DIRECCIONAMIENTO ESTRATÉGICO Y PLANEACIÓN

GUÍA PARA LA ADMINISTRACIÓN DE RIESGOS

JULIO DE 2024

CONTENIDO

1. INTRODUCCIÓN 7
2. OBJETIVO 7
3. ALCANCE 7
4. RESPONSABLE 7
5. DEFINICIONES 8
6. MARCO NORMATIVO 14
7. GENERALIDADES 15
8. CONTENIDO 15
8.1. LINEAMIENTOS GENERALES DE LA ADMINISTRACIÓN DE RIESGOS 15
8.1.1. Lineamientos de la Política de Administración del Riesgo 18
8.2. ANÁLISIS DEL CONTEXTO INSTITUCIONAL 20
8.2.1. Análisis de los Objetivos Estratégicos y de Proceso 20
8.2.2. Identificación de los Puntos de Riesgo 21
8.3. RIESGOS DE GESTIÓN 21
8.3.1. Identificación del Riesgo 21
8.3.1.1. Identificación de Áreas de Impacto 22
8.3.1.2. Identificación de Áreas de Factores de Riesgo 22
8.3.1.3. Descripción del Riesgo 23
8.3.1.4. Premisas para una adecuada redacción de Riesgo 25
8.3.1.5. Clasificación del Riesgo 26
8.3.2. Valoración del Riesgo 27
8.3.2.1. Determinar la Probabilidad de ocurrencia del Riesgo 28
8.3.2.2. Determinar el Impacto del Riesgo 30
8.3.2.3. Evaluación del Riesgo 32
8.3.3. Valoración de Controles 33
8.3.3.1. Estructura para la descripción del Control 33
8.3.3.2. Tipología de Controles 35
8.3.3.3. Análisis y Evaluación de los Controles – Atributos 36
8.3.3.4. Nivel de Riesgo - Riesgo Residual 40
8.3.4. Estrategias para combatir el Riesgo 44
8.3.5. Gestión de Eventos 45
8.3.6. Indicadores Clave de Riesgo 46
8.3.7. Monitoreo y Revisión 47
8.4. RIESGOS FISCALES 50

8.4.1. Control Fiscal Interno y Prevención del Riesgo Fiscal 50
8.4.2. Definición y Elementos del Riesgo Fiscal 51
8.4.3. Metodología y paso a paso para el levantamiento del Mapa de Riesgos Fiscales 52
8.4.3.1. Identificación de Riesgos Fiscales 52
8.4.3.2. Identificación de Áreas de Impacto 54
8.4.3.3. Identificación de la causa raíz o potencial hecho generador 54
8.4.4. Descripción del Riesgo Fiscal 55
8.4.5. Valoración del Riesgo 57
8.4.5.1. Determinar la Probabilidad 57
8.4.5.2. Determinar el Impacto del Riesgo 58
8.4.5.3. Evaluación del Riesgo 59
8.4.6. Valoración de Controles 63
8.4.7. Nivel de Riesgo - Riesgo Residual 69
8.4.8. Plan de Acción 70
8.5. RIESGOS DE CORRUPCIÓN 70
8.5.1. Definición de Riesgo de Corrupción 70
8.5.2. Valoración de Riesgos 71
8.5.2.1. Cálculo de la Probabilidad e Impacto 71
8.5.2.2. Análisis de Impacto 72
8.5.2.3. Análisis del Impacto en Riesgos de Corrupción 74
8.5.2.4. Diseño de Controles 74
8.5.2.5. Valoración de los Controles 75
8.5.2.6. Tratamiento del Riesgo 77
8.5.3. Monitoreo de Riesgos de Corrupción 78
8.5.4. Seguimiento de Riesgos de Corrupción 78
8.5.4.1. Seguimiento 78
8.5.4.2. Acciones para seguir en caso de materialización de Riesgos de Corrupción 79
8.6. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 79
8.6.1.1. Identificación de los Activos de Seguridad de la Información 79
8.6.1.2. Identificación del Riesgo 81
8.6.1.3. Descripción del Riesgo 83
8.6.1.4. Identificación de Amenazas 84
8.6.1.5. Vulnerabilidad del Riesgo de Seguridad de la Información 85
8.6.2. Valoración del Riesgo 85
8.6.3. Controles asociados a la Seguridad de la Información 87

8.6.4. Valoración de los Controles 89
8.6.5. Plan de Acción 89
8.7. IDENTIFICACIÓN Y PRIORIZACIÓN DE OPORTUNIDADES 89
8.7.1. Consecutivo 89
8.7.2. Oportunidad 89
8.7.3. Factor de Incidencia 90
8.7.4. Tratamiento de Oportunidades 91
8.8. SEGUIMIENTO A RIESGOS 91
8.9. SEGUIMIENTO A OPORTUNIDADES 94
9. ANEXOS 95
10. REFERENCIAS BIBLIOGRÁFICAS 95
11. HISTORIA DE MODIFICACIONES 95
12. CONTROL DE CAMBIOS 95

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Operatividad Institucional para la Administración del Riesgo 16
Ilustración 2. Metodología para la Administración del Riesgo 17
Ilustración 3. Estructuración Política de Administración de Riesgos 18
Ilustración 4. Análisis de Objetivos 20
Ilustración 5. Cadena de Valor 21
Ilustración 6. Estructura propuesta para la redacción del Riesgo 24
Ilustración 7. Ejemplo descripción del Riesgo 25
Ilustración 8. Relación ente Factores de Riesgo y Clasificación del Riesgo 27
Ilustración 9. Estructura para el desarrollo de la Valoración del Riesgo 28
Ilustración 10. Actividades relacionadas con la Gestión en Entidades Públicas 29
Ilustración 11. Criterios para definir el Nivel de Probabilidad 29
Ilustración 12. Criterios para definir el nivel de impacto 30
Ilustración 13. Resultados Ejemplo Tabla de Probabilidad e Impacto 31
Ilustración 14. Matriz de Calor - Niveles de Severidad del Riesgo 32
Ilustración 15. Resultados ejemplo Matriz de Calor 33
Ilustración 16. Ejemplo aplicado bajo la estructura propuesta para la redacción del Control 34
Ilustración 17. Ciclo de Procesos y Tipología de Controles 35
Ilustración 18. Movimiento en la Matriz de Calor de acorde con el Tipo de Control 37
Ilustración 19. Movimiento en la Matriz de Calor con el ejemplo propuesto 41
Ilustración 20. Estrategias para combatir el Riesgo 45
Ilustración 21. Indicadores Clave de Riesgo 47
Ilustración 22. Operatividad esquema Líneas de Defensa 50
Ilustración 23. Articulación Modelo Constitucional Control Fiscal y Sistema de Control Interno 51
Ilustración 24. Estructura propuesta para la redacción de Riesgos Fiscales 55
Ilustración 25. Redacción de Riesgos Fiscales 56
Ilustración 26. Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso 57
Ilustración 27. Criterios para definir el Nivel de Probabilidad 58
Ilustración 28. Criterios para definir el nivel de impacto 59
Ilustración 29. Matriz de Calor - Niveles de Severidad del Riesgo 60
Ilustración 30. Selección Probabilidad Riesgo Fiscal 61
Ilustración 31. Selección Impacto Riesgo Fiscal 62
Ilustración 32. Zona de Severidad del Riesgo Fiscal 62
Ilustración 33. Aplicación de los Controles definidos 69
Ilustración 34. Zona de Riesgo respecto al ejemplo 70
Ilustración 35. Definición Riesgo de Corrupción 71
Ilustración 36. Mapa de Calor 74
Ilustración 37. Pasos para diseñar un Control 75
Ilustración 38. Peso o participación de cada variable en el diseño del Control 76
Ilustración 39. Tratamiento del Riesgo 77
Ilustración 40. Conceptualización Activos de Información 79
Ilustración 41. Conceptualización de los Activos 80
Ilustración 42. Pasos para la identificación de Activos 80
Ilustración 43. Ejemplo de identificación de Activos del proceso 80
Ilustración 44. Ejemplo redacción de Riesgos de Seguridad de la Información 83
Ilustración 45. Niveles de Probabilidad 85
Ilustración 46. Determinación del Impacto 86
Ilustración 47. Matriz de Calor 87
Ilustración 48. Ejemplos de controles de Seguridad de la Información 88

ÍNDICE DE TABLAS

Tabla 1. Marco General para la definición de actividades propias de cada Línea de Defensa 19
Tabla 2. Factores de Riesgo 22
Tabla 3. Elementos estructura de descripción del Riesgo 24
Tabla 4. Descripción de Premisas 25
Tabla 5. Clasificación de Riesgos 26
Tabla 6. Estructura para la descripción del Control 34
Tabla 7. Atributos de para el diseño del Control 36
Tabla 8. Información para el Desarrollo del Ejemplo 38
Tabla 9. Aplicación tabla atributos a ejemplo propuesto 39
Tabla 10. Estructura del Control 40
Tabla 11. Aplicación de Controles para establecer el Riesgo Residual 40
Tabla 12. Ejemplo de Mapa de Riesgos acorde con el ejemplo propuesto 42
Tabla 13. Valoración del Riesgo 43
Tabla 14. Plan de Acción 44
Tabla 15. Componentes Estructura MECI 48
Tabla 16. Líneas de Defensa 49
Tabla 17. Elementos del Riesgo Fiscal 51
Tabla 18. Preguntas orientadoras para puntos Riesgo Fiscal y Causas Inmediatas 52
Tabla 19. Valoración de Controles de Riesgo Fiscal 64
Tabla 20. Catálogo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas 65
Tabla 21. Criterios para calificar la Probabilidad 71
Tabla 22. Criterios para calificar el Impacto en Riesgos de Corrupción 72
Tabla 23. Seguimientos Matriz de Riesgos de Corrupción 78
Tabla 24. Vulnerabilidades Riesgo de Seguridad de la Información 81
Tabla 25. Riesgo de Seguridad de la Información 84
Tabla 26. Factores de Incidencia - Factibilidad 90
Tabla 27. Factores de Incidencia - Impacto 90
Tabla 28. Factores de Evaluación de Riesgos y Controles 92
Tabla 29. Factores de Evaluación de Oportunidades 94

1. INTRODUCCIÓN

La administración de riesgos es una práctica esencial para garantizar la resiliencia y la capacidad de adaptación de las entidades públicas a los cambios y desafíos del entorno. Al implementar un enfoque sistemático y estructurado para la gestión de riesgos, las entidades públicas pueden reducir la incertidumbre y mejorar su capacidad para tomar decisiones informadas y estratégicas.

Esta guía tiene como objetivo proporcionar una herramienta práctica y útil para la gestión y administración efectiva de los riesgos en el Instituto Superior de Educación Rural - ISER. La administración de riesgos es un proceso esencial que ayuda a las entidades públicas a identificar, evaluar y mitigar los riesgos potenciales que puedan afectar su capacidad para cumplir sus objetivos y metas estratégicas.

Esta guía proporcionará una descripción detallada del proceso de Administración de Riesgos, desde la identificación hasta la evaluación y mitigación de los riesgos. También se discutirán los roles y responsabilidades de los diferentes actores involucrados en el proceso de administración de riesgos, así como las mejores prácticas y herramientas disponibles para implementar una gestión efectiva de riesgos en su entidad pública.

2. OBJETIVO

Establecer los lineamientos metodológicos para llevar a cabo la identificación, análisis, evaluación y tratamiento de riesgos por procesos para la generación de la Matriz de Riesgos y Oportunidades del Instituto Superior de Educación Rural - ISER.

3. ALCANCE

La administración del riesgo aplica para todos los procesos del Sistema de Gestión de la Calidad que operan en el Instituto Superior de Educación Rural - ISER. Inicia con la identificación de los riesgos y termina con su monitoreo y seguimiento, con el fin de evidenciar el cumplimiento de las acciones planteadas.

4. RESPONSABLE

La Alta Dirección, en el marco del Comité Institucional de Coordinación de Control Interno, debe asegurar el cumplimiento de las disposiciones descritas en la Política de Administración de Riesgos, realizar seguimiento a los riesgos críticos haciendo uso de la información suministrada por parte del Profesional Especializado adscrito al proceso de Control Interno de Gestión, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.

Los Líderes de Proceso son responsables frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo.

El Profesional Especializado adscrito al proceso de Direccionamiento Estratégico y Planeación debe, periódicamente, realizar seguimiento a los riesgos identificados, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de tal manera que los Líderes de Proceso puedan establecer mejoras en los riesgos y controles, así como garantizar su aplicación

efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento de manera permanente.

El Profesional Especializado adscrito al proceso de Control Interno de Gestión, a través de sus acciones de seguimiento y evaluación, debe determinar la eficacia de los controles que permitan evitar la materialización de estos.

5. DEFINICIONES

5.1. ACCIÓN: Se determina mediante verbos que indican la operación que deben realizar como parte del control.

5.2. ACTIVIDADES DE CONTROL: Su propósito es permitir el control de los riesgos identificados y como mecanismo para apalancar el logro de los objetivos y forma parte integral de los procesos

5.3. ACTIVIDADES DE MONITOREO: Su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública

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

5.5. AMBIENTE DE CONTROL: este componente busca asegurar un ambiente de control que le permita a la entidad disponer de las condiciones mínimas para el ejercicio del control interno. Requiere del compromiso, el liderazgo y los lineamientos de la alta dirección y del Comité Institucional de Coordinación de Control Interno.

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

5.7. 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.

5.8. BIEN PÚBLICO: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

- ✓ **Bien de uso público:** Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques, etc.

- ✓ **Bienes fiscales:** Aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

5.9. CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

5.10. CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

5.11. CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

NOTA: Tratándose de Riesgo Fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

5.12. CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

5.13. CAUSA RAÍZ - CAUSA EFICIENTE O CAUSA ADECUADA: Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

5.14. COMPLEMENTO: Corresponde a los detalles que permiten identificar claramente el objeto del control.

5.15. CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

5.16. 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.

NOTA: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

5.17. CONTROL: Medida que permite reducir o mitigar un riesgo.

5.18. CONTROL AUTOMÁTICO: Controles ejecutados por un sistema de información.

5.19. CONTROL CORRECTIVO: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

5.20. CONTROL DETECTIVO: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

5.21. CONTROL FISCAL INTERNO - CFI: Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público.

5.22. CONTROL FISCAL MULTINIVEL: Es la articulación entre el Sistema de Control Interno (primer nivel de control) y el Control Externo (segundo nivel de control), con la participación del control social.

5.23. CONTROL MANUAL: Controles que son ejecutados por personas.

5.24. 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.

5.25. 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.

5.26. DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.

5.27. EFECTO: Es el 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.

5.28. EJECUCIÓN Y ADMINISTRACIÓN DE PROCESOS: Pérdidas derivadas de errores en la ejecución y administración de procesos.

5.29. EVALUACIÓN DEL RIESGO: Su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales.

5.30. EVENTO POTENCIAL: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona 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. En esta guía, el evento potencial es equivalente a la causa raíz

5.31. FACTORES DE RIESGO: Término que se refiere a las fuentes generadoras de riesgos.

5.32. FALLAS TECNOLÓGICAS: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.

5.33. FRAUDE EXTERNO: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

5.34. 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.

5.35. GESTIÓN DEL RIESGO FISCAL: Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales.

5.36. GESTOR FISCAL: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas

y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

5.37. GESTOR PÚBLICO: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

5.38. IDENTIFICACIÓN DEL RIESGO: Proceso que determina que puede suceder, por qué y el cómo.

5.39. IMPACTO: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

5.40. INFORMACIÓN Y COMUNICACIÓN: Tiene como propósito utilizar la información de manera adecuada y comunicarla por los medios y en los tiempos oportunos. Para su desarrollo se deben diseñar políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos dentro y en el entorno de cada entidad, que satisfagan la necesidad de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de la entidad y de cada proceso sea adecuada a las necesidades específicas de los grupos de valor y grupos de interés.

5.41. INTEGRIDAD: Propiedad de exactitud y completitud.

5.42. INTERESES PATRIMONIALES DE NATURALEZA PÚBLICA: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

5.43. LÍNEA ESTRATÉGICA DE DEFENSA: Está conformada por la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta línea de defensa se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.

5.44. MODELO DE OPERACIÓN POR PROCESOS: Es el estándar organizacional que soporta la operación de la entidad pública, integrando las competencias constitucionales y legales que la rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos institucionales.

5.45. 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 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.

5.46. OPORTUNIDAD: Aquella acción para minimizar un efecto negativo, que no sólo minimiza el efecto, sino que ayuda a que se logre de forma más eficaz algún resultado previsto.

5.47. PATRIMONIO PÚBLICO: Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

5.48. PRIMERA LÍNEA DE DEFENSA: Esta línea de defensa les corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad. Se debe precisar que cuando se trate de servidores que ostenten un cargo de responsabilidad (jefe) dentro de la estructura organizacional, se denominan controles de gerencia operativa, ya que son aplicados por líderes o responsables de proceso. Esta línea se encarga del mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos.

