Cartilla
Gestión de riesgos

Macroproceso Gestión Estratégica
Proceso Administración Integral de Riesgos
Versión 01
Código CT-PEC-0151
Año 2025

El contenido de este documento corresponde a Información Pública

TABLA DE CONTENIDO

INTRODUCCIÓN

De acuerdo con lo establecido en la Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, la entidad administra su Sistema de Gestión de Riesgos conformada por las siguientes clases de riesgos:

- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos de capital humano.
- Riesgos ambientales.
- Riesgos de integridad.
- Riesgos fiscales.
- Riesgos seguridad de la información.
- Riesgos de Seguridad y Salud en el Trabajo - SST.
- Riesgos de cumplimiento Tributario, Aduanero y Cambiario TAC.
- Riesgos de lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LAFT/FPADM.

La metodología definida en esta cartilla no aplica para los riesgos de seguridad y salud en el trabajo - SST, los riesgos de seguridad de la información, los riesgos LAFT/FPADM y los riesgos de cumplimiento Tributario, Aduanero y Cambiario TAC, los cuales tienen otro abordaje de acuerdo con los lineamientos definidos por la Subdirección de Desarrollo de Talento Humano, la Oficina de Seguridad de la Información, la Subdirección de Apoyo en la Lucha contra el Delito Aduanero y Fiscal y la Subdirección de Riesgo y Programas respectivamente.

Así mismo, es importante resaltar que la presente cartilla de Gestión de Riesgos de la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales, en adelante UAE DIAN es un documento de carácter pedagógico que orienta la identificación, valoración y tratamiento de los riesgos de la entidad definidos en el alcance de este documento.

Se ha elaborado tomando como referencia:

- La Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6, noviembre 2022. Dirección de Gestión y Desempeño Institucional – Departamento Administrativo de la Función Pública.
- Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG. V6. Diciembre 2024.
- TADAT 2019 - Herramienta para el diagnóstico y evaluación de la administración tributaria.
- NTC-ISO 31000:2018. Gestión del riesgo – Directrices.
- Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, Versión 3 - 04 de diciembre de 2024."

1. OBJETIVO

Orientar la identificación, valoración, tratamiento y seguimiento de los riesgos en la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, en cumplimiento de los lineamientos institucionales y de acuerdo con las mejores prácticas en gestión de riesgos; contribuyendo al fortalecimiento de la cultura de gestión de riesgos en la entidad, a la toma de decisiones informadas y a la mejora continua de los procesos.

2. ALCANCE

Aplica para todos los procesos, niveles de operación y prestación de servicios de la entidad, conforme a la responsabilidad y autoridad definida para la gestión de los siguientes riesgos.

- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos de capital humano.
- Riesgos ambientales.
- Riesgos de integridad.
- Riesgos fiscales.

3. SIGLAS Y DEFINICIONES

- **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. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP.*

- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Causa Inmediata**: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. En el caso de riesgos fiscales, se usa el término Circunstancia Inmediata. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Causa Raíz**: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **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. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Control:** medida que permite reducir o mitigar un riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **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. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Factores de riesgo**: son las fuentes generadoras de riesgos. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP.*

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar la organización con relación al riesgo. *Fuente: NTC ISO 31000:2018. Gestión de riesgos.*

- **Hallazgo administrativo:** todos los hallazgos determinados son administrativos, sin perjuicio de sus efectos fiscales, penales, disciplinarios y corresponden a todas aquellas situaciones que hagan ineficaz, ineficiente, inequitativa, antieconómica o insostenible ambientalmente, la actuación del auditado, que viole la normatividad legal y reglamentaria o impacte la gestión y el resultado del auditado (efecto). *Fuente: Guía de Auditoría Territorial – GAT. Noviembre 2012.*

- **Hallazgo con presunta connotación disciplinaria:** hallazgo administrativo en el cual se evidencia que, por acción u omisión, servidores públicos o particulares, que transitoriamente ejerzan funciones públicas, han incurrido en un presunto incumplimiento del deber funcional tipificado en la ley como falta disciplinaria. *Fuente: Guía de Auditoría Territorial – GAT. Noviembre 2012.*

- **Hallazgo con presunta connotación fiscal:** hallazgo administrativo mediante el cual se establece que los servidores públicos y/o particulares han realizado una gestión fiscal ineficaz y antieconómica, contraria a los principios establecidos para la función pública, que han producido un daño patrimonial al Estado. *Fuente: Guía de Auditoría Territorial – GAT. Noviembre 2012.*

- **Hallazgo con presunta connotación penal:** hallazgo administrativo en el cual se observa que, por acción u omisión, servidores públicos o particulares, que transitoriamente ejercen funciones públicas, han incurrido en un presunto hecho punible tipificado en la ley como delito. *Fuente: Guía de Auditoría Territorial – GAT. Noviembre 2012.*

- **Impacto**: son las consecuencias a las cuales se ve expuesta la organización en caso de materializarse un riesgo, como pueden ser la afectación económica (o presupuestal) y reputacional, entre otros. *Fuente: Basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Mapa de Riesgo Inherente:** instrumento que permite visualizar los riesgos en un plano cuyas coordenadas representan la probabilidad e impacto de este, antes de ejecutar los controles. *Fuente: Subdirección de Procesos UAE DIAN.*

- **Mapa de Riesgo Residual:** instrumento que permite visualizar los riesgos en un plano cuyas coordenadas representan la probabilidad e impacto de este, una vez se hayan ejecutado los controles. *Fuente: Subdirección de Procesos UAE DIAN*.

- **Materialización de riesgo:** es un evento que genera o podría generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología. *Fuente: Basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Nivel de 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 es 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. Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP*.

- **Política para la gestión del riesgo**: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Probabilidad**: se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública – DAFP.*

- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgos ambientales:** posibilidad de generar daño en el ambiente, debido tanto a un fenómeno natural como a la acción humana en el desarrollo de las operaciones. *Fuente: Subdirección de Procesos UAE DIAN.*

- **Riesgo de capital humano:** incapacidad de maximizar la efectividad de la administración tributaria debido a la falta de competencia, capacidad, cumplimiento, costo y compromiso de sus funcionarios. *Fuente: Herramienta de evaluación y diagnóstico de la administración tributaria-TADAT.2019.*

- **Riesgo de integridad:** son aquellos riesgos que están asociados a conflictos de intereses, soborno, corrupción y fraude.
  - **Conflicto de intereses**: cuando el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público. Fuente: *artículo 44 del Código General Disciplinario (Ley 1952 de 2019).*
  - **Soborno:** es una conducta tipificada dentro del sistema penal colombiano que se refiere al acto de dar u ofrecer a otra persona una dádiva para conseguir que, de forma ilícita, se favorezcan sus intereses. (según la naturaleza de los sujetos este puede tipificarse como cohecho, soborno o soborno trasnacional).
  - **Corrupción:** se entiende como el uso del poder para desviar la gestión de lo público hacia el beneficio privado, afectando la garantía de los derechos humanos y derechos fundamentales de las personas. En esa medida, un acto de corrupción comprende diferentes conductas tipificadas por el sistema penal y el sistema disciplinario.
  - **Fraude:** cualquier acto ilegal caracterizado por ser un engaño, ocultación o violación de confianza, que no requiere la aplicación de amenaza, violencia o de fuerza física, perpetrado por individuos y/u organizaciones internos o ajenos a la entidad con el fin de apropiarse de dinero, bienes o servicios.

  Fuente. Anexo técnico programas de transparencia y ética pública. Secretaría de Transparencia.2024

- **Riesgos estratégicos:** son aquellos riesgos que pueden afectar el logro, desarrollo y/o ejecución de los objetivos estratégicos o de los elementos estratégicos de la UAE DIAN que hagan sus veces. Se obtienen a partir del ejercicio de análisis y contexto estratégico, el cual hace parte de la formulación del Plan Estratégico cuatrienal. *Fuente: Subdirección de Planeación y Cumplimiento UAE DIAN.*

- **Riesgo fiscal:** es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgos operacionales:** efecto que se causa sobre los objetivos del proceso, debido a eventos potenciales. *Fuente: Adaptado por la Coordinación de Procesos y Riesgos Operacionales. Basado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo Inherente**: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Riesgo Residual**: el resultado de aplicar la efectividad de los controles al riesgo inherente. *Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6, 2022. Departamento Administrativo de la Función Pública - DAFP.*

- **Sistema de Gestión de Riesgos:** comprende el marco y proceso estructurado para la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos que pueden afectar el cumplimiento de sus objetivos institucionales y operación de los procesos. *Fuente: Subdirección de Procesos UAE DIAN*.

- **Tratamiento**: consiste en seleccionar e implementar opciones para abordar el riesgo. *Fuente: NTC ISO 31000:2018. Gestión de riesgos.*

- **Valoración**: implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. *Fuente: NTC ISO 31000:2018. Gestión de riesgos.*

4. DESARROLLO DEL TEMA

La estructura metodológica para la gestión de los riesgos se basa en la establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6, noviembre 2022 y para la UAE – DIAN será como se muestra a continuación:

Figura 1. Metodología para la administración del riesgo

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

La UAE DIAN ha establecido que la gestión de los riesgos definidos en el alcance de esta cartilla se hará por medio de la herramienta GRC NOVASEC o la que la sustituya, para lo cual se definirá el manual de usuario que estará disponible en el Listado Maestro de Documentos de la Entidad.

4.1. Política para la administración de riesgos

La política para la administración de riesgos de la entidad debe incluir la declaración, compromiso y lineamientos integrales frente a la gestión de los riesgos en todos los niveles de su operación, enmarcado en el cumplimiento de su planeación estratégica.

