaccion en glosario de terminos.
		4 Descripcion	Cambio a Numeral 5
		4.1 Introducción	Cambio a Numeral 5.1 Se hizo un recuento de las transformaciones que se han generado en esta materia desde su implementacion hasta la fecha. Se hizo referencia a la Guia del DAFP edición 4, la armonización entre el MECI y la NTCGP1000:2009 y NTC ISO 31000
		4.2 Marco Conceptual	Cambio a Numeral 5.2 Se introdujo un enfoque y graficas de la NTC ISO 31000
		4.3 Roles y Responsabilidades	Se introdujo la responsabilidad de la alta y media direccion y se especifico las responsabilidades en personas
		4.4 Metodologia	Cambio a Numeral 5.4 Se actualizó teniendo en cuenta los lineamientos dados por el DAFP a través de la 4 edición de su guía publicada el 13 de febrero de 2012, la armonización entre el MECI y la NTCGP1000:2009 y lo establecido en la NTC ISO 31000 Gestión del Riesgo – Principios Directrices, emitido por el ICONTEC Se introdujeron ejemplos gráficos y de texto, así como se incluyeron los formatos a los que hace referencia el documento Se le estableció una numeración para cada aspecto y elemento de la administración del riesgo, la cual va del 5.4.1 al 5.4.8.
		5 Registro de Modificaciones	Cambio a Numeral 6
		Anexo: Formato Mapa de Riesgo	Se eliminaron los Anexos
04	10/08/2012	1. Objetivo General 1.1. Objetivos Especificos 2. Alcance	Se hizo referencia a los nuevos lineamientos establecidos por el DAFP en 2014. Se redefinieron los objetivos de la guía Se actualizo el alcance teniendo en cuenta la nueva estructura MECI 2014 y Riesgos de Corrupción dados por el Documento “Estrategias para la construcción del plan anticorrupción y atención al ciudadano”
		4 Generalidades	Se hizo referencia a los documentos MECI 2014, NTC ISO 31000, Guía del DAFP V3 – 2014 y Documento “Estrategias para la construcción del plan anticorrupción y atención al ciudadano”. En normas de referencia nacional se incluyeron MECI 2014 y la de Guía del DAFP V3-2014, la Ley Anticorrupción

Versión	Fecha	Ítem modificado	Descripción
		5.1 Introducción	Se hizo un recuento de las transformaciones que se han generado en esta materia desde su implementación hasta la fecha. A los documentos MECI 2014, NTC ISO 31000, Guía del DAFP V3 – 2014 y Documento "Estrategias para la construcción del plan anticorrupción y atención al ciudadano"
		5.2 Marco Conceptual	Se introdujo un enfoque de MECI 2014, NTC ISO 31000, Guía del DAFP V3 – 2014, Documento "Estrategias para la construcción del plan anticorrupción y atención al ciudadano" y graficas del MECI 2014
		5.3 Roles y Responsabilidades	Cambio a ítem del numeral 3.3.1.1 dentro de política de administración del riesgo. Se introdujeron responsabilidades teniendo en cuenta los cambios dados por MECI 2014, Guía del DAFP V3 – 2014 y Documento "Estrategias para la construcción del plan anticorrupción y atención al ciudadano"
		5.4 Metodologia	Cambio a numeral 5.3. Se actualizó teniendo en cuenta los nuevos lineamientos dados por el DAFP en MECI 2014, Guía del DAFP V3 – 2014 y Documento "Estrategias para la construcción del plan anticorrupción y atención al ciudadano", sin dejar a un lado la armonización entre el MECI y la NTCGP1000:2009 y lo establecido en la NTC ISO 31000 Gestión del Riesgo – Principios Directrices, emitido por el ICONTEC Se introdujeron ejemplos gráficos y de texto, así como se incluyeron los formatos a los que hace referencia el documento Se le estableció una numeración para cada aspecto y elemento de la administración del riesgo teniendo en cuenta la estructura MECI 2014, de la siguiente forma: 5.3.1. Política de administración del riesgo 5.3.2. Identificación del riesgo 5.3.3. Análisis y valoración del riesgo
05	14/072015	2. Alcance	Se Estableció que provee la guía y quienes deben aplicarla
		4. Generalidades	Se hizo referencia a la guía para la gestión de riesgos de corrupción. La cual también fue incluida dentro de las normas de referencia nacional, además se hace referencia a la ISO 9001:2015 en su numeral 6.1. En glosario de términos se incluyó la definición de riesgo inherente
		5.1 Introducción	Se hizo un recuento de las transformaciones que se han generado en esta materia desde su implementación hasta la fecha
		5.2 Marco Conceptual	Se actualizó el enfoque dado por la Guía de Administración de Riesgos y se incluyó el enfoque de la Guía para la Gestión de Riesgos de Corrupción.
		5.3 Metodologia	Se actualizó teniendo en cuenta los nuevos lineamientos dados por el DAFP y la Secretaria de Transparencia, en MECI 2014, Guía de Administración del Riesgo V3, Documento "Estrategias para la construcción del plan anticorrupción y atención al ciudadano" Versión 2, Guía para la Gestión de Riesgos de Corrupción, sin dejar a un lado la armonización entre el MECI y la NTCGP1000:2009 y lo establecido en la NTC ISO 31000 Gestión del Riesgo – Principios Directrices, emitido por el ICONTEC
		7. Anexos	Se incluyó el numeral 7 de anexos
06	08/11/2016	Encabezado	Se elimina "UNIVERSIDAD DEL MAGDALENA" y se agrega el nombre del proceso al cual pertenece el documento. Este documento pasa al proceso de Evaluación de la Gestión y Rendición de cuentas.
		Pie de pagina	Se ajustan los responsables de elaboró y aprobó según la delegación del rector.
		Código del proceso	Cambia la codificación EI-G03 del proceso de Evaluación Independiente a EG-G-003 del proceso de Evaluación de la Gestión y Rendición de cuentas.