5.49. PROBABILIDAD: Se entiende 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 1 año.

5.50. PUNTO DE RIESGO: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.

5.51. RECURSO PÚBLICO: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

5.52. 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.

5.53. 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.

5.54. RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

NOTA: 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.

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

5.56. RIESGO DE GESTIÓN: Posibilidad de que suceda algún evento que tendrá un impacto sobre cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

5.57. 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.

5.58. 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.

5.59. RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, lo que nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

5.60. RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.

5.61. SEGUNDA LÍNEA DE DEFENSA: Esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

5.62. TERCERA LÍNEA DE DEFENSA: Esta línea de defensa está conformada por la Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos o inadecuadamente cubiertos por la 2ª línea de defensa.

5.63. TOLERANCIA AL 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.

5.64. 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.

5.65. VALORACIÓN DEL RIESGO: Es el conjunto de procesos que permiten analizar y evaluar el riesgo.

5.66. VULNERABILIDAD: Representan la debilidad de un activo o un control que puede ser explotada por una o más amenazas.

6. MARCO NORMATIVO

6.1. Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno de las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

6.2. Ley 610 del 2000, por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.

6.3. Ley 1273 de 2009 - Ley de Delitos Informáticos, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

6.4. 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 gestión pública.

6.5. Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

6.6. Decreto 1499 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.

6.7. Acto Legislativo 04 de 2019, se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

6.8. Decreto 403, 2020, por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.

6.9. Acuerdo 021 de 2021, por medio de la cual se actualiza el Comité Institucional de Coordinación de Control Interno del Instituto Superior de Educación Rural - ISER.

6.10. Acuerdo 022 de 2021, por el cual se deroga el Acuerdo No. 018 del 21 de noviembre de 2019 y se establece la Política para la Administración de Riesgos en el Instituto Superior de Educación Rural - ISER.

6.11. Resolución 201 del 04 de marzo 2024, por la cual se emiten los lineamientos frente a la implementación del modelo integrado de planeación y gestión – MIPG del Instituto Superior de Educación Rural - ISER y se dictan otras disposiciones.

7. GENERALIDADES

7.1. La Matriz de Riesgos y Oportunidades debe ser construida con el apoyo de los Líderes de Proceso definidos por el Instituto Superior de Educación Rural – ISER.

7.2. La Matriz de Riesgos y Oportunidades se debe actualizar anualmente en conjunto con el Plan Anticorrupción y de Atención al Ciudadano y su publicación debe realizarse a más tardar el 31 de enero de cada vigencia.

7.3. Las actualizaciones requeridas a la Matriz de Riesgos y Oportunidades deben ser tramitadas por parte de los Líderes de Proceso ante el proceso de Direccionamiento Estratégico y Planeación, quién debe validar su pertinencia y aprobación.

7.4. Es responsabilidad del proceso de Direccionamiento Estratégico y Planeación mantener actualizada la Matriz de Riesgos y Oportunidades Institucional y gestionar su publicación oportuna en la página web institucional www.iser.edu.co.

7.5. Los Líderes de Proceso deben monitorear permanentemente la Matriz de Riesgos y Oportunidades y ejecutar los controles establecidos para evitar su materialización.

7.6. El seguimiento a la Matriz de Riesgos y Oportunidades se debe adelantar con una frecuencia cuatrimestral, seguimiento que debe ser coordinado por el proceso de Control Interno de Gestión.

7.7. Para el seguimiento adelantado por parte del proceso de Control Interno de Gestión, este debe definir el método que permita valorar la eficacia de los controles asociados a los Riesgos.

7.8. Se deben generar planes de mejora sobre la Matriz de Riesgos y Oportunidades, los cuales deben ser formulados por parte de los Líderes de Proceso conforme a los lineamientos definidos en el procedimiento **P-CIG-02 Gestión de Planes de Mejoramiento** y, en los siguientes casos:

- ✓ Seguimientos a la Matriz de Riesgos y Oportunidades
- ✓ Materialización de Riesgos
- ✓ Resultados de Auditorías

7.9. Los Planes de Mejoramiento resultantes deben ser radicados ante el proceso de Control Interno de Gestión y deben ser comunicados al proceso de Direccionamiento Estratégico y Planeación.

8. CONTENIDO

8.1. LINEAMIENTOS GENERALES DE LA ADMINISTRACIÓN DE RIESGOS

El Modelo Integrado de Planeación y Gestión – MIPG, define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a

través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

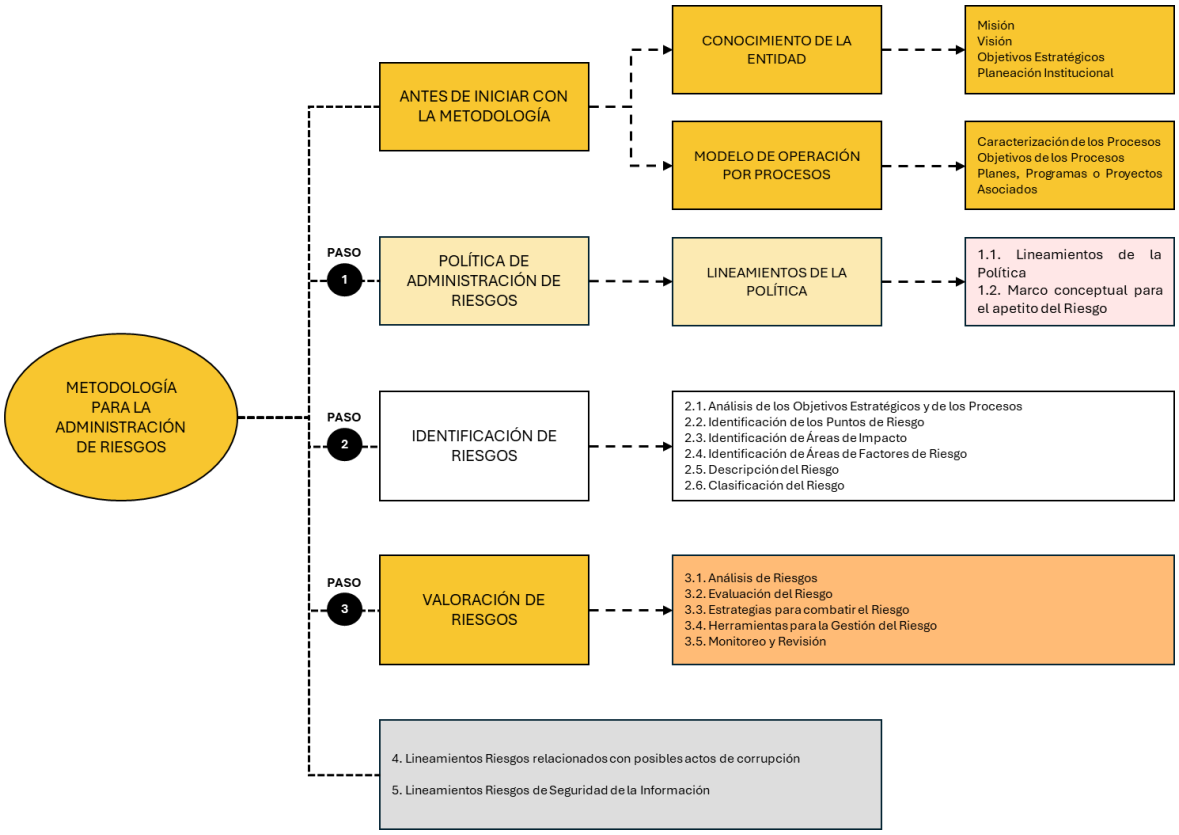
Ilustración 1.

Operatividad Institucional para la Administración del Riesgo

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6

Teniendo en cuenta la Metodología para la Administración del Riesgo recomendada por el Departamento Administrativo de la Función Pública - DAFP en su Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 6, de noviembre 2022, para el Instituto Superior de Educación Rural - ISER se definen las siguientes etapas para la Administración del Riesgo:

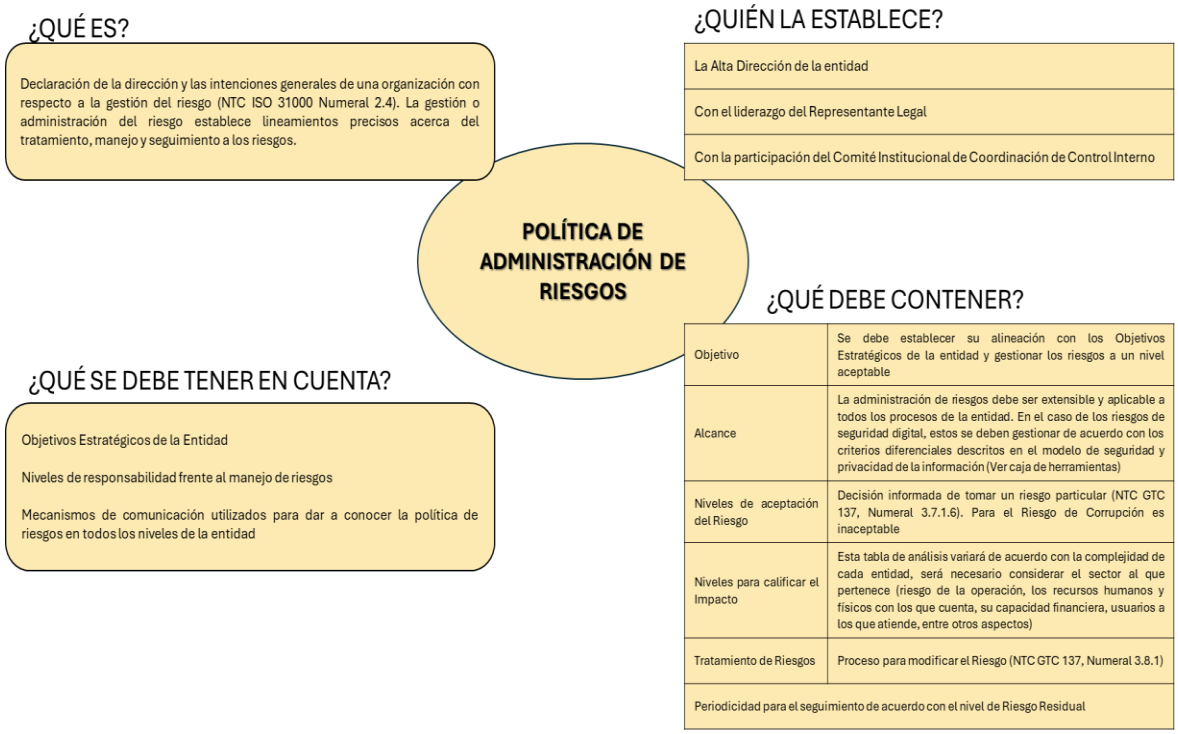
Ilustración 2.
Metodología para la Administración del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Así mismo, con el propósito de establecer la Política Institucional de Administración de Riesgos, el Instituto Superior de Educación Rural- ISER, ha contemplado los lineamientos para su definición conforme lo expresa la Guía de Administración del Riesgo versión 6, los cuales indican:

Ilustración 3.
Estructuración Política de Administración de Riesgos



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

En este sentido, el Instituto Superior de Educación Rural - ISER, se compromete a gestionar los Riesgos de Gestión, Corrupción, Fiscal y de Seguridad de la Información, monitorearlos y realizar seguimiento cuatrimestral, identificando y administrando los eventos potenciales que pueden afectar los objetivos y procesos propios del Instituto.

8.1.1. Lineamientos de la Política de Administración del Riesgo

- ✓ La Administración del Riesgo en el Instituto Superior de Educación Rural - ISER es una herramienta estratégica aplicada en la toma de decisiones de todos sus procesos, proyectos y planes institucionales.
- ✓ Los procesos de Direccionamiento Estratégico y Planeación y Control Interno de Gestión deben articular acciones de impulso que fomente la cultura de Administración del Riesgo, la cual debe estar integrada al Modelo Integrado de Planeación y Gestión - MIPG, el Modelo Estándar de Control Interno – MECI, el Modelo de Seguridad y Privacidad de la Información y las estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano.
- ✓ Los resultados de la identificación de los Riesgos, su valoración, la aplicación y evaluación de los controles, los planes de tratamiento formulados, las acciones de atención, casos de materialización y los Riesgos Residuales deben ser reconocidos y aceptados por cada uno de los propietarios de los Riesgos y debe ser específico para cada tipo de Riesgo (Corrupción, Gestión, Fiscal y Seguridad de la Información).

- ✓ Para el tratamiento del Riesgo, el Instituto debe ejecutar acciones para evitar, reducir, transferir o asumir el riesgo calificado como amenaza; para el caso de las Oportunidades se deben promover las acciones necesarias que permitan incrementar el desempeño y los resultados esperados. Dichas opciones establecen las orientaciones para que los Líderes de Proceso formulen las acciones que conforman el plan de manejo del Riesgo.

Dado que se plantea articular los niveles de autoridad y responsabilidad en el marco del esquema de líneas de defensa, a fin de facilitar la estructura para los seguimientos y monitoreos en todos los niveles organizacionales, frente a la Gestión del Riesgo se debe considerar el siguiente marco general para la definición de actividades o acciones propias de cada línea así:

Tabla 1.
Marco General para la definición de actividades propias de cada Línea de Defensa

LÍNEA	DESCRIPCIÓN
Línea Estratégica - Alta Dirección	Debe definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª Línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
1ª Línea de Defensa	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).
2ª Línea de Defensa	El Profesional Especializado adscrito al proceso de Direccionamiento Estratégico y Planeación o quién haga sus veces debe, periódicamente, hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los Mapas de Riesgos, de manera tal que las instancias de 1ª Línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los Líderes de Proceso y sus equipos para la mejora de este tema
3ª Línea de Defensa	Corresponde al proceso de Control Interno de Gestión o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con el proceso de Direccionamiento Estratégico y Planeación o quien haga sus veces.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.2. ANÁLISIS DEL CONTEXTO INSTITUCIONAL

8.2.1. Análisis de los Objetivos Estratégicos y de Proceso

Este paso es muy importante, dado que todos los Riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico y/o del proceso asociado.

Ilustración 4.
Análisis de Objetivos

ANÁLISIS DE OBJETIVOS ESTRATÉGICOS

La entidad debe analizar los Objetivos Estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

Es necesario revisar que los Objetivos Estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).

ANÁLISIS DE LOS OBJETIVOS DEL PROCESO

Los objetivos del proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero, además se debe revisar que los mismos estén alineados con la Misión y Visión, es decir, asegurar que los objetivos de proceso contribuyan a los Objetivos Estratégicos.

A continuación, encontrará un ejemplo de análisis en el proceso de contratación:

La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continúa operación.

IMPORTANTE

Los objetivos deben incluir el "qué", "cómo", "para qué", "cuando", "cuanto".

Si no están bien definidos los objetivos, no se puede continuar con la metodología de gestión del riesgo.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

El Instituto debe analizar los Objetivos Estratégicos plasmados en el Plan de Desarrollo Institucional vigente y valorar su grado de alineación con la Misión y la Visión Institucional, así como su despliegue hacia los objetivos de los procesos. Con el propósito de realizar el análisis de su adecuada formulación, es decir, que los objetivos cuenten con los atributos mínimos, ejercicio que se puede realizar con el uso del análisis FODA, de acuerdo con los lineamientos definidos en el procedimiento **P-DE-02 Planeación Estratégica** y los resultados descritos en el **F-DE-06 Matriz de Contexto Interno y Externo** y **F-DE-07 Matriz Necesidades y Expectativas de las Partes Interesadas**.

Estos insumos son suministrados a los procesos institucionales por parte del proceso de Direccionamiento Estratégico y Planeación, los cuales permiten realizar los análisis requeridos y descritos en este ítem.

Igualmente, es importante, que los objetivos y actividades claves del proceso se pueden extraer de cada una de las Caracterizaciones de Proceso definidas en el Sistema de Gestión de la Calidad del Instituto.

8.2.2. Identificación de los Puntos de Riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo, los cuales deben mantenerse bajo control para asegurar que el proceso cumpla y/o logre su objetivo.

Ilustración 5.
Cadena de Valor

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para este análisis, los Líderes de Proceso deben tener en cuenta los objetivos y actividades claves del proceso contenidos en cada una de las Caracterizaciones de Proceso definidas en el Sistema de Gestión de la Calidad del Instituto.

8.3. RIESGOS DE GESTIÓN

8.3.1. Identificación del Riesgo

Esta etapa tiene como objetivo identificar los Riesgos que estén o no bajo el control del Instituto Superior de Educación Rural - ISER, para ello se debe tener en cuenta el contexto institucional 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. Se aplican las siguientes fases:

8.3.1.1. Identificación de Áreas de 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. Los impactos que aplican son afectación económica (o presupuestal) y/o reputacional.

El Área de Impacto se debe seleccionar de la lista desplegable en la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "*Área de Impacto*".