Debe contemplar como mínimo el alcance, objetivo, principios, responsabilidad y autoridad frente a la gestión de los riesgos, la metodología y niveles de aceptación del riesgo de acuerdo con tipo de riesgo, y los términos y definiciones.

La Alta Dirección (con el liderazgo del representante legal) define y aprueba la política en el marco del Comité Institucional de Coordinación de Control Interno, así mismo, en el marco del Comité Institucional de Gestión y Desempeño, la Alta Dirección define los lineamientos estratégicos para la administración del Sistema de Gestión de Riesgos y realiza seguimiento de dicha gestión a partir de los resultados presentados por los diferentes tipos de riesgos.

La actualización de la Política se realizará considerando los análisis del entorno, posibles cambios en la operación o en los lineamientos de la entidad. La política se debe publicar en DIANNET y los responsables de los procesos deben asegurar su divulgación, socialización y entendimiento por parte de los servidores públicos de la entidad.

4.2. Analizar el contexto

Para el análisis del contexto, es fundamental conocer la Planeación Estratégica, el diagnóstico organizacional y el modelo de operación de los procesos de la entidad, identificando los elementos relevantes que guardan relación con el proceso objeto de análisis. Esta comprensión, permite reconocer las amenazas, oportunidades, fortalezas y debilidades que puedan incidir en el cumplimiento de los objetivos del proceso.

En el caso de los riesgos estratégicos, el análisis debe centrarse en el contexto estratégico de la entidad, considerando aspectos como la filosofía institucional, los elementos de visión, la alineación institucional y los resultados de la vigilancia estratégica, entre otros. El propósito, es identificar y evaluar aquellas situaciones que puedan impactar la capacidad de la entidad para generar valor público, así como aquellas que puedan obstaculizar el logro de sus objetivos o elementos estratégicos y metas institucionales.

Adicionalmente, se debe tener en cuenta el análisis del entorno que pueda afectar la continuidad del negocio. Este análisis será desarrollado por el equipo de continuidad de negocio que se defina en la entidad, conforme a los lineamientos y metodologías establecidos para tal fin.

4.3. Identificación de los riesgos

Los responsables de los procesos determinan los servidores públicos expertos que actualizarán los riesgos asociados al respectivo proceso, con el acompañamiento metodológico de los servidores públicos asignados por tipo de riesgo de acuerdo con el Anexo 1. Responsables metodológicos por tipo de riesgo.

A través de la utilización de herramientas como la lluvia de ideas, encuestas, entrevistas, entre otras, los servidores públicos expertos de los procesos con el acompañamiento de los responsables

metodológicos por tipo de riesgo identifican los riesgos que pueden incidir en el cumplimiento de los objetivos de la entidad y/o de los procesos, así como las causas que los generan y los impactos que implicarían su materialización.

Para identificar los riesgos asociados a los procesos o a los objetivos estratégicos/elementos estratégicos, se tendrá en cuenta el análisis del contexto y se analizarán los siguientes elementos:

4.3.1. Identificar puntos de riesgo

Teniendo en cuenta el mapa de procesos, se identifica el proceso al que se le van a establecer los riesgos, se revisa su caracterización o descripción de su funcionamiento (condiciones y elementos), para abordar los siguientes aspectos:

- A**lcance y objetivo del proceso,** se debe establecer su relación con los objetivos estratégicos/elementos estratégicos.

  Se debe realizar el análisis de estos objetivos de proceso, en cuanto a si están adecuadamente definidos, tienen metas claras, con tiempos establecidos *(Puede aplicar la técnica SMART: Specific, Mensurable, Achievable, Relevant, Timely que en español significa específico, medible, alcanzable, relevante y temporal)*[1]*.* El análisis incluye tener identificadas condiciones actuales de proceso que puedan afectar el logro de estos objetivos.

- Identificar las **actividades críticas** o actividades en las que potencialmente se genera el riesgo, es decir, aquellas actividades que se deben mantener bajo control para evitar que falencias en su ejecución puedan afectar el cumplimiento del objetivo. Dichas actividades críticas deben estar definidas en el diagrama o flujo del proceso.

- Identificar los **productos, servicios o salidas** que impactan de forma directa la prestación de los servicios de la entidad.

- Considerar factores de riesgo, incluyendo condiciones, situaciones, coyunturas, hechos o elementos del proceso, que puedan generar riesgo, y que es relevante tener controlados.

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal, es decir, las actividades que representen gestión fiscal como las de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

Se debe indagar en qué procesos de la entidad se realiza gestión fiscal y cuáles son esas actividades.

Así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal. Por tanto, se debe clasificar por proceso los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias

1 Fuentes: https://asana.com/es/resources/smart-goals *y https://www.coloradotech.edu/blog/2018/march/effective-goal-setting-tactics-how-students-can-set-smart-goals*

de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-.

Es importante consultar el "Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1) de la guía para la administración del riesgo y el diseño de controles en entidades públicas[2], y verificar si son aplicables a la entidad y por tanto si se tendrá en cuenta.

Para la identificación de los riesgos estratégicos se determinan los procesos responsables de gestionar cada elemento de visión o lineamiento estratégico, para establecer las actividades donde exista evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo como se indica en el primer párrafo del presente numeral.

4.3.2. Identificar áreas de impacto

Posterior a la identificación de los puntos de riesgos, y durante las reuniones del equipo de trabajo que está realizando el ejercicio de identificación de los riesgos, se debe señalar cuál es el impacto frente a cada punto de riesgo en caso de materializarse, con base en dos variables:

i) Consecuencia o afectación económica (recaudo y presupuesto).
ii) Consecuencia o afectación reputacional.

Nota: Las dos variables anteriores no son excluyentes, por tal razón, en caso de identificar que el impacto se materializa en las dos variables se podrán seleccionar ambas opciones (económica y reputacional).

Para el **riesgo fiscal**, el área de impacto siempre corresponderá a una **consecuencia económica** sobre el interés patrimonial o el bien, recurso de carácter público, al cual se vería expuesta la organización en caso de materializarse el riesgo.

4.3.3. Identificar factores de riesgo o fuentes generadoras de riesgos

La identificación de los factores de riesgo permite categorizar las causas inmediatas, circunstancias inmediatas y causas raíz según aplique.

Para determinar los factores asociados a los riesgos que se estén identificando se debe tener en cuenta la siguiente tabla, en la cual se describen:

Tabla 1. Factores de riesgo

Factor	Definición	Descripción – Causas asociadas
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización. ***Ejecución y administración de procesos***	• Diseños inadecuados de los procesos y herramientas de gestión, control y seguimiento o deficiencias en los mismos. • Falta, deficiencias o desactualización de los procedimientos o documentos que apoyan la ejecución de las actividades. • Planeación de necesidades, de recursos para realizar las actividades, programación presupuestal, entre otros.

[2] *Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6, noviembre 2022. Dirección de Gestión y Desempeño Institucional - Departamento Administrativo de la Función Pública.*

Talento Humano: 1. Competencia. 2. Capacidad. 3. Cumplimiento. 4. Costos. 5. Compromiso	Eventos relacionados con los efectos del comportamiento de personas sobre el trabajo	1) Competencia: considera la brecha entre habilidades existentes y necesidades, la búsqueda de habilidades críticas, el uso de la subcontratación y retención de talento, y el desarrollo de habilidades. 2) Capacidad: abarca la implementación de un marco de planificación de sucesión, la preparación para roles de liderazgo y la promoción de diversidad e inclusión. 3) Cumplimiento: implica asegurar una evaluación objetiva del desempeño, cumplimiento de leyes laborales, aplicar políticas de manera uniforme y adherirse a las regulaciones de salud y seguridad. 4) Costos: incluye garantizar la asequibilidad laboral, analizar el impacto de la pérdida de conocimiento, alinear la remuneración con el rendimiento, utilizar análisis para una visión a largo plazo de costos laborales y planificar recursos para gestionar talento. 5) Compromiso: promover el compromiso y la motivación de los funcionarios, e identificar y promover el intercambio de talento y habilidades en toda la entidad.
Integridad: 1. Conflicto de intereses 2. Soborno 3. Corrupción 4. Fraude	Se analiza posible dolo e intención frente al fraude y corrupción, así mismo, la prevalencia o priorización del interés privado/particular sobre el público o interés general. Posibles comportamientos no éticos de los servidores públicos.	• Conflicto de intereses: el interés general propio de la función pública entra en conflicto con el interés particular y directo del servidor público. • Soborno: dar u ofrecer a otra persona una dádiva para conseguir que, de forma ilícita, se favorezcan sus intereses. • Corrupción: uso del poder para desviar la gestión de lo público hacia el beneficio privado • Fraude: engaño, ocultación o violación de confianza, que no requiere la aplicación de amenaza, violencia o de fuerza física, perpetrado por individuos y/u organizaciones internos o ajenos a la entidad con el fin de apropiarse de dinero, bienes o servicios.
Tecnología*	Eventos relacionados con la infraestructura tecnológica de la Entidad. ***Fallas o afectación infraestructura tecnológica***	• Daño de equipos • Inexistencia de aplicaciones, plataformas, etc • Caída de aplicaciones • Caída de redes • Errores en programas • Vulnerabilidad de bases de datos / programas
Infraestructura	Eventos relacionados con la infraestructura física de la Entidad. ***Afectación a la propiedad, planta y equipos de la Entidad***	• Infraestructura deficiente • Daños a activos fijos • Condiciones inapropiadas de la infraestructura: edificio, equipos, maquinaria y herramientas.
Ambiental	Eventos que generan cambios adversos en el ambiente como resultado total o parcial de la interacción con los aspectos ambientales de una organización.	• Prácticas que generan contaminación del aire, suelo, agua. • Uso de tecnología obsoleta que genera impactos ambientales. • Prácticas que conllevan el aumento relevante en el consumo energético. • Prácticas que conllevan generación de residuos sin eficiente disposición.
Eventos externos o de emergencia	Situaciones externas o de emergencia que afectan la entidad.	• Afectación de orden público que impide movilidad, desplazamiento de los servidores o prestación de los servicios de la DIAN. • Atentados, asaltos a oficinas de la Entidad. • Situaciones de vandalismo que pueden afectar personas o activos de la DIAN. • Suplantación de Identidad de individuos actuando a nombre de la Institución. • Situaciones de emergencia (Derrumbes, Incendios, Inundaciones, entre otros), caso fortuito o de fuerza mayor que afecten la operación. (grupos de valor y prestación Productos o servicios).