Versión	Fecha	Ítem modificado	Descripción
		3. Responsable	Se quita la responsabilidad al jefe de la oficina de Control Interno.
		5.3 Metodología	Se ajusta el contenido de la metodología teniente a responsabilidades y herramientas utilizadas, dado que la creación y/o actualización de los mapas de riesgos será a través de ISOlución. Se elimina el ítem de anexos.
		7. Anexos	Se elimina.
07	10/11/2017	2. Alcance	Se amplía a los riesgos digitales
		3. Responsable	Se ajusta la responsabilidad de la Oficina de Control Interno
		4. Generalidades	En el glosario de términos, se incluyen otros términos relacionados con los riesgos digitales.
		5. Descripción	Se ajusta el contenido de la introducción.
		5.3 Metodología	Se ajusta el contenido de la metodología incorporando todo lo relacionado a los riesgos de seguridad digital.
08	04/02/2019	Código del proceso	Cambia la codificación EG-G-003 del proceso de Evaluación de la Gestión y Rendición de cuentas a DP-G-002 del proceso Dirección y Planeación.
		1. Objetivo	Se elimina la clasificación de los riesgos
		2. Alcance	Se elimina la clasificación de los riesgos
		4. Generalidades	Se ajusta el ítem de normativa, incluyendo nueva normativa y eliminando algunas obsoletas. Se incluyó nuevos términos en el Glosario
		5. Descripción	Se ajusta el ítem de Introducción, marco conceptual, comunicación y consulta, en el ítem de desarrollo, identificación y valoración del riesgo.
09	19/06/2020	4. Generalidades	Se ajusta el ítem de normativa, adicionando la nueva versión de la guía de administración de riesgo. Se incluyó nuevos términos en el Glosario y se actualizaron otros.
		5.2 Marco conceptual	Se actualiza la estructura de la ISO 31000 a su actual versión 2018
		5.3 Metodología	Se ajustó toda la metodología teniendo en cuenta la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 para los riesgos de gestión y seguridad de la información y la versión 4 de la guía mencionada para los riesgos de corrupción.
10	25/01/2022	1.Objetivo	Se ajusta la redacción del objetivo general y se incluye un especifico
		4.3. Glosario de términos	Se incluye la descripción del término “Riesgo Fiscal”, teniendo en cuenta la actualización de la guía dispuesta por el DAFP.
		7.4. Riesgos Fiscales	Se incluye lo relacionado a los riesgos fiscales teniendo en cuenta la actualización de la guía dispuesta por el DAFP.
		8.2.1 Riesgos de gestión	Se ajusta la descripción y se detallan las “Fases para la identificación de riesgos de gestión” haciendo uso de infografía.
		8.2.2 Riesgos de seguridad de la información	Se ajusta la descripción de activos y tipos de activos haciendo uso de infografía.
		8.2.4 Riesgos fiscales	Se agrega todo lo relacionado a los riesgos fiscales, como identificarlos y su redacción.

Elaboró	***Revisó***	***Aprobó***
Equipo Grupo Gestión de la Calidad *Oficina Asesora de Planeación* *28/06/2024*	*Yineth Pérez Torres* *Responsable Mejora Continua* *Sistema de Gestión COGUI+* *02/07/2024*	*Carlos Camacho Serge* *Jefe Oficina Asesora de Planeación* *03/07/2024*