8.3.1.2. Identificación de Áreas de Factores de Riesgo

Son las fuentes generadoras de Riesgos. Los factores presentados en la siguiente ilustración son una guía, cada entidad puede analizar los que considere de acuerdo con las características propias de cada entidad.

Tabla 2.
Factores de Riesgo

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	Hurtos 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		Derrumbes

	Eventos relacionados con la infraestructura física de la entidad	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

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

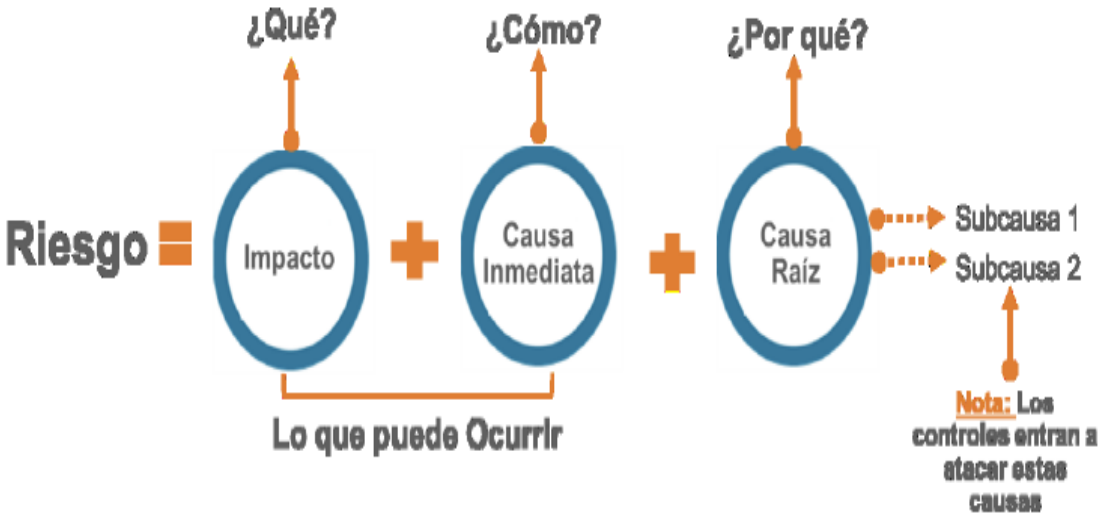
El Área de Factores de Riesgo se debe seleccionar de la lista desplegable en la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "*Área de Factores de Riesgo*".

8.3.1.3. Descripción del Riesgo

La descripción del Riesgo se debe realizar en el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, y seleccionar la opción de la lista desplegable en la columna "*Descripción del Riesgo*".

La descripción del Riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el Líder de Proceso como para personas ajenas a este. Se propone una estructura que facilita su redacción y claridad que inicia con la frase ***POSIBILIDAD DE*** y se analizan los siguientes aspectos:

Ilustración 6.
Estructura propuesta para la redacción del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Desglosando la estructura propuesta tenemos:

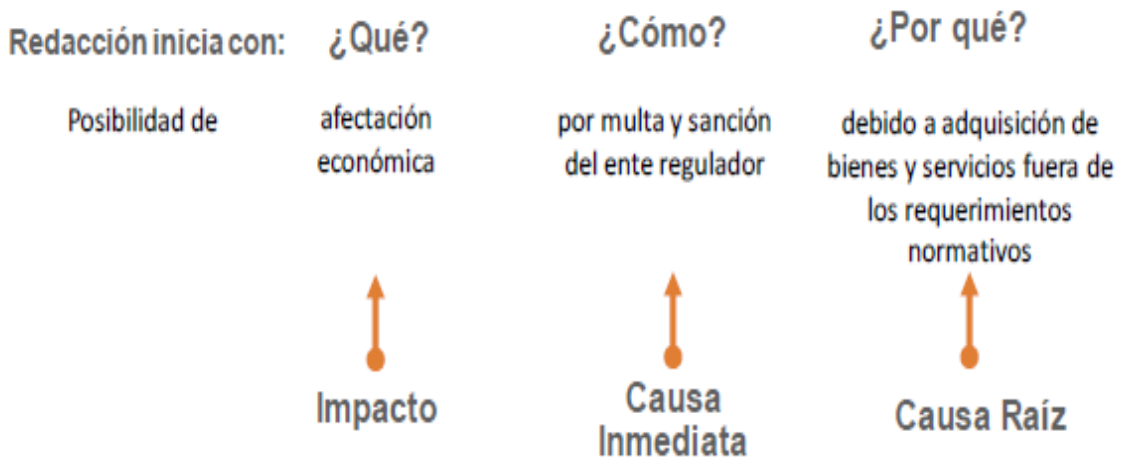
Tabla 3.
Elementos estructura de descripción del Riesgo

ELEMENTO	DESCRIPCIÓN
IMPACTO	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
CAUSA INMEDIATA - CIRCUNSTANCIA INMEDIATA EN RIESGOS FISCALES	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.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

EJEMPLO:

Ilustración 7.
Ejemplo descripción del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.3.1.4. Premisas para una adecuada redacción de Riesgo

Tabla 4.
Descripción de Premisas

PREMISA	EJEMPLO
No describir como Riesgos omisiones ni desviaciones del control	Errores en la liquidación de la nómina por fallas en los procedimientos existentes
No describir causas como Riesgos	Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación
No describir Riesgos como la negación de un control	Retrasos en la prestación del servicio por no contar con digiturno para la atención
No existen Riesgos transversales, lo que pueden existir son causas transversales	Pérdida de expedientes

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.3.1.5. Clasificación del Riesgo

La clasificación de los Riesgos permite agrupar los Riesgos identificados por parte del Instituto Superior de Educación Rural - ISER, los cuales pueden ser clasificados en cada una de las siguientes categorías:

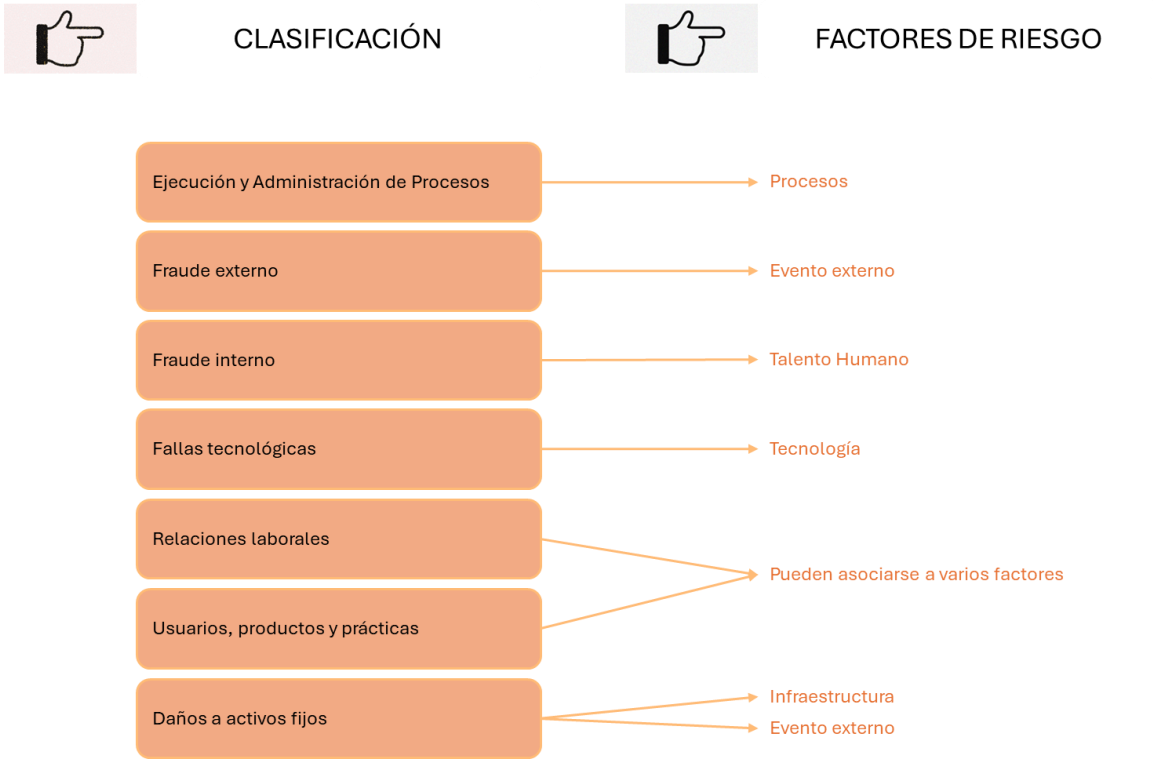
Tabla 5.
Clasificación de Riesgos

CLASIFICACIÓN DE RIESGOS	
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.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Teniendo en cuenta que en la Tabla 2, se definieron una serie de Factores generadores de Riesgo para poder definir la Clasificación de Riesgos, donde su interrelación se muestra a continuación:

Ilustración 8.
Relación ente Factores de Riesgo y Clasificación del Riesgo



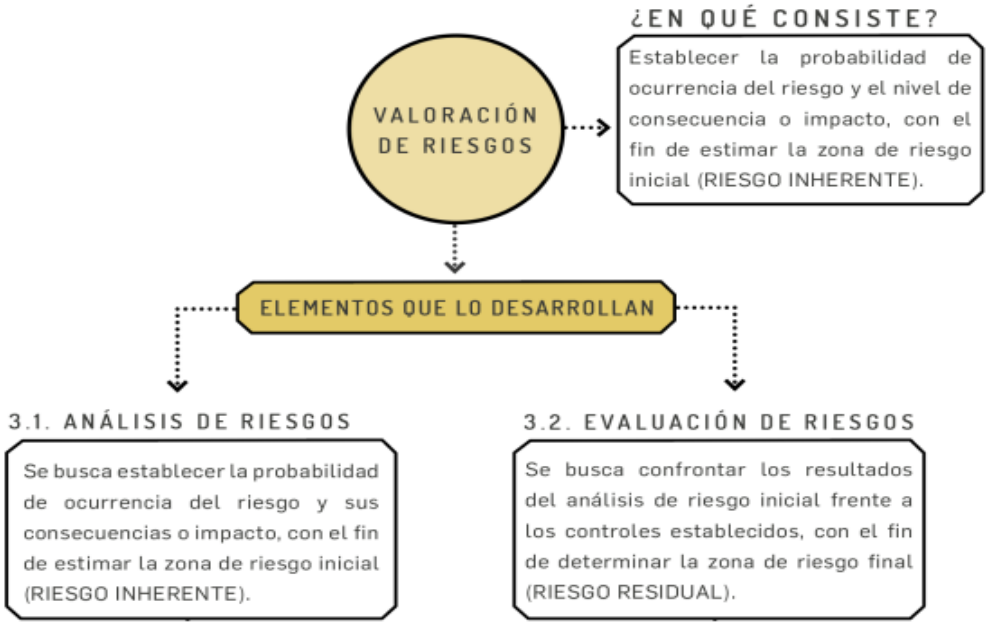
Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

La Clasificación del Riesgo se debe seleccionar en la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "Clasificación del Riesgo".

8.3.2. Valoración del Riesgo

En este punto se busca establecer la Probabilidad de Ocurrencia del Riesgo y sus Consecuencias o Impacto.

Ilustración 9.
Estructura para el desarrollo de la Valoración del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.3.2.1. Determinar la Probabilidad de ocurrencia del Riesgo

Se entiende como la posibilidad de ocurrencia del Riesgo. Para efectos de este análisis, la probabilidad de ocurrencia está asociada a la exposición al Riesgo del proceso o actividad que se esté analizando. De este modo, la Probabilidad Inherente es el número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de Probabilidad:

Ilustración 10.
Actividades relacionadas con la Gestión en Entidades Públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de Probabilidad, la exposición al Riesgo está 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 un (1) año. En la siguiente ilustración se establecen los criterios para definir el nivel de Probabilidad.

Ilustración 11.
Criterios para definir el Nivel de Probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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 y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Una vez cuente con esta información, se debe seleccionar de la lista desplegable definida en la columna denominada "*Frecuencia con la cual se realiza la actividad*" el nivel de *Probabilidad* para cada uno de los Riesgos identificados. La información de *Probabilidad Inherente* y *Porcentaje* se genera automáticamente, de acuerdo con la selección anterior.

8.3.2.2. Determinar el Impacto del Riesgo

Según el impacto económico y/o reputacional y el nivel de probabilidad seleccionada, el Líder de Proceso debe definir el nivel de *Impacto* o consecuencia del Riesgo.

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 seleccionar 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 debe tomar el más alto, en este caso sería el nivel moderado. Bajo este esquema se facilita el análisis para el Líder de Proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis. En la siguiente ilustración se establecen los criterios para definir el nivel de *Impacto*:

Ilustración 12.
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 organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad 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 entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar el Impacto del Riesgo, se debe seleccionar de la lista desplegable definida en la columna denominada "*Criterios de Impacto*" el *Impacto* para cada uno de los Riesgos identificados. La información de *Impacto Inherente* y *Porcentaje* se genera automáticamente, de acuerdo con la selección anterior.

EJEMPLO:

Proceso: Gestión de Recursos

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

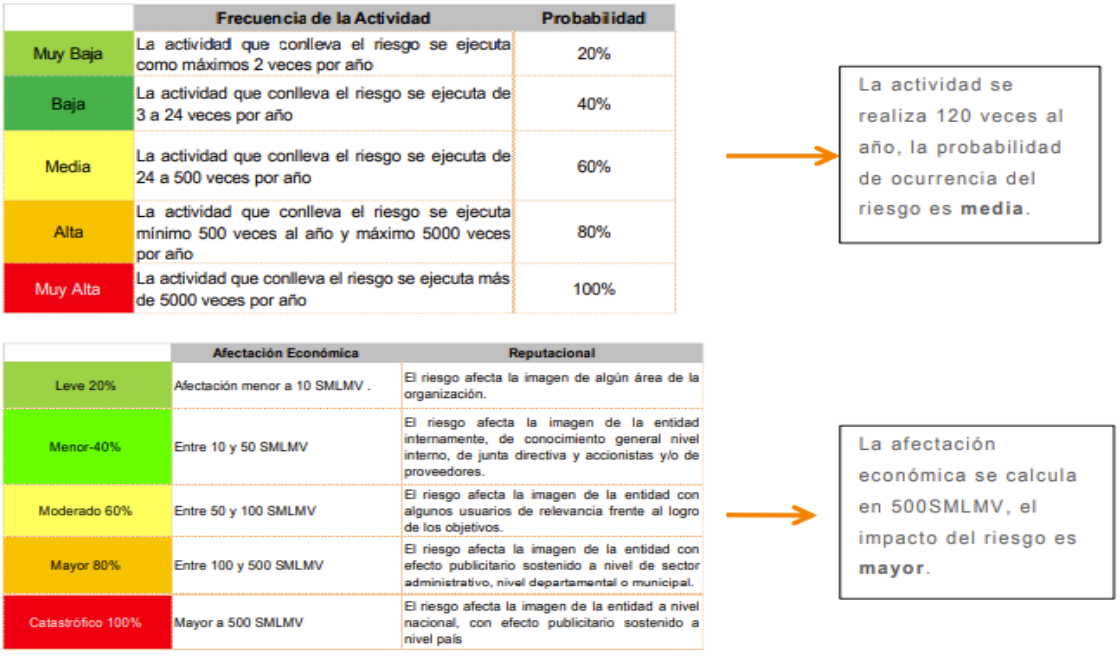
Riesgo Identificado: Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

No. de veces que se ejecuta la actividad: La actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.