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Se debe revisar los factores o fuentes de riesgos y con base a estos, asociar sus causas.

Notas:

Tecnología*: Cuando se presenta el factor de riesgo tecnología, se debe tener en cuenta que en el análisis es necesaria la revisión de la posible afectación de la disponibilidad, integridad y

confidencialidad de los activos de información identificados en el proceso, esta situación se evaluará en conjunto con la Oficina de Seguridad de la Información para la respectiva gestión.

Para el análisis de causas de los riesgos de integridad se podrá tener en cuenta la siguiente tabla:

Tabla 2. Causas para tener en cuenta en la identificación de los riesgos de Integridad

CAUSAS ASOCIADAS A RIESGOS DE INTEGRIDAD
• Deficiencias en los procesos que involucran manejo de dinero en efectivo. • Inexistencia de archivos contables. • Arqueos de caja adelantados por personal no idóneo y sin la autoridad requerida (adelantada por el mismo servidor o bien por otro servidor que no cuenta con un nivel jerárquico superior). • Gestión Documental con fondos acumulados que no garantizan los registros y memoria institucional. • Falta de segregación de funciones por restricciones de planta. • Discrecionalidad para la gestión de trámites y servicios (sin protocolos o procedimientos de atención). • Fallas en el apoyo jurídico interno que generan interpretación subjetiva de las normas o reglamentos. • Factores externos de presión en temas regulados que pueden incidir en las decisiones institucionales. • Servidores con conflictos de interés en los temas sobre los cuales pueden incidir con su toma de decisiones. • Ausencia o debilidad de medidas y/o políticas para la identificación y manejo de conflictos de interés. • Discrecionalidad para la toma de decisiones en grupos restringidos de servidores públicos. • Fases de análisis de los requisitos con excesiva reserva que impida la transparencia en determinado proceso. • Falta de inclusión de acuerdos de confidencialidad y manejo de información interna que facilita su divulgación y uso no autorizado de información privilegiada. • Falta de herramientas tecnológicas para la transmisión de datos e información entre procesos y a nivel externo. • Ausencia de sistemas de información, que pueden facilitar el acceso indebido a la información y su posible manipulación o adulteración. • Falta de controles internos y externos efectivos en los procesos y procedimientos, necesarios para el desarrollo de la gestión (Oportunidad) • Fallas éticas y de compromiso con lo público que afectan un desarrollo objetivo e imparcial en el manejo y regulación de los recursos públicos (Responsabilidad). • Factores que afectan las conductas de integridad pública y propician riesgos de corrupción. • Factores externos que afectan las conductas de integridad pública y propician riesgos de corrupción, tales como el contexto del mercado y variables culturales que se manifiestan en ofrecimiento de dádivas por acción u omisión de los servidores públicos provenientes de carteles de contratistas o grupos legales e ilegales (Presión).

Fuente: FURAG – Medición del desempeño institucional. Vigencia 2024. Función Pública.

Nota: Pueden existir otras causas que no se encuentren en la anterior tabla y que deberán ser contempladas en el análisis de acuerdo con el criterio de los expertos que estén participando del ejercicio.

Para el análisis de causas de los **riesgos fiscales** se podrá consultar el “Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas” (anexo1) de la guía para la

administración del riesgo y el diseño de controles en entidades públicas[3], y verificar si son aplicables a la entidad y por tanto si se tendrán en cuenta, no obstante, pueden existir otras causas de acuerdo con el criterio de los expertos que estén participando en el ejercicio.

4.3.4. Definir la clase de riesgo

Se debe establecer la clase del riesgo teniendo en cuenta el alcance de esta cartilla:

Clases:

- Riesgos estratégicos.
- Riesgos operacionales.
- Riesgos de capital humano.
- Riesgos ambientales.
- Riesgos de integridad.
- Riesgos fiscales.

En esta parte del análisis se debe considerar lo siguiente:

1. Cualquier clase de riesgos puede afectar **la continuidad de negocio**, se deben identificar y tener en cuenta en la definición de controles y se deben incluir aquellos asociados al **plan de continuidad del negocio como las estrategias para procesos críticos, protocolos de crisis, incidentes, planes de emergencias**, entre otros.

   Así mismo, en el análisis de riesgos se debe establecer si el riesgo en caso de materializarse podría afectar la **prestación de un producto o servicio** de la entidad.

2. Para determinar los posibles factores de riesgo de acuerdo con la clase de riesgo, se tendrá en cuenta la siguiente tabla:

Tabla 3. Relación entre los factores y clases de riesgos

CLASE DE RIESGO	FACTOR DE RIESGO ASOCIADO		POSIBLE AFECTACIÓN
• Operacionales • Fiscales • Estratégicos • Ambientales	Proceso Tecnología Infraestructura	Eventos externos o de emergencia	• Afectación de la Continuidad de negocio • Afectación a productos y servicios de la entidad
• Capital Humano • Operacionales • Fiscales • Estratégicos • Ambientales	Talento Humano: 1. Competencia. 2. Capacidad. 3. Cumplimiento. 4. Costos. 5. Compromiso		
• Integridad • Estratégicos	Integridad: 1. Conflicto de intereses 2. Soborno 3. Corrupción 4. Fraude		

[3] *Fuente: Ibid. 11.*

• Ambientales	Ambiental		

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

4.3.5. Describir el riesgo

En la identificación y descripción de los riesgos, debemos tener presente lo siguiente:

- Los participantes deben hacerse la pregunta dependiendo de la clase de riesgo:

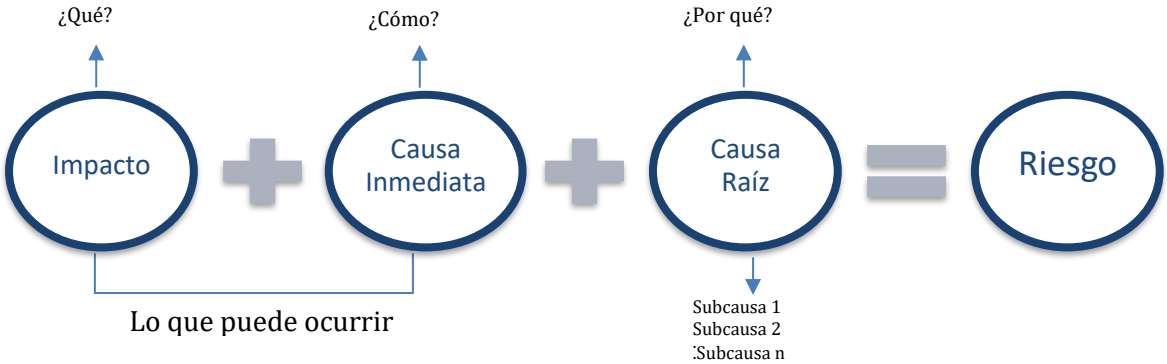
  - **Riesgos estratégicos:** ¿Qué puede suceder que afecte el logro de los lineamientos/objetivos o elementos estratégicos de la entidad?
  - **Riesgos operacionales:** ¿Qué puede suceder que afecte el logro de los objetivos del proceso?
  - **Riesgos de integridad:** ¿Qué puede suceder en el proceso que afecte el logro de sus objetivos y esté asociado al desvío de la gestión de lo público hacia un beneficio privado?
  - **Riesgos ambientales:** ¿Qué puede suceder dentro del proceso que genere impacto ambiental?
  - **Riesgos fiscales:** ¿Qué puede suceder dentro del proceso que genere un efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública?
  - **Riesgos de capital humano:** ¿Qué puede suceder que afecte la gestión del capital humano de la entidad?

Se debe tener en cuenta la planeación estratégica, las actividades críticas del proceso, sus productos, servicios o salidas principales y las situaciones que se han presentado y lo han afectado, con el fin de establecer las situaciones no deseadas.

- **¿Cómo se debe redactar el riesgo?**

Para describir el riesgo se debe tener en cuenta la siguiente estructura:

Figura 2. Descripción de los riesgos operacionales, estratégicos, de capital humano y ambientales



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Conforme a lo expuesto en la Guía de Administración del Riesgo Versión 6 del DAFP, se define:

- **Impacto**: las consecuencias que puede ocasionar a la organización la materialización del riesgo. Tener en cuenta lo definido en el ítem 4.3.2. Identificar áreas de impacto.

- **Causa inmediata**: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo y se genera el impacto, 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.

Ejemplo:

Tabla 4. Ejemplo descripción del riesgo

Redacción inicia con:	¿Qué	¿Cómo?	¿Por qué?
Posibilidad de	Afectación económica	Por multa o sanción del ente regulador	Debido a adquisición de bienes y servicios fuera de los requerimientos normativos

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Nota: una vez definida la causa raíz se identifican las subcausas asociadas según aplique, teniendo en cuenta los factores de riesgo establecidos en el numeral 4.2.4 Identificar factores de riesgo o fuentes generadoras de riesgos.