Cálculo afectación económica: De llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto tenemos:

Ilustración 13.
Resultados Ejemplo Tabla de Probabilidad e Impacto



	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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 y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad 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 entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Probabilidad Inherente = Media 60**%, Impacto Inherente**: mayor 80%

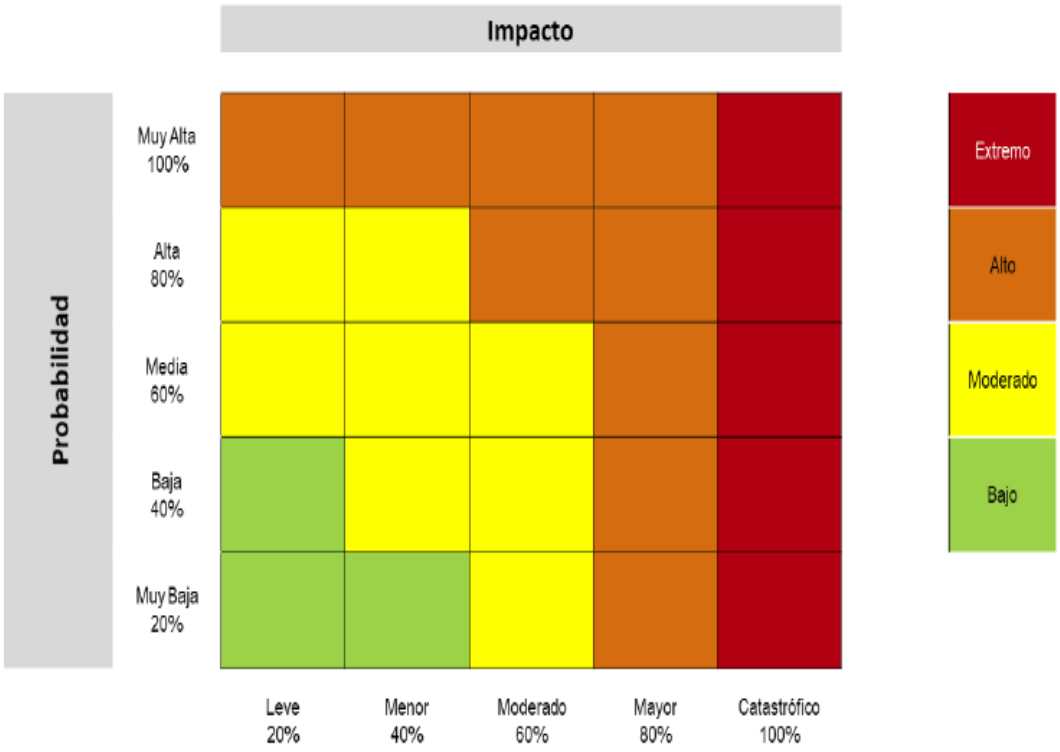
8.3.2.3. Evaluación del Riesgo

A partir del análisis de la Probabilidad de Ocurrencia del Riesgo y sus Consecuencias o Impactos, se busca determinar la Zona de Riesgo Inicial o Riesgo Inherente.

Análisis preliminar - Riesgo Inherente

Este análisis trata de determinar los niveles de severidad a través de la relación entre la probabilidad y el impacto de cada Riesgo identificado. Para este análisis, se definen cuatro (4) zonas de severidad en la matriz de calor:

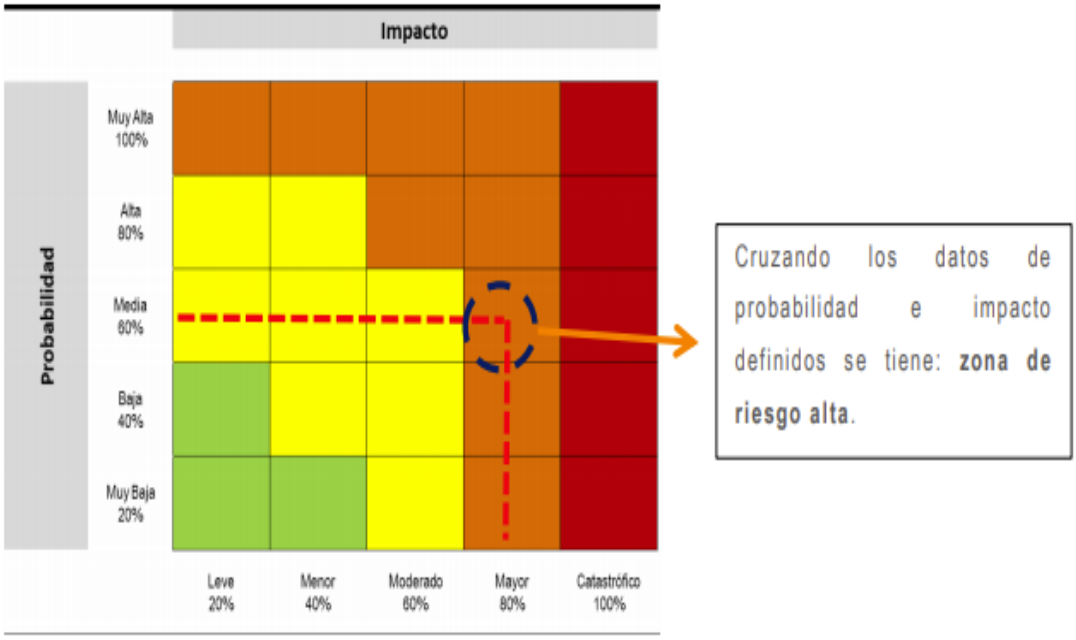
Ilustración 14.
Matriz de Calor - Niveles de Severidad del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

EJEMPLO: Continuando con el ejemplo anterior se había identificado en el proceso de gestión de recursos una Probabilidad inherente = Media 60% y un Impacto inherente: mayor 80%, ubicándolos en el Mapa de Calor se interceptarían en el siguiente punto, dando una zona de riesgo *ALTA*.

Ilustración 15.
Resultados ejemplo Matriz de Calor



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar la Zona de Riesgo Inherente y, de acuerdo con la selección realizada en las comunas "*Frecuencia con la cual se realiza la actividad*" y "*Criterios de Impacto*" para cada uno de los Riesgos identificados, se calcula automáticamente, el valor de Zona de Riesgo Inherente.

8.3.3. Valoración de Controles

En primer lugar, conceptualmente, un Control se define como la medida que permite reducir o mitigar el Riesgo. Para la valoración de controles se debe tener en cuenta:

- ✓ La identificación de controles, la cual se debe realizar a cada Riesgo a través de las entrevistas con los Líderes de Proceso 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.

8.3.3.1. Estructura para la descripción del Control

Para una adecuada redacción del Control se propone una estructura que facilita más adelante entender su tipología y atributos necesarios para su valoración. La estructura se presenta a continuación:

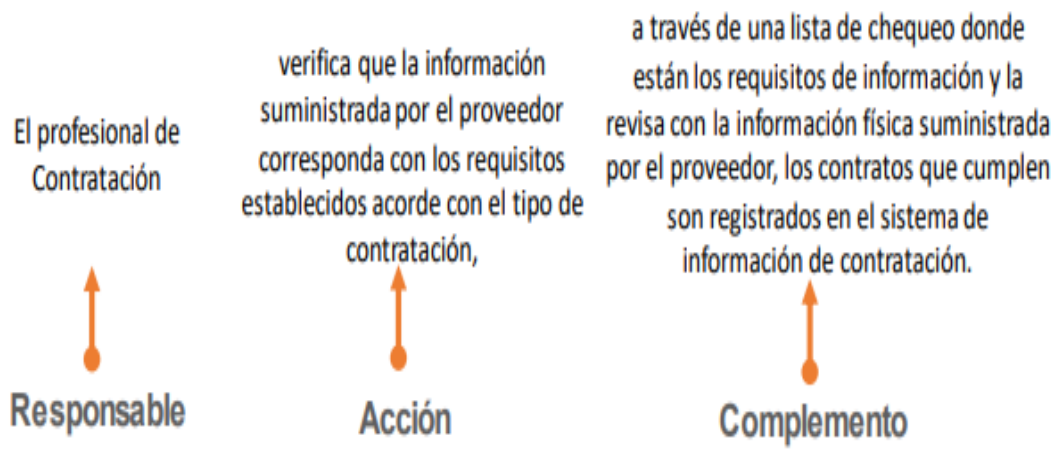
Tabla 6.
Estructura para la descripción del Control

ESTRUCTURA	DESCRIPCIÓN
Responsable de ejecutar el Control	Identificar el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se debe identificar el sistema de información que realiza la actividad.
Acción	Determinar 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.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Ejemplo

Ilustración 16.
Ejemplo aplicado bajo la estructura propuesta para la redacción del Control



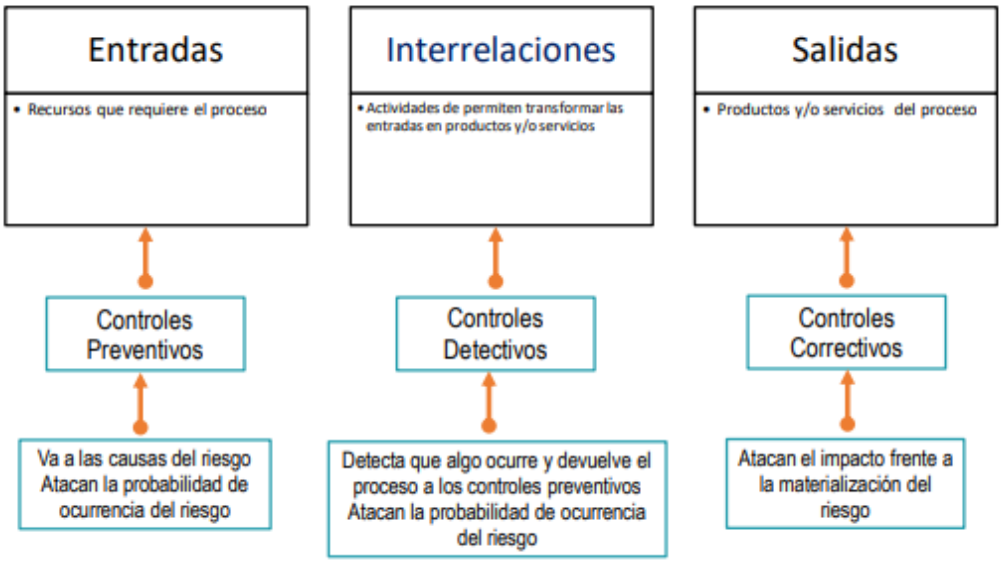
Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

La descripción de los controles asociados a cada Riesgo identificado, deben registrarse en el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "*Descripción del Control*", conforme a la estructura mencionada en este apartado.

8.3.3.2. Tipología de Controles

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. Para comprender esta estructura conceptual, se consideran tres (3) fases globales del ciclo de un proceso así:

Ilustración 17.
Ciclo de Procesos y Tipología de Controles



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Acorde con lo anterior, se definen las siguientes tipologías de controles:

a. **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.

b. **CONTROL DETECTIVO:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

c. **CONTROL CORRECTIVO:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

En el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "*Tipo de Control*", se debe seleccionar el tipo de control definido para el Riesgo identificado.

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

a. **CONTROL MANUAL:** Controles que son ejecutados por el personal del Instituto.

b. **CONTROL AUTOMÁTICO:** Controles que son ejecutados con el apoyo de un sistema de información o aplicación informática.

En el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, en la columna "*Implementación*", se debe seleccionar la forma de ejecución del control definido para el Riesgo identificado.

8.3.3.3. Análisis y Evaluación de los Controles – Atributos

Tabla 7.
Atributos de para el diseño del Control

CARACTERÍSTICAS			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	-

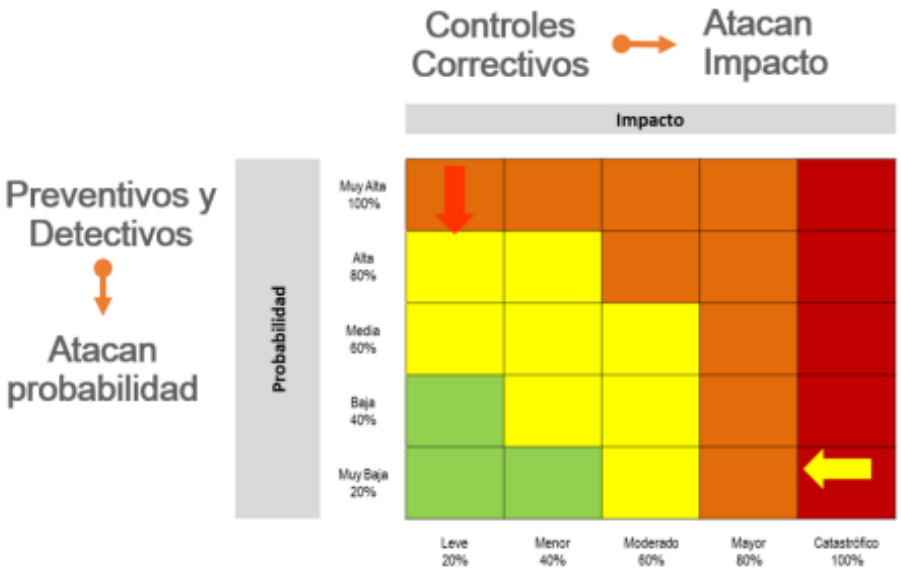
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con Registro	El control deja un registro permite evidencia la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

*** NOTA 1:** 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 siguiente Matriz de Calor 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 18.
Movimiento en la Matriz de Calor de acorde con el Tipo de Control



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Tabla 8.
Información para el Desarrollo del Ejemplo

PROCESO	GESTIÓN DE RECURSOS
Objetivo	Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Riesgo Identificado	Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
Probabilidad Inherente	Moderada 60%
Impacto Inherente	Mayor 80%
Zona de Riesgo	Alta
Controles Identificados	**Control 1**: el profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, 50 los contratos que cumplen son registrados en el sistema de información de contratación.
	Control 2: el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

En la siguiente ilustración se observa los atributos propuestos que apoya como ejemplo para el análisis y valoración de los dos Controles propuestos.

Tabla 9.
Aplicación tabla atributos a ejemplo propuesto

CONTROLES Y SUS CARACTERÍSTICAS				PESO
CONTROL 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		-
		Correctivo		-
	Implementación	Automático		-
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin Registro		-
TOTAL VALORACIÓN CONTROL 1				**40%**
CONTROL 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		-
	Implementación	Automático		-
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin Documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con Registro	X	-
		Sin Registro		-
TOTAL VALORACIÓN CONTROL 1				**30%**

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Tabla 10.
Estructura del Control

ESTRUCTURA DESCRIPCIÓN DEL CONTROL			ATRIBUTOS DE LOS CONTROLES				
RESPONSABLE	ACCIÓN	COMPLEMENTO	TIPO DE CONTROL	IMPLEMENTACIÓN	DOCUMENTACIÓN	FRECUENCIA	EVIDENCIA
Cargo del servidor que ejecuta el control	Lo que se debe realizar como parte del control	Corresponde a los detalles que permiten identificar claramente el objeto del control	Preventivo Detectivo correctivo	Automático o manual	Documentado Sin documentar	Continua aleatoria	Con registro sin registro

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Adicionalmente, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, se deben seleccionar los demás atributos asociados al control identificado en las columnas "*Documentación*", "*Frecuencia*" y "*Evidencia*".

Con la selección de las columnas "*Tipo de Control*" e "*Implementación*", se calcula automáticamente el valor de la columna "", valor que permite realizar el cálculo del Riesgo Residual.

8.3.3.4. Nivel de Riesgo - Riesgo Residual

El 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 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 aplica con el valor resultante luego de la aplicación del primer Control.

Para mayor claridad, en la siguiente ilustración se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Tabla 11.
Aplicación de Controles para establecer el Riesgo Residual

RIESGO	DATOS RELACIONADOS CON LA PROBABILIDAD E IMPACTO INHERENTES	DATOS VALORACIÓN DE CONTROLES	CÁCULOS REQUERIDOS

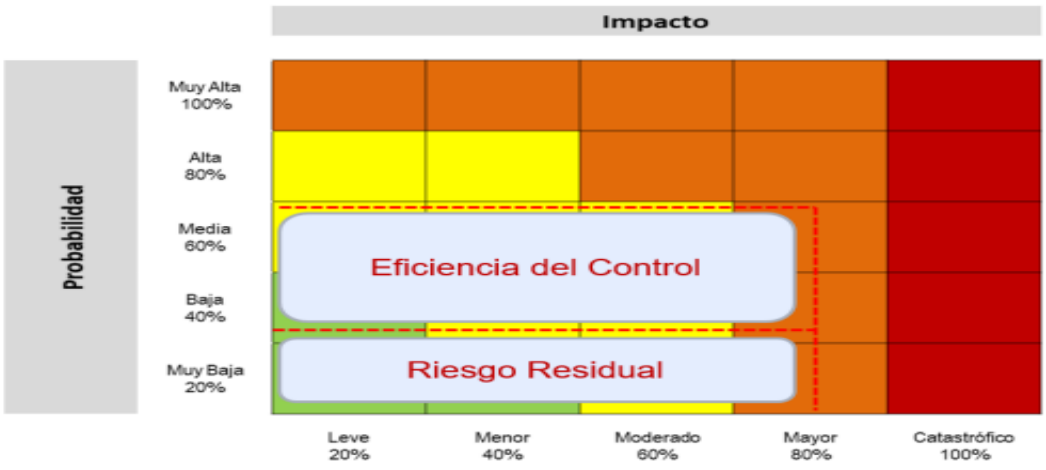
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos	Probabilidad inherente	60%	Valoración Control 1 Preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2o control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25.2%			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para este ejemplo propuesto, si bien el Riesgo se mantiene en zona *ALTA*, se bajó el nivel de probabilidad de ocurrencia del Riesgo.

En la siguiente ilustración, se observa el movimiento en la Matriz de Calor, en función al ejemplo propuesto:

Ilustración 19.
Movimiento en la Matriz de Calor con el ejemplo propuesto



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

NOTA: En caso de no contar con controles correctivos, el Impacto Residual es el mismo calculado inicialmente; es importante señalar que no es posible su movimiento en la matriz para el impacto. A continuación, se puede observar el formato propuesto para el Mapa de Riesgos, este incluye la Matriz de Calor correspondiente:

Tabla 12.
Ejemplo de Mapa de Riesgos acorde con el ejemplo propuesto

PROCESO	Gestión de Recursos
OBJETIVO	Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
ALCANCE	Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas

*Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia	Probabilidad Inherente	%	Impacto Inherente	%	Zona de Riesgo Inherente
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos de contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos	Ejecución y administración de procesos	120	Moderada	60 %	Mayor	80 %	Alta

*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150, pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la oficina asesora de planeación o gerencia de riesgos

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Valoración de Riesgos según los controles definidos acorde al ejemplo.

Tabla 13.
Valoración del Riesgo

No. Control	Descripción del Control	Afectación		Atributos						Probabilidad Residual (2 controles)	Probabilidad Residual final	%	Impacto Residual final	%	Zona de Riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1	El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25.2%	Mayor	80 %	Alta	Reducir
2	El jefe de del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25.2 %	Baja	25.2%				

	del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignados															

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Plan de Acción acorde al ejemplo propuesto:

Tabla 14.
Plan de Acción

Plan de Acción	Responsable	Fecha Implementación	Fecha seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso	Oficina de GTIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

En el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Gestión*, los campos agrupados en "*Evaluación del Riesgo - Nivel del Riesgo Residual*", se calculan de forma automática, de acuerdo con la selección o valoración de cada uno de los controles diseñados y asociados al Riesgo.

8.3.4. Estrategias para combatir el Riesgo

Decisión que se toma frente a un determinado Nivel de Riesgo; dicha decisión puede ser *Aceptar*, *Reducir* o *Evitar*. Se debe analizar frente al *Riesgo Residual*, esto para procesos en funcionamiento; cuando se trate de procesos nuevos, se procede a partir del *Riesgo Inherente*.

Ilustración 20.
Estrategias para combatir el Riesgo

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

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, se debe definir el Plan de Acción, únicamente para las opciones de Reducir – Compartir y Reducir - Mitigar, en el cual especifique:

a. Plan de Acción por desarrollar
b. Responsable,
c. Fecha de inicio y,
d. Fecha de terminación

NOTA: El Plan de Acción acá referido es diferente a un Plan de Contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un Control Correctivo.

8.3.5. Gestión de Eventos

La Gestión de Eventos se define como un Riesgo materializado, donde se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad; se debe contar con una base histórica de eventos (planes de mejora) 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. Algunas fuentes para establecer una base histórica de eventos pueden ser:

- ✓ GLPI
- ✓ PQRSFD
- ✓ Proceso de Gestión Jurídica, principalmente

$$\textbf{\textit{Desempeño del Control}} = \frac{\textbf{\textit{No. de eventos}}}{\textbf{\textit{Frecuencia del Riesgo}}}$$

8.3.6. Indicadores Clave de Riesgo

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados Riesgos. No indica la materialización de los Riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un Riesgo identificado previamente y que es considerado *Alto*, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

Los procesos institucionales pueden identificar Key Risk Indicators de acuerdo con los lineamientos descritos en el procedimiento **P-DE-03 Diseño y Seguimiento de Indicadores**.

En la siguiente ilustración, se puede observar ejemplo de Indicadores Claves de Riesgo:

Ilustración 21.
Indicadores Clave de Riesgo

PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.3.7. Monitoreo y Revisión

El Modelo Integrado de Planeación y Gestión – MIPG, desarrolla en la dimensión 7 el Modelo Estándar de Control Interno - MECI y las Líneas de Defensa como eje articulador para identificar la responsabilidad de la Gestión del Riesgo y Control.

La estructura del MECI busca una alineación a las buenas prácticas de control referenciadas desde el Modelo COSO, razón por la cual la estructura del MECI se fundamenta en cinco componentes.

En la siguiente tabla se relacionan los cinco componentes con su respectiva descripción de acuerdo con lo estipulado en el Manual Operativo MIPG versión 6.

Tabla 15.
Componentes Estructura MECI

COMPONENTES	DESCRIPCIÓN
Ambiente de Control	Este componente busca asegurar un ambiente de control que le permita a la entidad disponer de las condiciones mínimas para el ejercicio del control interno. Requiere del compromiso, el liderazgo y los lineamientos de la alta dirección y del Comité Institucional de Coordinación de Control Interno
Evaluación del Riesgo	Su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales.
Actividades de Control	Su propósito es permitir el control de los riesgos identificados y como mecanismo para apalancar el logro de los objetivos y forma parte integral de los procesos.
Información y Comunicación	Tiene como propósito utilizar la información de manera adecuada y comunicarla por los medios y en los tiempos oportunos. Para su desarrollo se deben diseñar políticas, directrices y mecanismos de consecución, captura, procesamiento y generación de datos dentro y en el entorno de cada entidad, que satisfagan la necesidad de divulgar los resultados, de mostrar mejoras en la gestión administrativa y procurar que la información y la comunicación de la entidad y de cada proceso sea adecuada a las necesidades específicas de los grupos de valor y grupos de interés.
Actividades de Monitoreo	Su propósito es desarrollar las actividades de supervisión continua (controles permanentes) en el día a día de las actividades, así como evaluaciones periódicas (autoevaluación, auditorías) que permiten valorar: (i) la efectividad del control interno de la entidad pública; (ii) la eficiencia, eficacia y efectividad de los procesos; (iii) el nivel de ejecución de los planes, programas y proyectos; (iv) los resultados de la gestión, con el propósito de detectar desviaciones, establecer tendencias, y generar recomendaciones para orientar las acciones de mejoramiento de la entidad pública

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

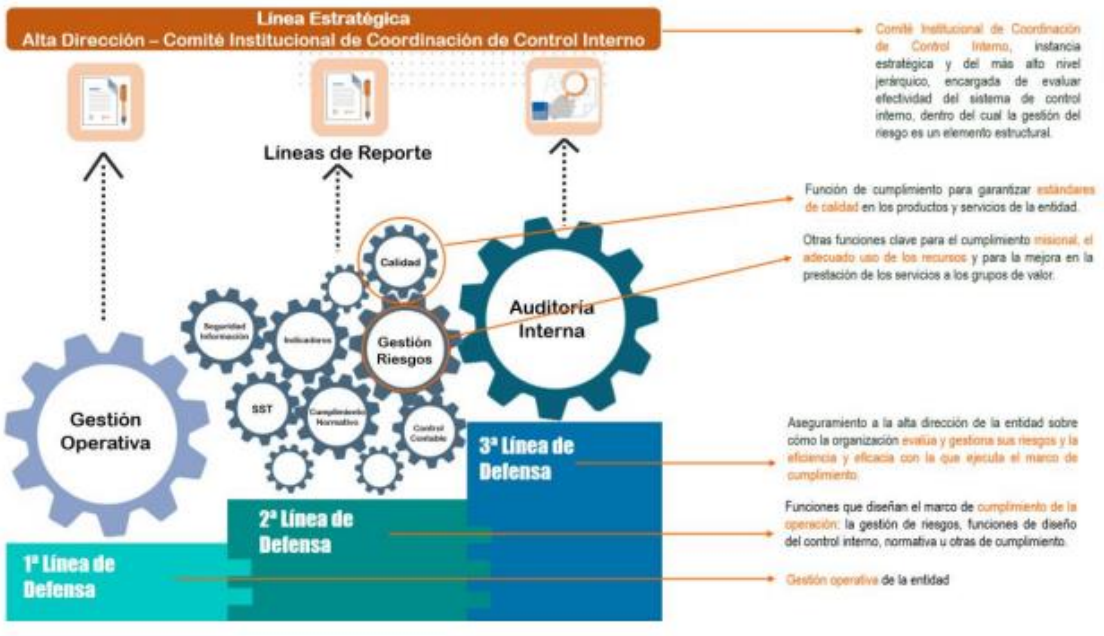
En cuanto al esquema de Líneas de Defensa se define lo siguiente:

Tabla 16.
Líneas de Defensa

LÍNEA	DESCRIPCIÓN
Línea Estratégica (Alta Dirección)	Se debe definir y aprobar la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.
1ª línea de defensa	Todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo)
2ª línea de defensa	El jefe de planeación o quien haga sus veces debe periódicamente hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema
3ª línea de defensa	Corresponde a la Oficina de Control Interno o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Ilustración 22.
Operatividad esquema Líneas de Defensa



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

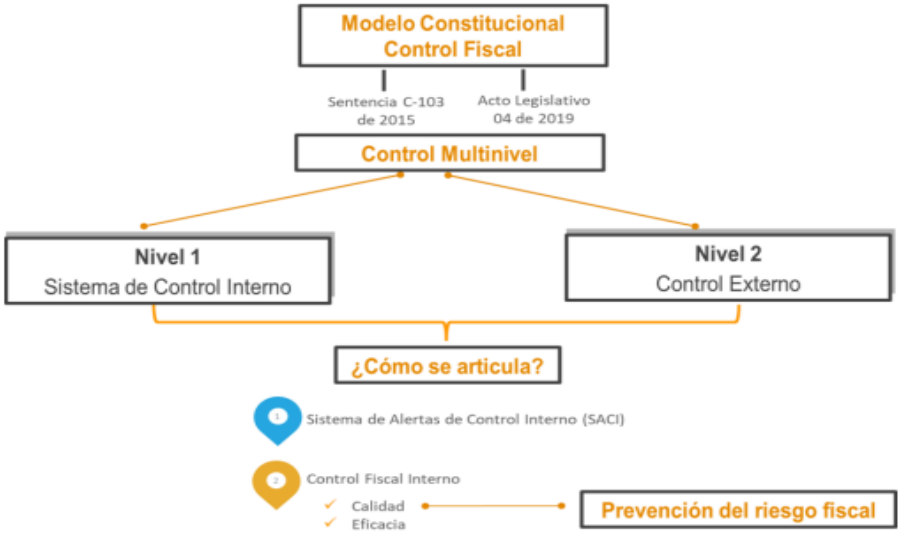
8.4. RIESGOS FISCALES

8.4.1. Control Fiscal Interno y Prevención del Riesgo Fiscal

Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000. Para tener claro el ámbito normativo y jurídico, es necesario precisar que sus bases están sentadas en los artículos 267 y 268 de la Constitución Política de 1991, los cuales fueron modificados por el Acto Legislativo 04 de 2019 que se fundamentó en la necesidad de un ejercicio preventivo del control fiscal, que detuviera el daño fiscal e identificara riesgos fiscales; de esta manera, la administración y el gestor fiscal podrían adoptar las medidas respectivas para prevenir la concreción del daño patrimonial de naturaleza pública.

En el nuevo modelo constitucional el control externo adquiere un enfoque preventivo y a su vez el control interno potencia el enfoque preventivo, partiendo de la premisa de que el Sistema de Control Interno es fundamental para conjugar el logro de resultados, con la prevención de riesgos de gestión, corrupción y fiscales, así como, con la seguridad del gestor público (jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores y responsables de la planeación contractual, supervisores, responsables de labor es de cobro, entre otros), a través de la prevención de responsabilidades.

Ilustración 23.
Articulación Modelo Constitucional Control Fiscal y Sistema de Control Interno



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.4.2. Definición y Elementos del Riesgo Fiscal

El Riesgo Fiscal es concebido con el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

ELEMENTOS QUE COMPONEN LA DEFINICION DEL RIESGO FISCAL

Tabla 17.
Elementos del Riesgo Fiscal

ELEMENTO	DESCRIPCIÓN
EFECTO	Es el 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
EVENTO POTENCIAL	Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona 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. En esta guía, el evento potencial es equivalente a la causa raíz

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

$$Riesgo\ Fiscal = \frac{Evento\ Potencial\ (Potencial\ Conducta) +}{Efecto\ dañoso}$$

Se debe tener especial cuidado en no confundir el Riesgo Fiscal, con el Daño Fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

8.4.3. Metodología y paso a paso para el levantamiento del Mapa de Riesgos Fiscales

A continuación, se presenta el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del Riesgo Fiscal.

8.4.3.1. Identificación de Riesgos Fiscales

Para la identificación del Riesgo Fiscal es necesario establecer los Puntos de Riesgo:

1. Fiscal
2. Circunstancias Inmediatas

Para poder identificar los puntos de riesgo y las circunstancias inmediatas, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de Riesgo Fiscal (actividades de gestión fiscal en las que potencialmente se genera Riesgo Fiscal), y Circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del Riesgo Fiscal). Para este taller, puede usar las siguientes preguntas orientadoras:

Tabla 18.
Preguntas orientadoras para puntos Riesgo Fiscal y Causas Inmediatas

SIRVE PARA IDENTIFICAR	PREGUNTAS Y RESPUESTAS PARA LA IDENTIFICACIÓN
Puntos de Riesgo Fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).

Puntos de Riesgo Fiscal y Circunstancias Inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), 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 de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-. Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias Inmediatas	En un ejercicio autocritico, realista y objetivo, ¿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 3 años? Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de Riesgo Fiscal y Circunstancias Inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.4.3.2. Identificación de Áreas de Impacto

Dentro del contexto de Riesgo Fiscal, el Área de Impacto siempre corresponde a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Son ejemplo de efectos económicos que no son Riesgos Fiscales, los siguientes:

a. Los Riesgos de daño antijurídico - Riesgo de pago de condenas y conciliaciones
b. Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público (ver definición de gestor público en el capítulo uno de conceptos básicos).

Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar Riesgos Fiscales es tener claro el concepto de Patrimonio Público, así como el de las tres expresiones de Patrimonio Público que se derivan del artículo 6 de la Ley 610 de 2000:

a. Bienes Públicos;
b. Recursos Públicos
c. Intereses Patrimoniales de naturaleza Pública (consultar definiciones en el capítulo uno de conceptos básicos).

El Área de Impacto se debe seleccionar de la lista desplegable en la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada *Mapa de Riesgos Fiscales*, en la columna "*Área de Impacto*".

8.4.3.3. Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa / efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador

Ejemplo:

Una entidad X se atrasó en el pago del canon de arriendo de una de sus sedes, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago.

¿Cuál es el daño?

El daño fiscal corresponde al monto pagado por concepto de intereses moratorios

¿Cuál es el hecho generador?

La omisión de pagó oportuno del canon de arrendamiento.

Conclusión: El hecho generador del daño no es el pago de los intereses moratorios, ya que el pagó es una acción diligente que da cumplimiento a una obligación adquirida y evita que se sigan generando intereses.

8.4.4. Descripción del Riesgo Fiscal

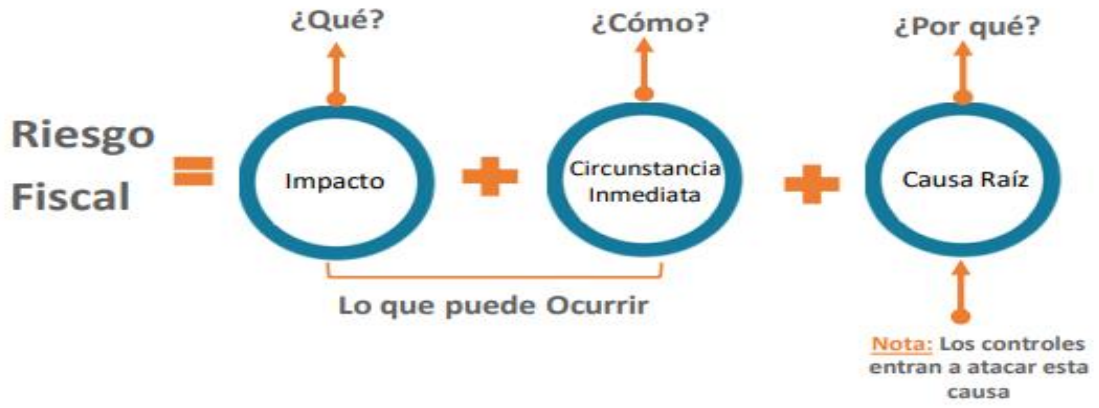
A continuación, se presenta la estructura de redacción de Riesgos Fiscales en la que se conjugan los elementos antes descritos; así mismo, se presentan algunos ejemplos de Riesgos Fiscales identificados como resultado del estudio de fallos de Contralorías Territoriales y Contraloría General de la República.

Para redactar un Riesgo Fiscal se debe tener en cuenta:

a. **Iniciar con la oración:** Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
b. **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).
c. **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.
d. **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

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

Ilustración 24.
Estructura propuesta para la redacción de Riesgos Fiscales



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6

Ejemplo:

Proceso: Gestión de Recursos

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

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Ilustración 25.
Redacción de Riesgos Fiscales

¿Qué?	¿Cómo?	¿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

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6

Como complemento a continuación se muestran otros ejemplos de redacción de Riesgos Fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso, es decir efecto dañoso sobre bienes públicos, recursos públicos o sobre intereses patrimoniales de naturaleza pública.