Riesgos de integridad.

Para evitar confusiones entre un riesgo operacional y un riesgo de integridad, en el análisis se debe tener en cuenta que en el riesgo de integridad la situación no deseada se puede presentar por conflictos de intereses, soborno, corrupción y fraude.
Ejemplos:

Soborno:
- Posibilidad de recibir o solicitar beneficios o dádivas con el fin de celebrar un contrato para beneficio propio y/o de terceros.

Corrupción:
- Posibilidad de divulgar información confidencial, sin autorización, inoportuna o de reserva para beneficio propio y/o de terceros.
- Posibilidad de dilación o aceleración de trámites irregularmente para beneficio propio y/o de terceros.

Fraude:
- Posibilidad de ocultar, alterar o eliminar la información que sustenta la decisión para beneficio propio y/o de terceros.
- Posibilidad de alterar saldos y desvío de recursos públicos para beneficio propio y/o de terceros.
- Posibilidad de emitir decisión final de un proceso de control basada en hechos falsos o información adulterada para beneficio propio y/o de terceros.

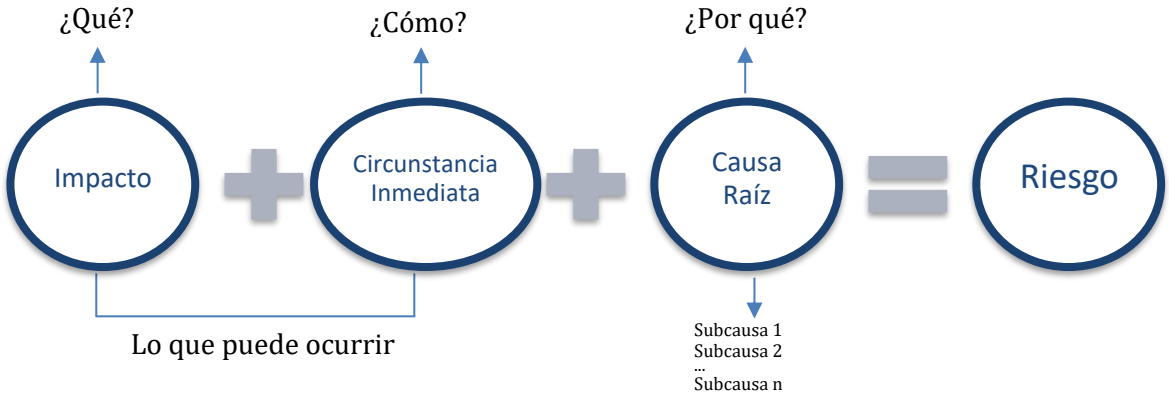
Conflictos de intereses:

- Posibilidad de contraer obligaciones con personas naturales o jurídicas con las cuales se tengan relaciones oficiales debido al cargo que desempeña violando el régimen de inhabilidades e incompatibilidades señaladas en las normas vigentes.

Riesgos fiscales.

Para la descripción del riesgo fiscal se debe tener en cuenta el impacto, la circunstancia inmediata y la causa raíz como se muestra a continuación:

Figura 3. Descripción de los riesgos fiscales



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Conforme a lo expuesto en la Guía de Administración del Riesgo Versión 6 del DAFP, se define:

- **Impacto**: consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.
  Efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).
  Tener en cuenta lo definido en el ítem 4.3.2. Identificar áreas de impacto.

- **Circunstancia inmediata:** se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica -causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas. Corresponde al cómo.

  Para facilitar la definición de circunstancia inmediata se puede tener en cuenta lo siguiente:

  Revisar cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos años. Analizar dichas causas y corroborar si aplica para el riesgo identificado.

Consultar el "Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1) de la guía para la administración del riesgo y el diseño de controles en entidades públicas[4], y verificar si son aplicables a la entidad y por tanto se tendrán en cuenta.

- **Causa raíz**: cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015). Corresponde al por qué, al hecho generador del daño.
  Ejemplos:

Tabla 5. Ejemplo descripción del riesgo fiscal

Impacto ¿Qué?	Circunstancia inmediata ¿Cómo?	Causa raíz ¿Por qué?
Posibilidad de efectos dañoso sobre bienes públicos	por pérdida, extravío o hurto de bienes muebles de la entidad	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén
Posibilidad de efecto dañoso sobre los recursos públicos,	por pago de multa impuesta por la autoridad ambiental,	a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.
Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública,	por no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo,	a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

La descripción del riesgo debe incluir los elementos mencionados anteriormente para que se pueda entender, tanto por los involucrados en el proceso, como por cualquier persona o miembro de la organización. En consecuencia, exige un esfuerzo de redacción con un ánimo de entendimiento y claridad.

Es importante evitar describir el riesgo como la negación, omisión o desviación del control.

4.4. Valorar los riesgos

La valoración del riesgo incluye el análisis y la evaluación de riesgos, los cuales se describen a continuación:

4.4.1. Analizar los riesgos

Consiste en establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, determinando la zona de riesgo inicial o riesgo inherente.

[4] *Fuente: Ibid. 11.*

4.4.1.1. Determinar la probabilidad

Hace referencia a la posibilidad de ocurrencia del riesgo, asociada a su exposición en la entidad y/o el proceso; por tanto, la probabilidad es el número de veces que se pasa por el punto de riesgo en el periodo de un año. Es decir, se analiza la frecuencia con la que se lleva a cabo la actividad que conlleva el riesgo.

Tabla 6. Criterios para definir la probabilidad

	FRECUENCIA DE LA ACTIVIDAD		PROBABILIDAD
	Actividades que se ejecutan máximo 15000 veces en el año	***Actividades que se ejecutan más de 15000 veces en el año***	
MUY BAJA	La actividad que conlleva el riesgo se ejecuta como máximo 1 vez al año (x≤1)	La actividad que conlleva el riesgo se ejecuta entre 15000 < x ≤ 23000	**20%**
BAJA	La actividad que conlleva el riesgo se ejecuta más de 1 vez a 20 veces en el año	La actividad que conlleva el riesgo se ejecuta de 23001 a 70000 veces en el año	**40%**
MEDIA	La actividad que conlleva el riesgo se ejecuta de 21 a 500 veces en el año	I >70.001 <=900.000	**60%**
ALTA	La actividad que conlleva el riesgo se ejecuta de 501 a 900 veces en el año	>900.001 <=2.000.000	**80%**
MUY ALTA	La actividad que conlleva el riesgo se ejecuta de 901 a 15000 veces en el año	I > 2.000.000	**100%**

Fuente: Construcción propia. UAE DIAN 2025.

4.4.1.2. Determinar el impacto

El área de impacto es la consecuencia económica y/o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.

Para evaluar las consecuencias que se deriven de la materialización de un riesgo se tendrán en cuenta las siguientes dimensiones:

i) Consecuencia o afectación económica (recaudo y presupuesto): costo asociado a la materialización del riesgo analizado desde la perspectiva de la disminución en el recaudo de los tributos y desde la perspectiva del deterioro del presupuesto asignado para el funcionamiento de la entidad.

ii) Consecuencia o afectación reputacional. Detrimento de la imagen de la entidad evaluado desde la percepción del cliente interno y externo, teniendo en cuenta el nivel de alcance o efecto publicitario que se genere.

Nota: cuando se presenten ambas dimensiones de impacto para un riesgo, tanto económico como reputacional con diferentes niveles se debe tomar el nivel más alto.

Para el **riesgo fiscal**, el área de impacto siempre corresponderá a una **consecuencia económica** sobre el interés patrimonial o el bien, recurso de carácter público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

En concordancia con lo expuesto, se define el siguiente cuadro de evaluación del Impacto para riesgo, exceptuando riesgo de integridad:

Tabla 7. criterios para evaluación de impacto del riesgo, excepto integridad			
CATEGORIA	**DIMENSIÓN ECONÓMICA**		**DIMENSIÓN REPUTACION**
	RECAUDO	PRESUPUESTO	
CATASTROFICO 100%	Mayor a 1.000.000 SMLV	Mayor a 1.000 SMLV	El riesgo afecta la imagen de la entidad a nivel nacional, con conocimiento de la situación en los medios de comunicación a nivel nacional y/o internacional.
MAYOR 80%	de 500.001 SMLV a 1.000.000 SMLV	400 SMLV < x ≤ 1.000 SMLV	El riesgo afecta la imagen de la entidad a nivel local, con conocimiento de la situación en medios de comunicación local. (Ciudad, departamento, municipio, etc)
MODERADO 60%	de 25.001 SMLV a 500.000 SMLV	200 SMLV < x ≤400 SMLV	El riesgo afecta la imagen con algunos usuarios, sin repercusión en los medios de comunicación.
MENOR 40%	de 1.001 SMLV a 25.000 SMLV	40 SMLV < x ≤ 200 SMLV	El riesgo afecta la imagen al interior de toda la entidad.
LEVE 20%	Cero a 1000 SMLV	de Cero a 40 SMLV	El riesgo afecta la imagen de algún área de la entidad.

Fuente: Construcción propia. UAE DIAN 2025.

Para los riesgos de integridad no se utilizan las variables de impacto económico o impacto reputacional. Se aplica un cuestionario de 17 preguntas, que se expone a continuación:

Tabla 8. criterios para evaluación de impacto del riesgo integridad

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de servidores del proceso?	0	0
2	¿Afectar el cumplimiento de metas y objetivos del proceso?	0	0
3	¿Afectar el cumplimiento de misión de la entidad?	0	0
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?	0	0
5	¿Afectar la confianza de la entidad, incidiendo en su reputación?	0	0
6	¿Afectar los recursos económicos de la entidad?	0	0
7	¿Afectar la generación de los productos o la prestación de servicios?	0	0
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?	0	0
9	¿Causar pérdida de información de la entidad?	0	0
10	¿Dar lugar a intervención de los órganos de control, de la Fiscalía u otro ente?	0	0
11	¿Dar lugar a procesos sancionatorios?	0	0
12	¿Dar lugar a procesos disciplinarios?	0	0
13	¿Dar lugar a procesos fiscales?	0	0
14	¿Dar lugar a procesos penales?	0	0
15	¿Afectar la credibilidad del sector?	0	0

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA	
		SÍ	NO
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?	0	0
17	¿Ocasionar afectaciones en el ambiente?	0	0
CONTEO RESPUESTAS POR COLOR		**0**	**0**
CALIFICACIÒN DE IMPACTO SEGÚN CONDICIONES AFIRMATIVAS		**MAYOR O CATASTRÓFICO**	

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Responder afirmativamente DE UNO a OCHO preguntas genera un impacto MAYOR.
Responder afirmativamente de NUEVE a DIECISIETE preguntas genera un impacto CATASTROFICO.

Los expertos de los procesos con el acompañamiento metodológico de los responsables por tipo de riesgo deben estimar la zona de riesgo inherente, la cual se obtiene de la combinación entre la estimación de la probabilidad de ocurrencia y el impacto de sus consecuencias, así:

a. Por votación de los integrantes se determina el nivel de probabilidad e impacto, la medición se establece por el criterio de la mayoría de los votos, es decir, la moda.

En los casos mencionados, a continuación, se hace necesario realizar una nueva votación:
• Cuando las calificaciones sean iguales en varios niveles y exista empate.
• Cuando las calificaciones sean demasiado dispersas.
• Cuando persiste empate se vota solamente sobre las opciones que presentan empate. En caso de persistir, el responsable del proceso y los jefes de coordinación deben dirimir.

b. La medición del impacto para cada uno de los riesgos (exceptuando riesgo de fraude y corrupción) debe realizarse para todas las dimensiones. Si no aplica, o es mínimo se debe escoger el valor más bajo, es decir la categoría leve.

Para los riesgos de integridad, el impacto se califica con la tabla adoptada por la DIAN – tabla 8. Criterios para evaluación de impacto del riesgo integridad, de acuerdo con los lineamientos de la DAFP (estos tipos de riesgos no admiten aceptación, es decir, no pueden estar ubicados en zona aceptable o moderada).

c. La calificación final del impacto y probabilidad por riesgo corresponde al nivel más alto que se haya registrado en cualquiera de las dimensiones.

d. La calificación del riesgo es la máxima afectación a la cual puede estar expuesta la entidad.

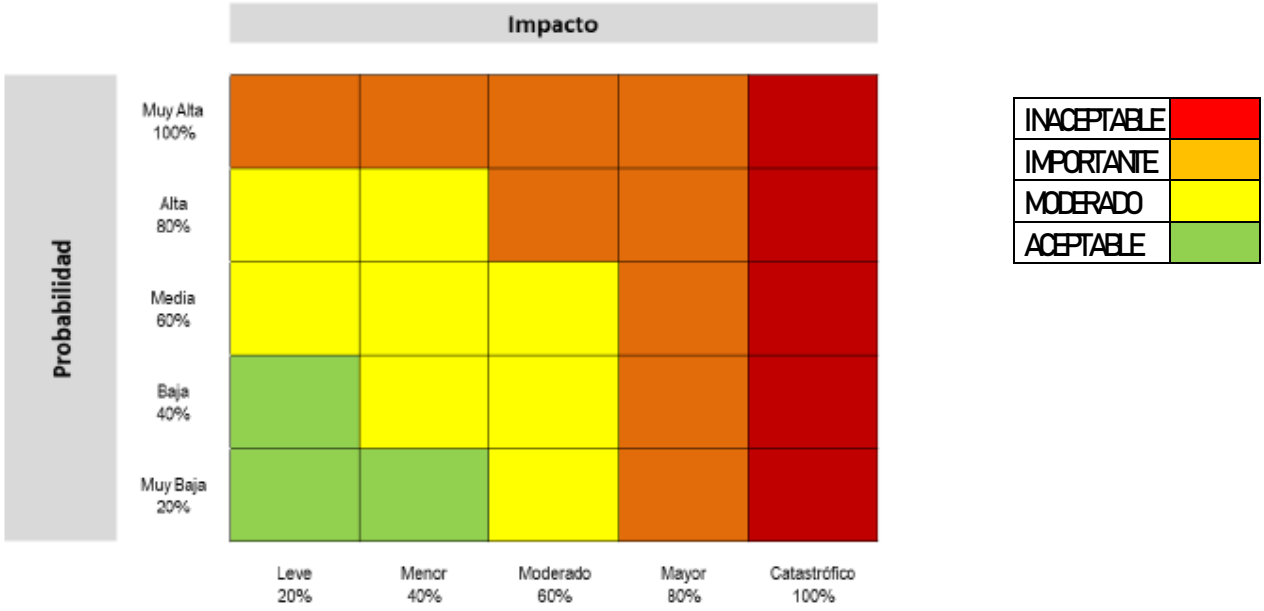
e. La calificación se realiza por parte de los servidores públicos designados para esta labor y los responsables del proceso según aplique.

4.4.2. Evaluar los riesgos

4.4.2.1. Determinar riesgo inherente.

Del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias se determina la zona de riesgo inicial o riesgo inherente. Para la entidad, se determinaron 4 zonas de severidad en el mapa de calor, como se muestra a continuación:

Figura 4. Mapa de calor de riesgos



Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.

Tanto la identificación de los riesgos, como la calificación de la probabilidad e impacto deben ser registradas en el formato Matriz de Riesgos o en la herramienta que se establezca para el efecto.

Ejemplo 1:

Proceso: *Gestión Documental y Archivística*

Objetivo: *Administrar y controlar la gestión Archivística y la Gestión Documental de la Institución, con el propósito de salvaguardar la memoria institucional, para contribuir a la toma de decisiones informadas, trazabilidad de la gestión y brindar la información pertinente a las partes interesadas en las actividades y funciones de la entidad.*

Punto de Riesgo o actividad crítica: *Actualizar y depurar los instrumentos archivísticos y fondos documentales.*

Riesgo identificado - R1: Riesgo identificado - R1: *Posibilidad de pérdida económica y reputacional (área de impacto) por multas y sanciones aplicadas por la Autoridad Archivística (causa inmediata),*

debido a tener los instrumentos archivísticos desactualizados y/o fondos documentales sin depurar (causa raíz).

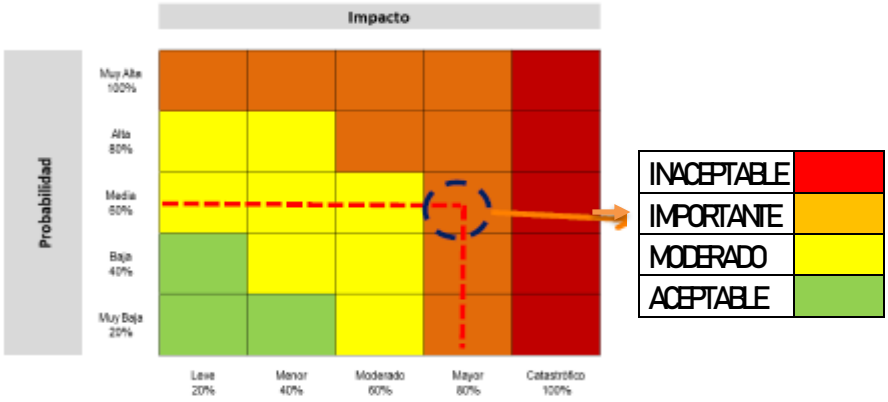
***Clase de riesgo**: Operacional.*

Probabilidad Inherente: media 60%

***Impacto Inherente:** mayor* 80%

***Ubicación matriz de calor**: Cruzando los datos de probabilidad e impacto definidos, el riesgo queda ubicado en la zona de severidad **importante**, como se muestra a continuación.*

Figura 5. Ubicación zona de riesgo operacional



Fuente: Construcción propia. UAE DIAN 2025.

Ejemplo 2:

***Proceso:** Gestión de Recursos*

***Objetivo:** Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.*

***Punto de Riesgo o actividad crítica**: Ingreso, custodia y salida de bienes muebles de la entidad.*
***Riesgo identificado - R1**: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).*

***Clase de riesgo**: Fiscal.*

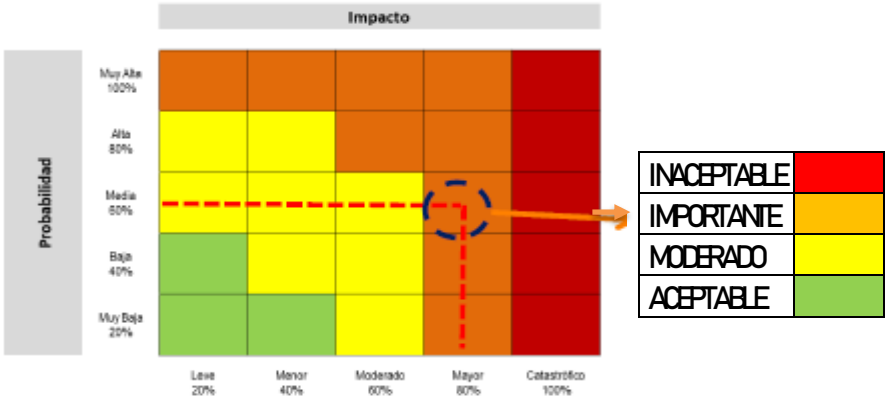
Probabilidad Inherente: media 60%
(Porque para el ejemplo, la actividad de ingreso, custodia y salida de bienes muebles de la entidad se realiza entre 25 a 500 veces al año, por tanto, de acuerdo con la tabla 6. Criterios para definir la probabilidad, quedaría en nivel media).