Ilustración 26.
Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	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 tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	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

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6

La descripción del Riesgo Fiscal se debe registrar en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** en la hoja "*Mapa de Riesgos Fiscales*", en la columna denominada "*Descripción del Riesgo*" teniendo en cuenta la estructura indicada es este apartado.

8.4.5. Valoración del Riesgo

En este punto se busca se busca establecer la probabilidad inherente de ocurrencia del Riesgo Fiscal y sus consecuencias o impacto inherentes.

8.4.5.1. Determinar la Probabilidad

Se entiende como la posibilidad de ocurrencia del Riesgo Fiscal. Se determina según al número de veces que se pasa por el punto de Riesgo Fiscal en el periodo de un (1) año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

En la siguiente ilustración se establecen los criterios para definir el nivel de Probabilidad.

Ilustración 27.
Criterios para definir el Nivel de Probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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 y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Una vez cuente con esta información, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable definida en la hoja "*Mapa de Riesgos Fiscales*", en la columna denominada "*Frecuencia con la cual se realiza la actividad*" el nivel de *Probabilidad* para cada uno de los Riesgos identificados. La información de *Probabilidad Inherente* y *Porcentaje* se genera automáticamente, de acuerdo con la selección anterior.

8.4.5.2. Determinar el Impacto del Riesgo

Considerando la naturaleza y alcance del Riesgo Fiscal, éste siempre tiene un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de Riesgos Fiscales, sin perjuicio de ello, existen diferentes niveles de impacto En la siguiente ilustración se establecen los criterios para definir el nivel de *Impacto*:

Ilustración 28.
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 organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad 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 entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

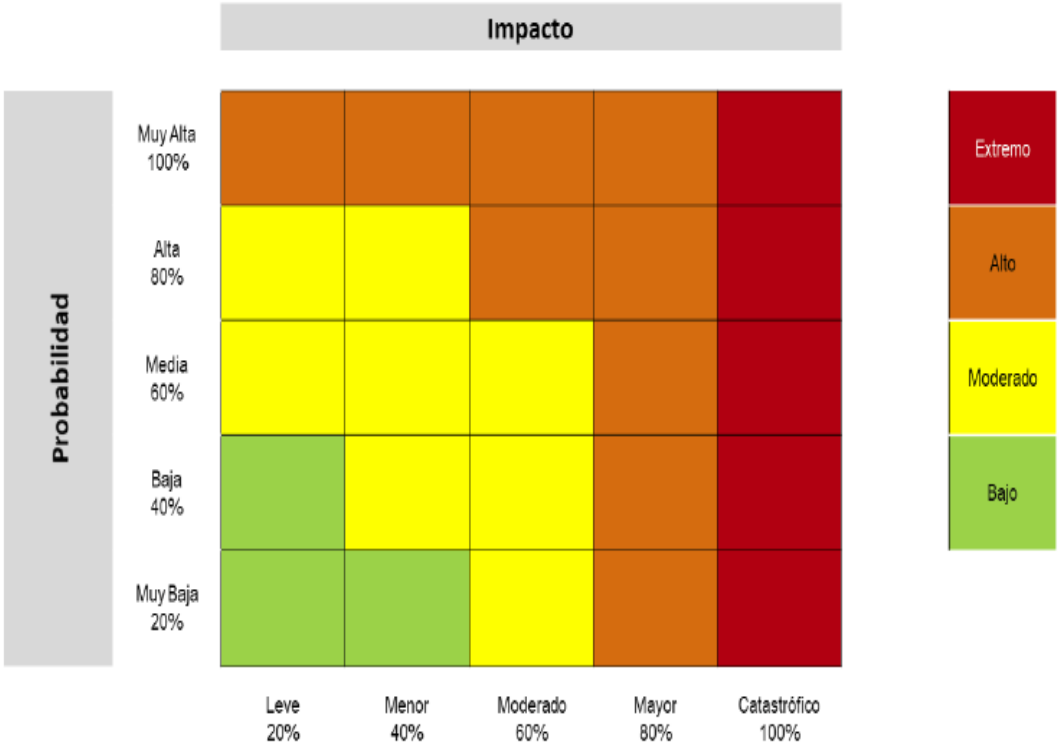
Para determinar el Impacto del Riesgo Fiscal, se debe seleccionar de la lista desplegable definida en la columna denominada "*Criterios de Impacto*" el *Impacto* para cada uno de los Riesgos identificados. La información de *Impacto Inherente* y *Porcentaje* se genera automáticamente, de acuerdo con la selección anterior.

8.4.5.3. Evaluación del Riesgo

A partir del análisis de la Probabilidad y su Impacto, se busca determinar la Zona de Riesgo Inicial o Riesgo Inherente.

Este análisis trata de determinar los niveles de severidad a través de la relación entre la probabilidad y el impacto de cada Riesgo Fiscal identificado. Para este análisis, se definen cuatro (4) zonas de severidad en la matriz de calor:

Ilustración 29.
Matriz de Calor - Niveles de Severidad del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

EJEMPLO:

Proceso: Gestión de recursos

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

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

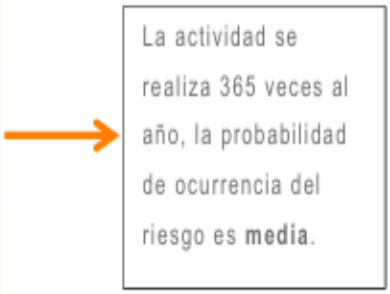
Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad Riesgo Fiscal: Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de la omisión en la aplicación del procedimiento 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).

Probabilidad: Las veces que se pasa por el punto de riesgo en un año es 365, puesto que todos los días del año de debe ejercer la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta que los bienes muebles en cada entidad varían en cantidad y son de distinto valor en el inventario, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más ácido que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, ejemplo: equipos de cómputo, muebles y enseres, entre otros.

Aplicando las tablas de probabilidad e impacto tenemos:

Ilustración 30.
Selección Probabilidad Riesgo Fiscal

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

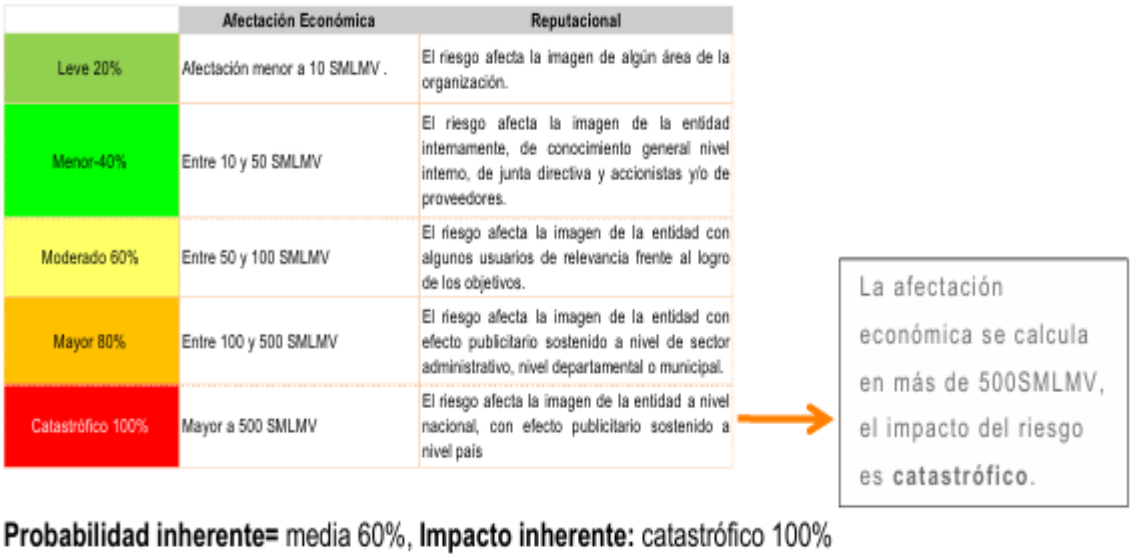


Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar el impacto es necesario cuantificar 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 que para el ejemplo se determina que es de $2.500 millones de pesos, lo cual corresponde a 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.

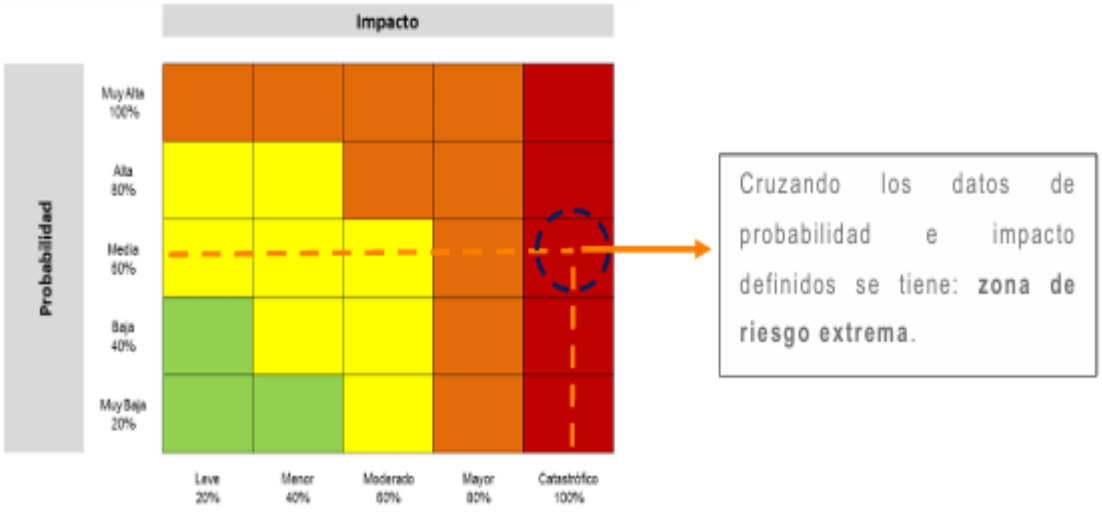
Ilustración 31.
Selección Impacto Riesgo Fiscal



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Zona de severidad o nivel de riesgo: De acuerdo con la tabla para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.

Ilustración 32.
Zona de Severidad del Riesgo Fiscal



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar la Zona de Riesgo Inherente y, de acuerdo con la selección realizada en las comunas "*Frecuencia con la cual se realiza la actividad*" y "*Criterios de Impacto*" para cada uno de los Riesgos Fiscales identificados, se calcula automáticamente el valor de Zona de Riesgo Inherente.

8.4.6. Valoración de Controles

Para la redacción de los controles asociados a los Riesgos Fiscales se aplican los lineamientos para la redacción del control establecidos en el numeral 8.2.3.1 y tabla definida en el numeral 8.2.3.3 de la presente guía.

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Tipologías de Controles:

- ✓ **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el Riesgo Fiscal - Punto de Riesgo. Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.

- ✓ **Control Detectivo:** Control accionado durante la ejecución de la actividad en la que potencialmente se origina el Riesgo Fiscal - Punto de Riesgo. Estos controles detectan el riesgo fiscal, pero generan reprocesos.

- ✓ **Control Correctivo:** Control accionado en la salida de la actividad en la que potencialmente se origina el Riesgo Fiscal - Punto de Riesgo y después de que se materializa el Riesgo Fiscal. Estos controles tienen costos implícitos.

Ejemplo

Proceso: Gestión de Recursos

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

Alcance: Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y la prestación de los servicios, acorde con la disponibilidad de recursos.

Punto de Riesgo: Ingreso, custodia y salida de bienes muebles de la entidad.

Riesgo Fiscal: 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).

Probabilidad Inherente: Media 60%

Impacto Inherente: Catastrófico 100%

Zona de Riesgo: Extrema

Tabla 19.
Valoración de Controles de Riesgo Fiscal

CONTROL 1	CRITERIOS DE EFECTIVODAD			PESO
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 = 40%			
CONTROL 2	**CRITERIOS DE EFECTIVODAD**			**PESO**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema, en caso de encontrar inconsistencias solicita al jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 2 = 30%			
CONTROL 3	**CRITERIOS DE EFECTIVODAD**			**PESO**
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	X	10%
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 3 = 25%			

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Teniendo en cuenta que es a partir de los controles que se da movimiento en la matriz de calor que corresponde, 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 y su respectiva valoración, a fin de determinar el Riesgo Residual.

A continuación, se enuncian el Catálogo de Controles que aplican para los Riesgos Fiscales identificados por parte del Instituto y que, según su aplicabilidad, se podrían definir para la mitigación de este tipo de Riesgos:

Tabla 20.
Catálogo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas

CATÁLOGO INDICATIVO Y ENUNCIATIVO DE PUNTOS DE RIESGO FISCAL Y CIRCUNSTANCIAS INMEDIATAS

Introducción

Como resultado de la metodología de investigación que ha venido implementando el Semillero de Investigación de la Academia de la Gestión Pública desde el año 2018, fue posible identificar los principales puntos de riesgo fiscal y circunstancias inmediatas de dichos riesgos, mediante el estudio de: i) los avances que los diferentes órganos de control tienen frente a la definición de riesgo fiscal y la identificación de los principales riesgos fiscales en sus sujetos vigilados, ii) el estudio de fallos con responsabilidad fiscal en firme, emitidos tanto por contralorías territoriales como por la Contraloría General de la República.

Así las cosas, los puntos de riesgo fiscal que se enuncian en este catálogo indicativo y enunciativo corresponden a actividades que representan gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública y que potencialmente pueden generar un efecto dañoso al patrimonio público.

Este listado enunciativo y no restrictivo, también posibilita identificar y conocer las Circunstancias Inmediatas más comunes en la gestión pública, que se derivan de los Puntos de Riesgo Fiscal.

Así las cosas, como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 puntos de riesgo fiscal e igual número de circunstancias inmediatas, así:

Id Referencia	**Puntos de Riesgo Fiscal**	**Circunstancia Inmediata**
	Actividad en la que potencialmente se origina el riesgo fiscal	***Situación por la que se presenta el riesgo***
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios

3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodia de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodia de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la Entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron

19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y cuyos costos colaterales asume la Entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la Entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado

35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la Entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la Entidad
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado

50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Nota. Elaboración Dirección de Gestión y Desempeño Institucional, 2022.

8.4.7. 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, siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

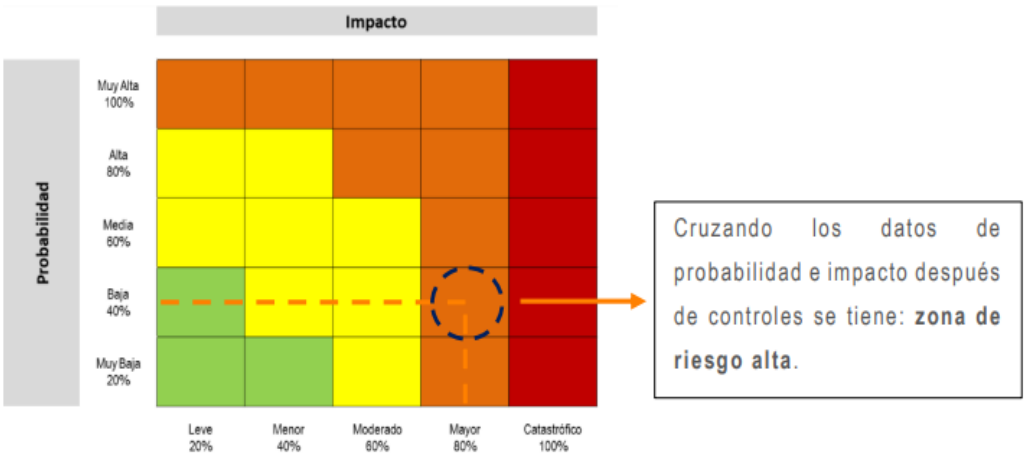
Ilustración 33.
Aplicación de los Controles definidos

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
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 de cumplimiento 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)*.	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	**36%**	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual	**75%**			

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

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 y cálculo final:

Ilustración 34.
Zona de Riesgo respecto al ejemplo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.4.8. Plan de Acción

Para efectos del Mapa de Riesgos, se debe definir el Plan de Acción, únicamente para las opciones de Reducir – Compartir y Reducir - Mitigar, en el cual especifique:

e. Plan de Acción por desarrollar
f. Responsable,
g. Fecha de inicio y,
h. Fecha de terminación

8.5. RIESGOS DE CORRUPCIÓN

8.5.1. Definición de Riesgo de Corrupción

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

Es necesario que en la descripción del riesgo concurran los componentes de su definición, como se muestra a continuación:

$$\textit{ACCIÓN U OMISIÓN} + \textit{USO DEL PODER} + \textit{DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO} + \textit{BENEFICIO PRIVADO}$$

Los Riesgos de Corrupción se establecen sobre procesos. El Riesgo de Corrupción 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.