***Impacto Inherente:** mayor* 80%

Se cuantifica el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública. En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles asumido en $676 millones de pesos, que corresponde a 520 SMLV. De acuerdo con la tabla 7. Criterios para evaluación de impacto del riesgo, el nivel sería mayor.

***Ubicación matriz de calor**: Cruzando los datos de probabilidad e impacto definidos, el riesgo queda ubicado en la zona de severidad o nivel de riesgo **importante**, como se muestra a continuación.*

Figura 6. Ubicación zona de riesgo fiscal



Fuente: Construcción propia. UAE DIAN 2025.

4.4.2.2. Valorar los controles:

Una vez realizado el análisis de probabilidad e impacto de los riesgos, se deben determinar los controles para cada riesgo identificado que se encuentre ubicado en el mapa de riesgo inherente en zona moderada, importante o inaceptable. Para los riesgos que en el análisis de impacto y probabilidad queden ubicados en la zona aceptable del mapa de riesgos inherente, no será necesaria la definición de controles.

El equipo asignado para la identificación de los riesgos (expertos del proceso y responsables metodológicos por tipo de riesgos) identifican los controles a implementar para mitigar dichos riesgos. Estos controles pueden ser: lineamientos definidos en las políticas, en las estrategias de la entidad, actividades de control establecidas en los procesos, procedimientos, dispositivos, entre otros.

Para la redacción del control se debe tener en cuenta la siguiente estructura, de acuerdo con lo definido en la Guía de riesgos DAFP:

- **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, incluyendo manejo de desviaciones según se requiera.

Ejemplos de redacción de controles:

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

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

Una vez definidos los controles, se deben analizar y evaluar de acuerdo con los siguientes atributos:

Tabla 9. Atributos para el diseño de los controles

Atributo	Características		Descripción	Peso
Atributo de eficiencia	**Tipo o propósito del control**	**Preventivo**	Encaminado hacia las causas del riesgo, mitiga la probabilidad de ocurrencia del riesgo.	**30%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Encaminado a mitigar la probabilidad de ocurrencia del riesgo.	**25%**
		Correctivo	Encaminado a mitigar el impacto de la materialización de riesgo.	**20%**
	Sistema de Control	**Automático**	se refiere a que existen servicios informáticos que son los que se encargan de llevar a cabo la ejecución del control.	**15%**
		Semiautomático	Se refiere a los controles que se llevan a cabo mediante el ingreso de datos a un sistema o aplicativo de manera manual.	**10%**
		Manual	Son los controles que se ejecutan sin la ayuda de ningún sistema o aplicativo y que deben ser ejecutados y documentados por los servidores públicos de la Entidad.	**5%**
Atributos informativos	**Evidencia**	**Con registro**	Corresponde a si el control deja evidencia de su operación.	N/A
		Sin registro	El control no deja registro de la ejecución del control.	N/A
	Descripción Evidencia		Se refiere al tipo de evidencia que existe en caso de responder SI a la pregunta anterior. Por ejemplo: Formato, lista de chequeo, actas u otros documentos o registros.	N/A
	Documentado SI/No		Corresponde a si el control está descrito o no, en los procedimientos, lineamientos o cualquier documento del sistema de gestión de la Entidad como una actividad recurrente y formal.	N/A
	Frecuencia		Es la periodicidad con la que se ejecuta el control y puede ser: - **Permanente** - **Diario** - **Semanal** - **Quincenal** - **Mensual** - **Trimestral** - **Cuatrimestral** - **Semestral** - **Anual** - **Por demanda**	N/A
	Nivel de ejecución del Control		Se refiere a dónde debe ser ejecutado el control, teniendo en cuenta para ello los siguientes niveles: - Nivel central - Nivel seccional - Nivel delegado - Central y Seccional - Seccional y Delegado - Todos los niveles	N/A
	Responsable de ejecutar el		Cargo de los servidores públicos que ejecutan el control en el	N/A

Atributo	Características	Descripción	Peso
	Control	proceso, dependencia, entre otros. Según aplique. Está en la redacción del control.	

Fuente: *Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6.*

Los atributos informativos permiten darle formalidad al control y su fin es conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, éstos no tienen una incidencia directa en su eficiencia.

NOTA:
No se acepta zona de riesgo residual moderado o aceptable en los riesgos de fraude y corrupción.
En lo posible máximo 5 controles por riesgos.
Se recomienda implementar un control correctivo, según aplique.

Retomando el ejemplo 1 enunciado en el ítem 4.4.2.1. Determinar riesgo inherente. Se continúa con el análisis para la evaluación de los controles:

Ejemplo 1:

Proceso: *Gestión Documental y Archivística*

Objetivo: *Administrar y controlar la gestión Archivística y la Gestión Documental de la Institución, con el propósito de salvaguardar la memoria institucional, para contribuir a la toma de decisiones informadas, trazabilidad de la gestión y brindar la información pertinente a las partes interesadas en las actividades y funciones de la entidad.*

Riesgo identificado - R1: *Posibilidad de pérdida económica y reputacional por multas y sanciones aplicadas por la Autoridad Archivística por tener los instrumentos archivísticos desactualizados y/o fondos documentales sin depurar.*

Clase de Riesgo*: Operacional.*

Probabilidad Inherente: media 60%

Impacto Inherente: *mayor* 80%

Se identifican 2 controles, y en el siguiente análisis se establecen los cambios en la probabilidad y el impacto del riesgo para determinar el nivel del riesgo residual, teniendo en cuenta los atributos de los controles, conforme a la tabla anterior:

Tabla 10. Datos – análisis de controles ejemplo 1

Probabilidad Inherente	Media	60%
Impacto Inherente	Mayor	80%
zona de severidad	Importante	
Características Control 1:		**Disminuye probabilidad en:** 45%
Tipo de Control	**Preventivo**	30%
Sistema de Control	Automático	15%
Características Control 2:		**Disminuye probabilidad en:** 30%
Tipo de Control:	**Detectivo**	25%
Sistema de Control:	Manual	5%

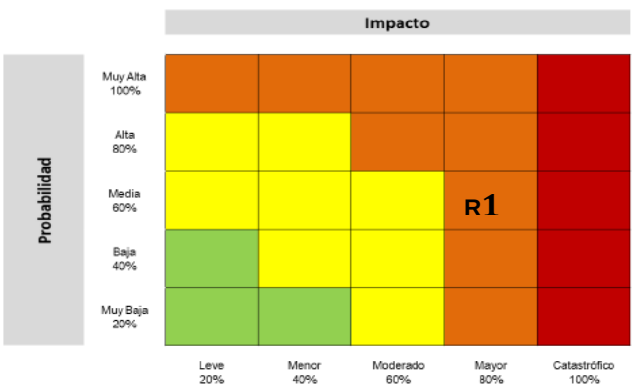
Cálculos que se deben realizar para la aplicación de controles y determinar zona de riesgo residual	Probabilidad Inherente * Valoración control 1 = 60% * 45% = 27% 60 - 27 = 33% Probabilidad aplicado control 1 * Valoración control 2 = **33%** * 30% = 9,9% **33%** - 9,9% = **23,1%** **Probabilidad residual = 23,1%**
	Impacto Inherente = 80% No se establecieron controles correctivos que afectan el impacto, por tanto: **Impacto residual = 80%**

Fuente: Construcción propia. UAE DIAN 2025.

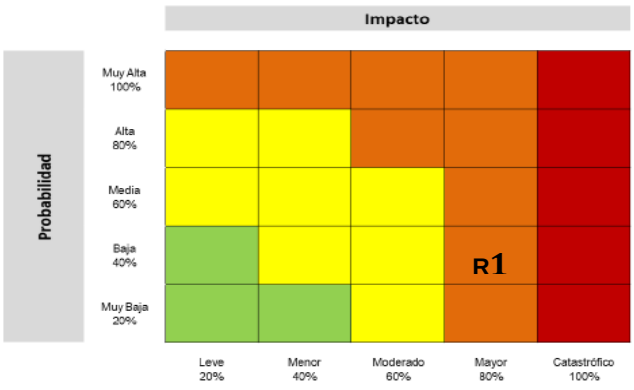
Como se observa, la aplicación de los controles permite mitigar el riesgo de forma acumulativa, entonces una vez se aplica el valor del primer control, al valor resultante se le aplica el siguiente control y así para los siguientes controles que se tengan establecidos para ese riesgo.

Figura 7. Ubicación zona de riesgo inherente y residual

Mapa riesgo inherente



Mapa riesgo residual

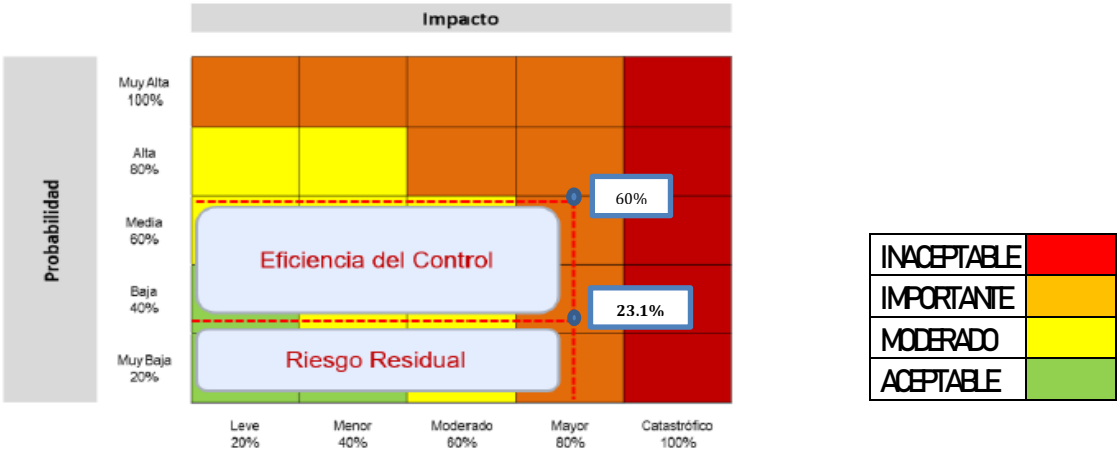


Fuente: Construcción propia. UAE DIAN 2025.

Como se puede observar en las gráficas anteriores, después de aplicados los dos controles, se disminuye la probabilidad de ocurrencia del riesgo quedando ubicado en **probabilidad residual baja y se mantiene en impacto residual mayor,** es decir, **zona de severidad importante.**

Por tanto, la eficiencia de los controles se puede observar, así:

Figura 8. Movimiento en la matriz de calor – eficiencia de los controles



Fuente: Construcción propia. UAE DIAN 2025.

4.4.3. Definir tratamientos o estrategias para combatir el riesgo

Una vez los expertos de los procesos hayan realizado la valoración de los controles y obtenido el riesgo residual, deben establecer el tipo de tratamiento, que puede ser aceptar, reducir o evitar el riesgo.

Figura 9. Estrategias para combatir el riesgo

Fuente: *Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022. V6*

Acorde con lo definido en la Política para la Administración de Riesgos de la entidad: los riesgos estratégicos, operacionales, ambientales, de capital humano y fiscales se deben gestionar por medio de los controles y dependiendo de su ubicación en la zona de riesgo residual se definen los siguientes tratamientos:

Tabla 11. Tratamiento riesgo residual

Zona riesgo residual		Decisión tratamiento riesgo residual
	Inaceptable	Se debe reducir, para lo cual se dan dos opciones: • Transferir: tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. • Mitigar: establecer plan de acción.
	Importante	
	Moderado	Se asume el riesgo y se realiza seguimiento a los controles definidos, el responsable del proceso puede realizar un plan de acción si lo considera necesario.
	Aceptable	Se acepta el riesgo y se realiza seguimiento a los controles definidos.

Fuente: Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, V3. 2024

Establecido el tipo de tratamiento, para la opción **Reducir**, si no se transfiere el riesgo, y se decide mitigar, los expertos técnicos deben formular la(s) acción(es) según aplique, para lo cual se deben tener en cuenta los siguientes elementos:

Tabla 12. Ejemplo de la opción reducir / mitigar – elementos plan de acción

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Digitalizar e implementar software de gestión documental que facilite la actualización de los documentos, su depuración y optimización del acceso a la información.	Oficina de Gestión Documental	01/02/2025	30/12/2025	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la definición del software.	En curso

Fuente: Construcción propia. UAE DIAN 2025.

Para definir el plan de acción, se debe tener en cuenta que, éste no es necesariamente un control adicional, en lo preferible puede estar asociado a un proyecto o tarea específica que esté o se vaya a implementar para apoyar la ejecución de controles definidos previamente.

Este es el paso final en el registro de creación o actualización de la matriz de riesgos aplicable. Dicha matriz debe ser revisada y aprobada por el responsable del proceso.

Para el caso de los riesgos estratégicos, la matriz será revisada por los Directores de Gestión y Oficinas según corresponda y será aprobada por el Subdirector de Planeación y Cumplimiento, quien posteriormente la presentará al Comité Institucional de Gestión y Desempeño (CIGD).
El responsable del proceso debe gestionar la creación o actualización de la matriz de riesgos en la herramienta NOVASEC o la que la sustituya.

4.5. Monitorear y revisar los riesgos

Las herramientas definidas en la UAE DIAN para la gestión de los riesgos son:

4.5.1. Gestión de controles

Establecidos los riesgos que pueden incidir en el cumplimiento de los objetivos estratégicos o elementos de la estrategia, y en los objetivos del proceso respectivamente, los servidores públicos deben ejecutar los controles definidos en las correspondientes matrices de riesgos, atendiendo al nivel de ejecución y periodicidad, y manteniendo las evidencias que demuestran su aplicación. Los líderes de las dependencias deben realizar seguimiento y verificación a la ejecución de los controles que les apliquen y disponer las evidencias de éstos.

Cuatrimestralmente, los gestores de riesgos asignados en las diferentes direcciones seccionales y en los procesos de nivel central, deben informar a los líderes de los procesos el estado de la ejecución de los controles, aspectos relevantes y buenas prácticas realizadas en el periodo. Este reporte lo realizan de acuerdo con lo definido en el numeral 4.5.3 del presente documento.

4.5.2. Gestión de las materializaciones de riesgos

Si como resultado de la ejecución de las labores diarias que deben realizar los servidores públicos en los diferentes niveles, consideran que se ha materializado un riesgo, deben informar a su Jefe inmediato para su análisis en conjunto, definición y ejecución de las acciones y planes de mejora requeridos para atender la situación. Entre las acciones a realizar se encuentran: informar a los entes, clientes, áreas o responsables de los procesos cuando aplique, realizar correcciones inmediatas, actualizar matrices de riesgos, entre otras.

Mensualmente se deben registrar las materializaciones del periodo vigente en la herramienta GRC NOVASEC o la que la sustituya, de la siguiente forma:

Direcciones Seccionales: El Jefe de la División correspondiente, o Jefe de Grupo Interno de Trabajo cuando no dependa de una División, con el apoyo del gestor de riesgos asignado por Dirección Seccional, cargarán en la herramienta GRC NOVASEC o la que la sustituya, los reportes de materialización del mes. En la herramienta, los reportes son notificados para la revisión y aprobación del Director Seccional. Si como resultado del análisis éste considera que corresponde a una materialización, procede a aprobar el evento, y la herramienta notifica al líder del proceso para su revisión y aprobación.

Nivel Central: Los gestores de riesgos asignados por proceso en nivel central cargarán en la herramienta GRC NOVASEC o la que la sustituya los reportes de materialización del mes. En la herramienta el reporte es notificado para revisión y aprobación del jefe inmediato. Si como resultado del análisis éste considera que corresponde a una materialización, procede a aprobar el evento; una vez lo apruebe, la herramienta notifica al líder del proceso para su revisión y aprobación.

En caso de que el líder del proceso no apruebe la situación como una materialización de un riesgo, el sistema notificará al jefe inmediato indicando las razones que justifican el rechazo.

Para los casos de materialización de riesgos reportados, en los cuales no hay claridad en los reportes o hay desacuerdos, es importante un diálogo entre líderes de los procesos y las áreas de nivel central y direcciones seccionales involucradas, de tal forma que se puedan realizar los análisis pertinentes, se

establezcan las acciones y decisiones objetivas con base en las directrices y definiciones tanto metodológicas en riesgos como técnicas propias de cada proceso.

Para realizar el reporte de materialización de riesgos se deben tener en cuenta las siguientes consideraciones:

1) Existen diferentes fuentes por las que se puede obtener información de una posible materialización de riesgo, y las áreas las deben tener en cuenta para realizar el reporte de materialización en el aplicativo NOVASEC o la herramienta que lo sustituya:

   - Autoevaluación o identificación directa por parte de los servidores públicos del proceso o área.
   - Revisión por parte de los responsables del proceso o área.
   - PQRS o denuncias recibidas por los distintos canales.
   - Reporte o revisión realizada por funcionarios de otros procesos o áreas de la Entidad.
   - Auditorías internas o externas.
   - Auditorías o revisiones de calidad RUT (muestra seleccionada, revisión 1% calidad, entre otros).
   - Auditorías ente(s) de control.
   - Reportes de la mesa de ayuda de tecnología a nivel interno.
   - Información del área o procesos asociados a atención del cliente/usuario/ciudadano.
   - Dirección de Gestión Jurídica.
   - Líneas internas de denuncia.
   - Denuncias internas o externas dirigidas a la Dirección General de la UAE DIAN.
   - Reportes de noticias o problemas de imagen debido a fallas en la gestión de la entidad.
   - Reportes de los entes de gobierno.

2) Cuando el riesgo materializado, o sus causas o controles no estén identificados en la matriz de riesgos publicada, de todos modos, deben registrar su materialización en NOVASEC, y después solicitar por correo las respectivas actualizaciones según se requiera al líder metodológico del tipo de riesgo que aplique de acuerdo con el alcance de esta cartilla. Dicha solicitud se hará mediante el diligenciamiento del formato FT-PEC-2100 Solicitud de creación, modificación o inactivación matriz de riesgos para los riesgos operacionales, fiscales, ambientales, de integridad, para los demás riesgos (capital humano y estratégicos) la descripción se realiza en el cuerpo del correo.

3) En el reporte Materialización de Riesgos se debe indicar con un lenguaje claro y preciso, que pasó con la materialización del riesgo, porqué pasó, si afectó un producto o servicio, un elemento de la estrategia o si afectó la continuidad del negocio, si el riesgo materializado se colocó en conocimiento de alguna autoridad (si aplica), el posible alcance que tuvo (administrativo, disciplinario, penal, fiscal) y cuáles fueron las acciones que se implementaron una vez reportado el evento (acciones inmediatas, decisiones tomadas para atender la situación o planes de mejoramiento FT-PEC-1996 Plan de Mejoramiento o de Acción definidos en caso de aplicar).