Con el fin de facilitar la identificación de Riesgos de Corrupción y evitar que se presenten confusiones con otro tipo de riesgos, se sugiere la utilización de la matriz de definición de Riesgo de Corrupción, que incorpora cada uno de los componentes de su definición.

Ilustración 35.
Definición Riesgo de Corrupción

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.5.2. Valoración de Riesgos

8.5.2.1. Cálculo de la Probabilidad e Impacto

El Líder de Proceso debe analizar qué tan posible es que se materialice el riesgo, lo que se expresa en términos de frecuencia o factibilidad, donde la frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; la factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda:

Los criterios para calificar la probabilidad son:

Tabla 21.
Criterios para calificar la Probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año

4	Probable	Es viable que ele vento ocurra en la mayoría de las circunstancias	Al menos 1 vez al año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Una vez se cuente con la información, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable definida en la hoja "*Mapa de Riesgos Corrupción*", en la columna denominada "*Frecuencia*" el nivel de *Probabilidad* para cada uno de los Riesgos identificados. Una vez se seleccione la opción correcta, la información de los campos de "*Descriptor*, "*Descripción*", "*Nivel*" y "*Probabilidad*" se calculan automáticamente.

8.5.2.2. Análisis de Impacto

Para la determinación del *Impacto* frente a posibles materializaciones de Riesgos de Corrupción, se deben analizar únicamente los niveles Moderado, Mayor y Catastrófico**,** dado que estos riesgos siempre son significativos; en tal sentido, no aplican los niveles de impacto Insignificante y/o Menor, los cuales sí aplican para las demás tipologías de riesgos.

Para establecer estos niveles de *Impacto* se deben aplicar las siguientes preguntas frente al riesgo identificado:

Tabla 22.
Criterios para calificar el Impacto en Riesgos de Corrupción

TABLA PARA ESTABLECER LA ZONA DE RIESGO DE CORRUPCIÓN		
PREGUNTA	**RESPUESTA**	
SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA	**SI**	**NO**
1. ¿Afectar al grupo de funcionarios del proceso?		
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3. ¿Afectar el cumplimiento de la misión de la entidad?		
4. ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		

5. ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6. ¿Generar pérdida de recursos económicos?		
7. ¿Afectar la generación de productos o la prestación del servicio?		
8. ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9. ¿Generar pérdida de información de la entidad?		
10. ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11. ¿Dar lugar a procesos sancionatorios?		
12. ¿Dar lugar a procesos disciplinarios?		
13. ¿Dar lugar a procesos fiscales?		
14. ¿Dar lugar a procesos penales?		
15. ¿Generar pérdida de credibilidad del sector?		
16. ¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17. ¿Afectar la imagen regional?		
18. ¿Afectar la imagen nacional?		
19. ¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas genera un impacto Moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto Catastrófico		

MODERADO	Genera medianas consecuencias sobre la entidad
MAYOR	Genera altas consecuencias sobre la entidad
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

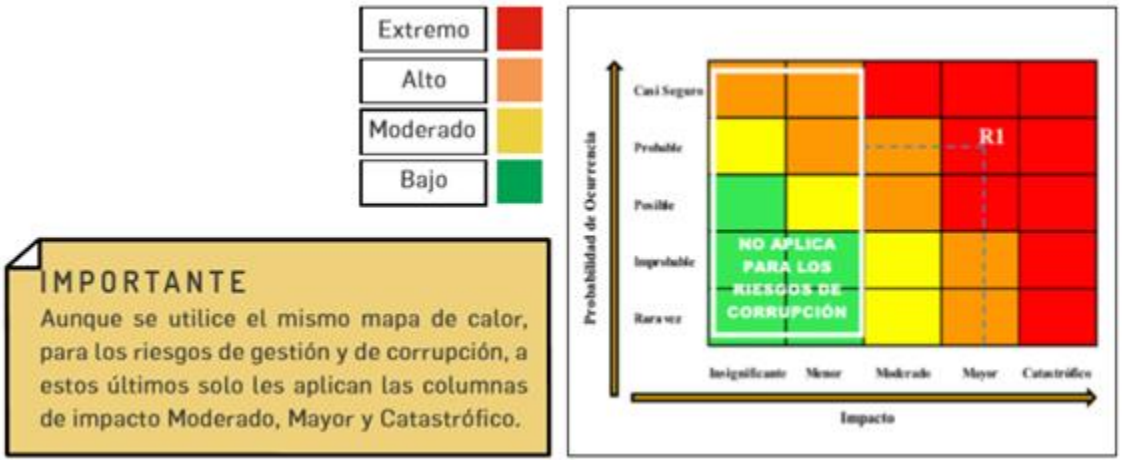
Para la determinación del *Impacto*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe dar respuesta a **TODAS** las 19 preguntas, seleccionando de la lista desplegable la opción "SI" o "NO". Una vez se responden todas las preguntas, el formato automáticamente realiza el cálculo del nivel de *Impacto* del Riesgo de Corrupción.

8.5.2.3. Análisis del Impacto en Riesgos de Corrupción

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de Riesgo Inicial o Riesgo Inherente.

Para la evaluación del riesgo y determinación de la zona de Riesgo Inherente se debe utilizar el mapa de calor que se encuentra relacionado a continuación:

Ilustración 36.
Mapa de Calor



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

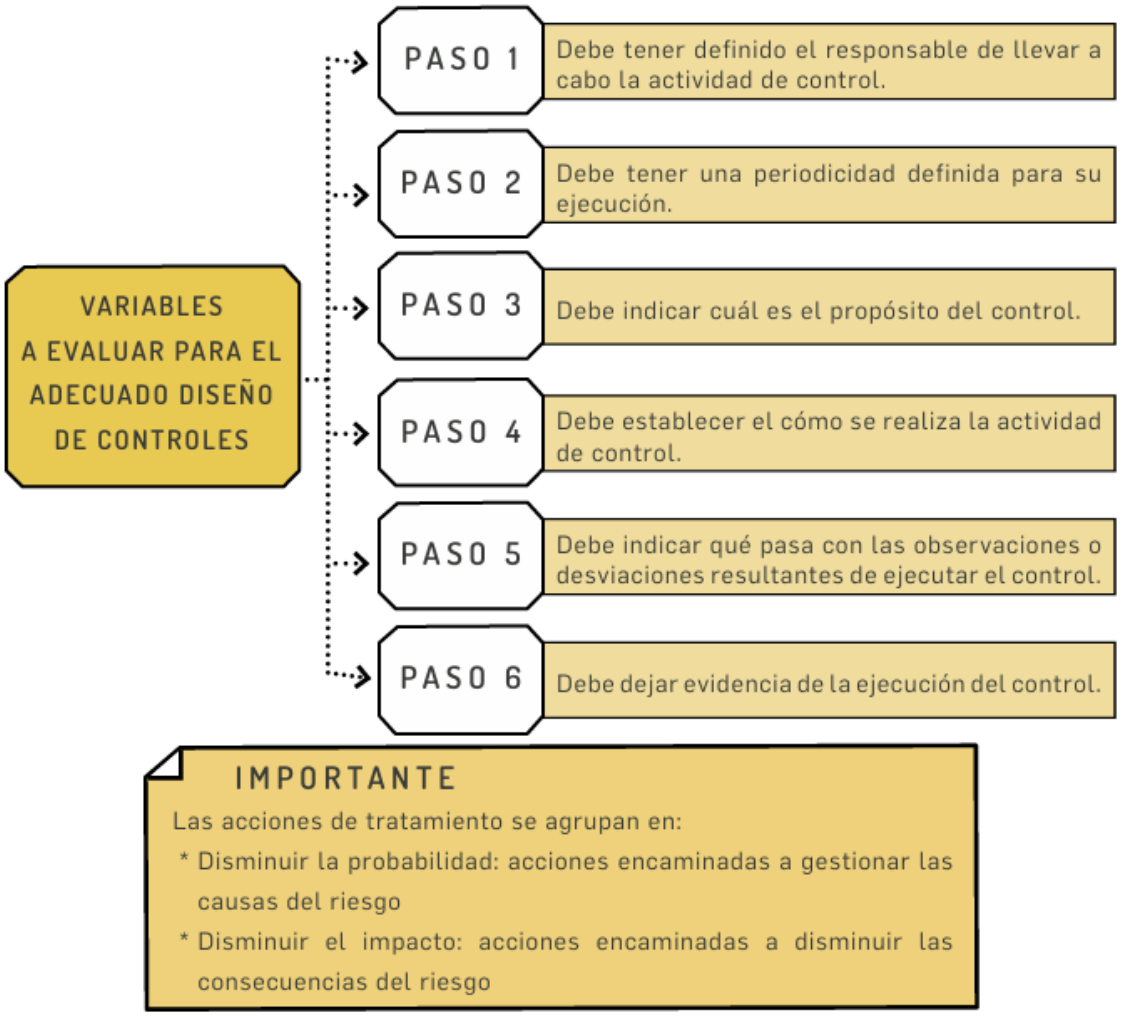
Ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos, el cual corresponde al Nivel de Riesgo Inherente. El punto donde se cruza los datos de la probabilidad y el impacto indica la severidad del riesgo, que se puede clasificar en Extremo, Alto o Moderado.

En el formato **F-DE-13 Matriz de Riesgos y Oportunidades**, el cálculo de la Zona de Riesgo Inherente se realiza automáticamente, luego de seleccionar los niveles de probabilidad e impacto del riesgo.

8.5.2.4. Diseño de Controles

Antes de valorar los controles es necesario conocer cómo se diseña un Control, para lo cual mostramos la siguiente ilustración:

Ilustración 37.
Pasos para diseñar un Control



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 4.

Para el presente documento, es preciso que los Líderes de Proceso definan como mínimo dos (2) controles para cada Riesgo de Corrupción identificado, esto con el propósito de realizar el cálculo matemático descrito en el numeral 8.5.2.5.

8.5.2.5. Valoración de los Controles

Para la valoración de los controles, conforme lo indica la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, se tienen en cuenta los lineamientos descritos en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 4.

En este sentido, para la valoración de los controles, se tienen en cuenta los siguientes criterios y calificaciones respectivas:

Ilustración 38.
Peso o participación de cada variable en el diseño del Control

CRITERIO DE EVALUACIÓN.	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

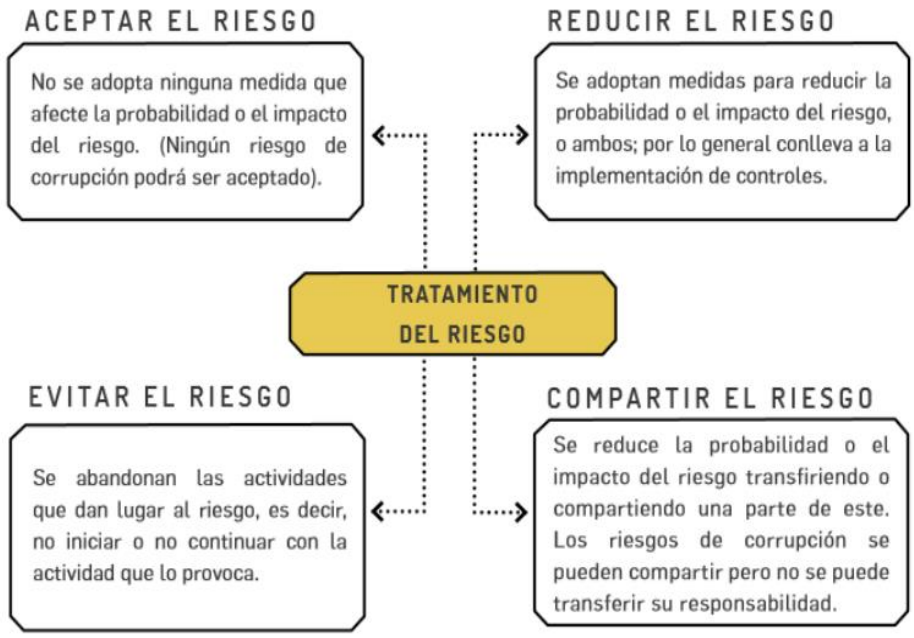
Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 4.

Para la valoración de los *Controles* definidos para cada Riesgo de Corrupción, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe dar respuesta a **TODAS** las columnas "*Asignación del responsable*", "*Segregación de la Autoridad del responsable*", "*Periodicidad*", "*Propósito*", "*Cómo se realiza la actividad de Control*", "*Qué pasa con las observaciones o desviaciones*" y "*Evidencia de la ejecución del Control*"; una vez seleccionadas las opciones de las listas desplegables para cada una de estas columnas, el formato automáticamente realiza el cálculo del nivel de la "*Solidez Individual del Control*", su "*Rango de Calificación*", la "*Solidez del conjunto de Controles*", la "*Calificación del conjunto de Controles*", la "*Probabilidad Residual*", la "*Probabilidad Residual Final*", el "*Resultado Probabilidad Residual Final*", el "*Impacto residual Final*" y la "*Zona de Riesgo Residual*".

8.5.2.6. Tratamiento del Riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción, el tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Ilustración 39.
Tratamiento del Riesgo



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar el *Tratamiento del Riesgo*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Tratamiento*" la opción "Aceptar", "*Evitar*", "*Reducir - Compartir*", o "*Reducir - Mitigar*".

Para efectos del Mapa de Riesgos, se debe definir el Plan de Acción, únicamente para las opciones de Reducir – Compartir y Reducir - Mitigar, en el cual especifique:

a. Plan de Acción por desarrollar
b. Responsable,
c. Fecha de inicio y,
d. Fecha de terminación

8.5.3. Monitoreo de Riesgos de Corrupción

El Rector de Institución Tecnológica y los Líderes de Procesos, en conjunto con sus equipos de trabajo, deben monitorear y revisar periódicamente la gestión de Riesgos de Corrupción y, si es el caso, ajustarlo (primera línea de defensa). Le corresponde, igualmente, al proceso de Direccionamiento Estratégico y Planeación adelantar el monitoreo (segunda línea de defensa).

8.5.4. Seguimiento de Riesgos de Corrupción

8.5.4.1. Seguimiento

El Profesional Especializado adscrito al proceso de Control Interno de Gestión o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante el seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

En este sentido, los seguimientos deben realizarse teniendo en cuenta los siguientes lineamientos:

Tabla 23.
Seguimientos Matriz de Riesgos de Corrupción

SEGUIMIENTO	OBSERVACIÓN
Primer seguimiento	Con corte al 30 de abril. En esa medida, la publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de mayo.
Segundo seguimiento	Con corte al 31 de agosto. La publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.
Tercer seguimiento	Con corte al 31 de diciembre. La publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

Nota. Proceso de Direccionamiento Estratégico y Planeación, ISER, 2024.

El seguimiento adelantado por el proceso de Control Interno de Gestión se debe publicar en la página web institucional www.iser.edu.co en un lugar de fácil acceso para la ciudadanía.

8.5.4.2. Acciones para seguir en caso de materialización de Riesgos de Corrupción

En el evento de materializarse un Riesgo de Corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción.
2. Revisar el Mapa de Riesgos de Corrupción, en particular, las causas, riesgos y controles.
3. Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
4. Llevar a cabo un monitoreo permanente

El proceso de Control Interno de Gestión debe asegurar que los controles sean efectivos, le apunten al Riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a:

- ✓ Determinar la efectividad de los Controles.
- ✓ Mejorar la valoración de los Riesgos.
- ✓ Mejorar los controles.
- ✓ Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los Riesgos de Corrupción.
- ✓ Determinar si se adelantaron acciones de monitoreo.
- ✓ Revisar las acciones del monitoreo.

8.6. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.6.1.1. Identificación de los Activos de Seguridad de la Información

Como primer paso para la identificación de Riesgos de Seguridad de la Información es necesario y, prerrequisito, identificar los activos de información del proceso.

Ilustración 40.
Conceptualización Activos de Información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Ilustración 41.
Conceptualización de los Activos

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Ilustración 42.
Pasos para la identificación de Activos

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Ilustración 43.
Ejemplo de identificación de Activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.6.1.2. Identificación del Riesgo

Se pueden identificar los siguientes tres (3) Riesgos inherentes de Seguridad de la Información:

- ✓ Pérdida de la Confidencialidad
- ✓ Pérdida de la Integridad
- ✓ Pérdida de la Disponibilidad

Para determinar el *Riesgo*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Riesgo*" la opción "*Pérdida de la Confidencialidad*", "*Pérdida de la Integridad*" o "*Pérdida de la Disponibilidad*".

El Líder de Proceso debe identificar el "*Tipo de Activo*" asociado que le permitan analizar las posibles amenazas y vulnerabilidades que podrían causar la materialización del Riesgo de Seguridad de la Información, los cuales se enuncian a continuación:

Tabla 24.
Vulnerabilidades Riesgo de Seguridad de la Información

TIPO DE ACTIVO	VULNERABILIDAD
HARDWARE	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
SOFTWARE	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección

	Software nuevo o inmaduro
RED	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
INFORMACIÓN	Falta de controles de acceso físico
	Interceptación de servicios de señales de interferencia comprometida
	Espionaje remoto
PERSONAL	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
LUGAR	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
ORGANIZACIÓN	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar el *Tipo de Activo*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Activo*" las opciones predefinidas en el documento.