Nota 1. En caso de materialización de un riesgo de integridad o cualquier otro riesgo que tenga o pueda tener implicaciones disciplinarias, penales o fiscales, deberá ser reportado de manera inmediata a la Subdirección de Asuntos Disciplinarios o a la autoridad competente por parte del Jefe de la dependencia en la cual se materializó el riesgo.

Así mismo, en los casos en que se materialicen riesgos de integridad o riesgos ubicados en zona inaceptable (color rojo) del mapa de riesgo residual, se debe realizar plan de mejoramiento utilizando el formato "FT-PEC-1996 Plan de mejoramiento o de acción", y se debe adjuntar en el reporte de materialización de riesgos en NOVAEC o la herramienta que la sustituya. Los líderes de los procesos y directores seccionales según aplique deben realizar el seguimiento a dichos planes e informar el avance en los informes de monitoreo de riesgos del siguiente cuatrimestre.

Si como resultado del análisis realizado de los reportes de materialización de riesgos y de las demás fuentes de información analizadas, el responsable del proceso determina la necesidad de actualizar la matriz de riesgos, debe solicitar por correo las respectivas actualizaciones según se requiera y remitirlo al buzón del área responsable del tipo de riesgo para los cuales aplica la presente cartilla. Ver anexo 1.

Para las solicitudes de actualización de la matriz de riesgos solicitada por los responsables de los procesos, las áreas líderes de los tipos de riesgos que aplica esta cartilla, de acuerdo con las prioridades y cargas de trabajo, debe coordinar con las áreas solicitantes la agenda de trabajo para la realización de reuniones de actualización de las matrices de riesgos.

4.5.3. Monitoreo y revisión

El monitoreo y revisión de la gestión de riesgos se realizará teniendo en cuenta las responsabilidades definidas en el numeral 5. Tabla 1. Responsables metodológicos por tipo de riesgo y lo definido en el numeral 7. Monitoreo y revisión de la Política para la administración de riesgos de la Dirección de Impuestos y Aduanas Nacionales – UAE DIAN, basado en el marco del esquema de líneas de defensas.

4.5.3.1. Monitoreo y revisión riesgos estratégicos

- Las áreas responsables de la ejecución de los tratamientos (estrategias, controles y planes de acción, entre otros) asociados a los diferentes riesgos estratégicos deben informar cuatrimestralmente el seguimiento por correo electrónico al buzón de la Subdirección de Planeación y Cumplimiento - planeacion@dian.gov.co. Para este seguimiento, tendrán en cuenta los reportes realizados en la herramienta NOVASEC si se materializó un riesgo, así mismo, el estado de la ejecución de los controles, tratamientos y planes de acción.

- A partir de los reportes recibidos, la Subdirección de Planeación y Cumplimiento, debe elaborar el informe consolidado de la gestión de riesgos estratégicos, donde se relacione entre otros, el estado de la ejecución de los tratamientos, planes de acción y si se han materializado riesgos o posibles cambios en la gestión de riesgos *si aplica*; una vez revisado y aprobado el informe por el Subdirector de Planeación y Cumplimiento, es remitido por correo electrónico al Director de Gestión Estratégica y de Analítica, así mismo, se presenta en el Comité Institucional de Gestión y Desempeño.

4.5.3.2. Monitoreo riesgos de capital humano

- Las áreas responsables de la ejecución de los tratamientos (estrategias, controles y planes, entre otros) asociados a los diferentes riesgos de capital humano deben informar cuatrimestralmente el seguimiento por correo electrónico a la Dirección de Gestión Corporativa.

- A partir del reporte recibido, los expertos metodológicos de riesgos de capital humano asignados por la Dirección de Gestión Corporativa, deben elaborar el informe consolidado de la gestión de riesgos de capital humano, donde se relacione entre otros, el estado de la ejecución de los tratamientos, si se han materializado riesgos o posibles cambios en la gestión de riesgos si aplica; una vez revisado el informe por los subdirectores de la Subdirección de Gestión del Empleo Público, la Subdirección de Desarrollo del Talento Humano y la Subdirección Escuela de Impuestos y Aduanas, y aprobado por el Director de Gestión Corporativa, se presenta en el Comité Institucional de Gestión y Desempeño.

4.5.3.3. Monitoreo y revisión de riesgos operacionales, fiscales, ambientales y de integridad

a) Primera Línea de defensa:

- Cuatrimestralmente las Direcciones Seccionales, la Dirección Operativa de Grandes Contribuyentes, y las dependencias de nivel central, con el apoyo de los gestores de riesgos asignados deben informar los resultados del monitoreo de riesgos realizado en las diferentes áreas, para lo cual, deben diligenciar en NOVASEC informando el estado de la ejecución de los controles, materializaciones de riesgos y buenas prácticas realizadas en el periodo. En caso de materialización de riesgos de corrupción deben adjuntar el plan de mejoramiento realizado.

- Con la información registrada en el formulario de NOVASEC, los líderes de los procesos – Nivel Central, con el apoyo del gestor de riesgos asignado por proceso deben reportar el seguimiento consolidado en NOVASEC (cantidad de riesgos materializados por proceso, acciones de mejora implementada, buenas prácticas, seguimiento controles e informar si en el periodo se actualizó la matriz), tanto los responsables de los macroprocesos como la Oficina de Control Interno y la Subdirección de Procesos tendrán acceso a esta información para los respectivos análisis.

  Para el Informe monitoreo de riesgos en NOVASEC, los líderes de los procesos deberán considerar, además de la información asociada al monitoreo realizado por las Direcciones Seccionales, la Dirección Operativa de Grandes Contribuyentes y Nivel central, lo siguiente:

- Los resultados de las autoevaluaciones, seguimientos independientes, auditorias de calidad, auditorias de entes externos de control y el informe del estado de implementación de las acciones de mejora.

  El informe del monitoreo de los riesgos debe hacerse de manera cuatrimestral, así:
  Primeros diez (10) días calendario del mes de mayo para el cuatrimestre enero – abril.
  Primeros diez (10) días calendario del mes de septiembre para el cuatrimestre mayo – agosto.
  Primeros quince (15) días calendario del mes de enero para el cuatrimestre septiembre – diciembre

b) Segunda Línea de defensa:

- A partir del reporte cuatrimestral realizado por los líderes de los procesos en NOVASEC, la Subdirección de Procesos - Coordinación de Procesos y Riesgos Operacionales, debe elaborar el informe consolidado. Una vez revisado y aprobado por el Subdirector de Procesos, el informe es remitido por correo electrónico a los responsables de los procesos, directores seccionales,

director operativo y al Director de Gestión Estratégica y de Analítica, así mismo, se presenta en el Comité Institucional de Gestión y Desempeño.

4.6. Comunicación y socialización

Los responsables de los procesos deben asegurar la divulgación y socialización de la gestión de riesgos a todos los niveles de operación, según aplique.

5. CONTROL DE CAMBIOS

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	12/06/2025		Versión Inicial. La Cartilla de Gestión de Riesgos reemplaza el instructivo IN-PEC-0201 Gestión de Riesgos, e incluye los lineamientos metodológicos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 6 – Departamento Administrativo de la Función Pública DAFP.	Pública

Elaboró	Maribel Verano Palencia Jhon Ferney Abril Jiménez **Elaboración técnica**	Gestor II Gestor III	Coordinación de Procesos y Riesgos Operacionales
	Carlos Anibal Parra Rodríguez Angela Johanna Marquez Mora **Elaboración técnica**	Inspector I Inspector I	Subdirección Planeación y Cumplimiento
	María Ismenia Sosa Ávila Miryam Esther Hernández Rodríguez Miryam Fernanda Cuenca Rodríguez **Elaboración técnica**	Inspector III Inspector III Gestor III	Dirección de Gestión Corporativa
	Maribel Verano Palencia Jhon Ferney Abril Jiménez **Elaboración metodológica**	Gestor II Gestor III	Coordinación de Procesos y Riesgos Operacionales

Revisó:	Héctor Edilson Hortua Baquero	Jefe	Coordinación de Procesos y Riesgos Operacionales
	Jhonn Lenin Bautista Guzmán	Subdirector (A)	Subdirección Planeación y Cumplimiento
	Pedro José Arrieta Melendrez	Director	Dirección de Gestión Corporativa
Aprobó:	Iván Mauricio Quintero Sosa	Subdirector (A)	Subdirección de Procesos

6. ANEXOS

Anexo 1. Responsables metodológicos por tipo de riesgos

Tabla 13. Responsables metodológicos por tipo de riesgo

Tipo de riesgo	Responsable
Riesgos estratégicos.	Subdirección de Planeación y Cumplimiento.
Riesgos operacionales, ambientales, de integridad y riesgos fiscales.	Subdirección de Procesos.
Riesgos de seguridad de la información, incluyen riesgos de ciberseguridad y protección de datos personales.	Oficina de Seguridad de la Información.
Riesgos de Capital humano.	Dirección de Gestión Corporativa.
Riesgos de seguridad y salud en el trabajo.	Subdirección de Desarrollo de Talento Humano.
Riesgos de Cumplimiento TAC	Subdirección de Análisis de Riesgo y Programas
Riesgos de lavado de activos, financiación del terrorismo y financiación para la proliferación de armas de destrucción masiva – LAFT/FPADM.	Subdirección de Apoyo en la Lucha contra el Delito Aduanero y Fiscal