Es importante recalcar que 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.

De la misma manera, se debe determinar el *Impacto*, como la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Para determinar el *Impacto*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Impacto*" las opciones predefinidas en el documento.

8.6.1.3. Descripción del Riesgo

Es necesario que en la descripción del riesgo concurran los componentes de su definición, como se muestra a continuación:

AUSENCIA DE CONTROLES DEL RIESGO + CONSECUENCIA + AFECTACIÓN DEL ACTIVO

Ilustración 44.
Ejemplo redacción de Riesgos de Seguridad de la Información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.6.1.4. Identificación de Amenazas

Se plantean los siguientes listados de *Amenazas*, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los Riesgos de Seguridad de la Información.

Tabla 25.
Riesgo de Seguridad de la Información

TIPO	AMENAZA	ORIGEN
DAÑO FÍSICO	Fuego	F, D, A
	Agua	F, D, A
EVENTOS NATURALES	Fenómenos climáticos	E
	Fenómenos sísmicos	E
PÉRDIDAS DE LOS SERVICIOS ESENCIALES	Fallas en el sistema de suministro de agua	E
	Fallas den el suministro de aire acondicionado	F, D, A
PERTURBACIÓN DEBIDA A LA RADIACIÓN	Radiación electromagnética	F, D, A
COMPROMISO DE LA INFORMACIÓN	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
FALLAS TÉCNICAS	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
ACCIONES NO AUTORIZADAS	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F

COMPROMISOS DE LAS FUNCIONES	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D
CONVENCIONES: F: Fortuito D: Deliberadas A: Ambientales		

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar las *Amenazas*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Amenaza*" las opciones predefinidas en el documento.

8.6.1.5. Vulnerabilidad del Riesgo de Seguridad de la Información

Igualmente, es importante seleccionar las vulnerabilidades asociadas a la amenaza identificada para cada uno de los Riesgos de Seguridad de la Información determinados, las cuales se encuentran descritas en la Tabla 23 del presente documento.

Para determinar la *Vulnerabilidad*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Vulnerabilidad*" las opciones predefinidas en el documento.

8.6.2. Valoración del Riesgo

Para esta etapa se asocian las tablas de *Probabilidad* e *Impacto* definidas en la primera parte de la presente guía.

Ilustración 45.
Niveles de Probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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 y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar la *Frecuencia*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "*Frecuencia con la cual se realiza la actividad*" las opciones predefinidas en el documento.

Ilustración 46.
Determinación del Impacto

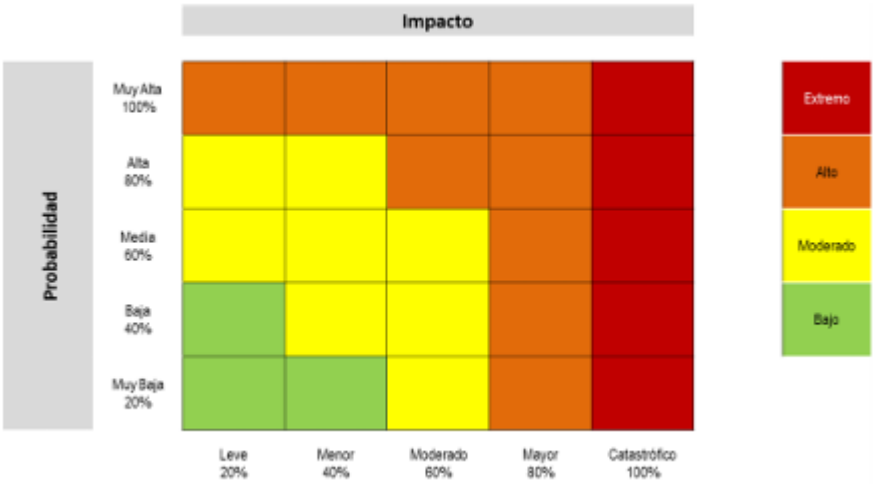
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad 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 entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar el *Impacto*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** se debe seleccionar de la lista desplegable de la columna denominada "Criterios de *Impacto*" las opciones predefinidas en el documento.

Para el análisis del Riesgo Inherente, en esta etapa se define el *Nivel de Severidad* para el Riesgo de Seguridad de la Información identificado, para ello se aplica la matriz de calor establecida la cual se evidencia a continuación:

Ilustración 47.
Matriz de Calor



Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

Para determinar la *Zona de Riesgo Inherente*, en el formato **F-DE-13 Matriz de Riesgos y Oportunidades** esta se calcula automáticamente, de acuerdo con la selección de las opciones predeterminadas en la *Probabilidad* e *Impacto* determinado para el Riesgo de Seguridad de la Información en evaluación.

8.6.3. Controles asociados a la Seguridad de la Información

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del Documento Maestro del Modelo de Seguridad y Privacidad de la Información - MSPI:

Ilustración 48.
Ejemplos de controles de Seguridad de la Información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Nota. Departamento Administrativo de la Función Pública – DAFP, Guía de Administración del Riesgo versión 6.

8.6.4. Valoración de los Controles

Para valorar los Controles asociados a los Riesgos de Seguridad de la Información, se deben seguir los lineamientos definidos en el numeral 8.3.3 de la presente guía, actividades que finalmente nos permiten calcular el valor del Riesgo Residual.

8.6.5. Plan de Acción

Para efectos del Mapa de Riesgos, se debe definir el Plan de Acción, únicamente para las opciones de Reducir – Compartir y Reducir - Mitigar, en el cual especifique:

a. Plan de Acción por desarrollar
b. Responsable,
c. Fecha de inicio y,
d. Fecha de terminación

8.7. IDENTIFICACIÓN Y PRIORIZACIÓN DE OPORTUNIDADES

La norma ISO 9001 define el Riesgo como el efecto de la incertidumbre sobre un resultado esperado. La Oportunidad, en cambio, es la posibilidad de obtener un resultado favorable. Ambos pueden afectar a la calidad de los productos y servicios y al desempeño del Sistema de Gestión de la Calidad.

Las Oportunidades pueden conducir a la adopción de nuevas prácticas, lanzamiento de nuevos productos, apertura de nuevos mercados, acercamiento a nuevos clientes, establecimiento de asociaciones, utilización de nuevas tecnologías y otras posibilidades deseables y viables para abordar las necesidades de la organización o las de sus clientes.

La gestión de Oportunidades es la evaluación que se realiza de la gestión interna y externa, la cual tiene como objetivo mejorar la eficacia del sistema de gestión de calidad obteniendo unos mejores resultados, adelantándose o previniendo efectos negativos.

En tal sentido, el Instituto Superior de Educación Rural – ISER, dando cumplimiento al numeral 6.1 de la NTC ISO 9001:2015, pretende identificar las Oportunidades que fomenten la mejora integral institucional y abordar las acciones necesarias que conlleven a su materialización.

Para este objetivo, se ha definido la F-DE-13 Matriz de Riesgos y Oportunidades, donde se debe establecer y definir las Oportunidades resultantes del Análisis del Contexto Interno y Externo, al igual que se debe determinar los factores de incidencia para priorizar las Oportunidades a ejecutar.

8.7.1. Consecutivo

Se debe establecer el consecutivo de cada una de las Oportunidades identificadas por parte del proceso. Para la asignación de los consecutivos, esta se debe hacer en orden ascendente comenzando con **1** hasta numerar el número total de Oportunidades que identifique el proceso.

8.7.2. Oportunidad

El Líder del Proceso debe redactar cada una de las Oportunidades con las que cuenta el proceso, de la manera más clara y precisa, en la cual no se generen dudas ni ambigüedades. La redacción

de la Oportunidad debe enunciar lo que se el proceso o la Institución quiere alcanzar y qué pretende beneficiar su desempeño.

8.7.3. Factor de Incidencia

Para la priorización de las Oportunidades del proceso, para cada una de ellas se debe calificar los factores de incidencia, en la cual se le asigna un puntaje por cada factor, cálculo que permite establecer la priorización de las Oportunidades.

Los factores de incidencia, su descripción y el valor por cada nivel se encuentra definido en la siguiente tabla:

Tabla 26.
Factores de Incidencia - Factibilidad

FACTIBILIDAD	
ESCALA	**DESCRIPCIÓN**
1	El Instituto no cuenta con los recursos necesarios y suficientes para materializar la Oportunidad descrita.
2	El Instituto cuenta con por lo menos el 5% con los recursos necesarios y suficientes para materializar la Oportunidad descrita.
3	El Instituto cuenta con por lo menos el 25% con los recursos necesarios y suficientes para materializar la Oportunidad descrita.
4	El Instituto cuenta con por lo menos el 50% con los recursos necesarios y suficientes para materializar la Oportunidad descrita.
5	El Instituto cuenta con los recursos necesarios y suficientes para materializar la Oportunidad descrita.

Nota. Instituto Superior de Educación rural - ISER, proceso de Direccionamiento Estratégico, 2024.

Tabla 27.
Factores de Incidencia - Impacto

IMPACTO	
ESCALA	**DESCRIPCIÓN**
1	La Oportunidad no apoya el logro de los Objetivos Estratégicos de la Institución.
2	La Oportunidad permite dar complementariedad el logro del plan de acción del proceso de la Institución.

3	La Oportunidad permite dar complementariedad el logro de otros proyectos estratégicos de la Institución.
4	La Oportunidad permite mejorar el desempeño del proceso frente al cumplimiento de objetivos propios de la Institución.
5	La Oportunidad apoya significativamente el logro de los Objetivos Estratégicos de la Institución.

Nota. Instituto Superior de Educación Rural - ISER, proceso de Direccionamiento Estratégico, 2024.

Una vez se realiza la calificación de cada factor para cada Oportunidad, el formato F-DE-13 Matriz de Riesgos y Oportunidades automáticamente calcula, en la columna denominada "*Total*", el valor producto del cruce de los dos (2) factores. Aquellas Oportunidades que obtengan mayor valor, en lo posible, deben ser priorizadas por parte de los Líderes de Proceso.

Las estrategias priorizadas pueden o no ser proyectadas por parte de los Líderes de Proceso para su posterior definición del plan de acción, que conlleve a su materialización. Para esto, el Líder de Proceso debe seleccionar la opción "*SI*" o la opción "*NO*" de la columna "*Oportunidad Proyectada*".

Aquellas Oportunidades priorizadas y proyectadas, debe definirse el documento o herramienta desde donde se abordará su tratamiento, por lo que el Líder de Proceso debe describir el documento o herramienta en la columna denominada "*Documento o herramienta donde se abordará la oportunidad priorizada*". En esta columna se pueden incluidas opciones tales como el Plan de Acción, Proyecto u otro mecanismo en donde se pueda demostrar la ejecución de las acciones necesarias para lograr la Oportunidad priorizada y proyectada.

8.7.4. Tratamiento de Oportunidades

Para el Tratamiento de las *Oportunidades*, es preciso definir el objetivo de la Oportunidad priorizada y proyectada, es decir, lo que espera lograr con esta estrategia, objetivo que se debe describir en la columna "*Objetivo de la Oportunidad*".

Acto seguido, el Líder de Proceso debe definir el Plan de Acción (Conjunto de acciones) con el que se pretende abordar la Oportunidad, el responsable (s), los recursos requeridos para su ejecución, su fecha de implementación (por cada actividad definida) y los mecanismos de verificación (Indicadores o soporte que verifique su implementación) requeridos para su monitoreo.

8.8. SEGUIMIENTO A RIESGOS

En la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada "*Seguimiento a Riesgos*" se puede encontrar la estructura para realizar el seguimiento y evaluación de Riesgos definidos por parte de los procesos institucionales.

En este sentido, para realizar el respectivo seguimiento a los Riesgos de Gestión, Fiscales, de Corrupción y Seguridad de la Información, se debe diligenciar la siguiente información:

Tabla 28.
Factores de Evaluación de Riesgos y Controles

CAMPO	DESCRIPCIÓN
Corte de seguimiento	Se refiere al período de seguimiento adelantado por parte del proceso de Direccionamiento Estratégico y Planeación, los cuales están definidos con una frecuencia cuatrimestral. Es por ello, que se debe seleccionar de la lista desplegable de este campo una de las opciones parametrizadas (I cuatrimestre, II cuatrimestre o III cuatrimestre).
Descripción del Riesgo	En este campo, es preciso que se relacionen cada una de las descripciones de los diferentes tipos de riesgo definido por parte de los procesos institucionales, tal cual como se han descrito en cada una de las hojas correspondientes.
Tipo de Riesgo	En este campo se debe seleccionar la opción correspondiente al tipo de riesgo a evaluar (Gestión, Fiscal, Corrupción o Seguridad de la Información), dato que debe coincidir con lo descrito en cada una de las hojas creadas para cada tipología de riesgo.
Zona de Riesgo Inherente	Este valor corresponde al valor de evaluación inherente que obtiene el riesgo en evaluación y, el cual debe ser seleccionado de la lista desplegable configurada para este campo (Extremo, Alto, Moderado o Bajo).
Controles	En este campo se deben listar cada uno de los controles definidos para cada uno de los riesgos, en sus diferentes tipologías, identificados.
Zona de Riesgo Residual	Este valor corresponde al valor de evaluación después de los controles que obtiene el riesgo en evaluación y, el cual debe ser seleccionado de la lista desplegable configurada para este campo (Extremo, Alto, Moderado o Bajo).
EVALUACIÓN DISEÑO Y EJECUCIÓN DEL CONTROL	
Esta sección se encuentra compuesta por una serie de factores, los cuales tienen como objetivo valorar el nivel de eficacia del control de acuerdo con los siguientes parámetros:	
Asignación del responsable	En este campo se debe valorar que el control debe tener definido el responsable de realizar la actividad de control. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (responsable asignado) o 0 (responsable no asignado).
Segregación y autoridad del responsable	En este campo se debe definir la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (adecuado) o 0 (inadecuado).

Periodicidad	En este campo se debe valorar si se tiene una periodicidad definida para la ejecución de cada uno de los controles a evaluar. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (oportuna) o 0 (inoportuna).
Propósito	En este campo se debe valorar si se define cuál es el propósito de cada uno de los controles a evaluar. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (prevenir), 10 (detectar) o 0 (no es un control).
Cómo se realiza la actividad de control	En este campo se debe valorar si se establece el cómo se realiza la actividad de control de cada uno de los controles a evaluar. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (confiable) o 0 (no confiable).
Qué pasa con las observaciones o desviaciones	En este campo se debe valorar si se indica qué pasa con las observaciones o desviaciones resultantes de ejecutar el control, de cada uno de los controles a evaluar. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 15 (confiable) o 0 (no confiable).
Evidencia de la ejecución del control	En este campo se debe valorar si se deja evidencia de la ejecución del control de cada uno de los controles a evaluar. De acuerdo con la validación realizada, se debe seleccionar de la lista desplegable configurada en este campo los valores 10 (completa), 5 (incompleta) o 0 (no existe).

Nota. Instituto Superior de Educación rural - ISER, proceso de Direccionamiento Estratégico, 2024.

Una vez se completa la valoración de cada uno de los controles asociados a cada tipo de riesgo, los campos de "*Peso de la evaluación del diseño del control*", "*Rango de Calificación del Diseño*", "*Peso en la ejecución de cada control*", "*Rango de calificación*", "*Resultado solidez individual de los controles*" y "*Debe establecer acciones para fortalecer el control* (SI / NO)" se calculan automáticamente, de acuerdo con los valores asignados a cada uno de los factores evaluados.

Este último campo, nos indica si es o no necesario formular acciones para fortalecer el control, los cuales deben realizarse teniendo en cuenta los lineamientos definidos en el procedimiento **P-CIG-02 Gestión de Planes de Mejoramiento**.

En el campo denominado "*Riesgo materializado*", el proceso de Direccionamiento Estratégico y Planeación debe constatar si el riesgo se ha materializado o no, esto con el propósito de establecer las acciones necesarias y requeridas para su mitigación. En caso de que el proceso de Direccionamiento Estratégico y Planeación evidencie que el riesgo se ha materializado, el Líder de Proceso debe establecer una Plan de Mejoramiento conforme los lineamientos descritos en el procedimiento **P-CIG-02 Gestión de Planes de Mejoramiento**.

Finalmente, en el campo de "*Observaciones*", se deben registrar los comentarios adicionales que el proceso de Direccionamiento Estratégico y Planeación haga respecto a la ejecución del control.

8.9. SEGUIMIENTO A OPORTUNIDADES

En la **F-DE-13 Matriz de Riesgos y Oportunidades**, en la hoja denominada "*Seguimiento a Oportunidades*" se puede encontrar la estructura para realizar el seguimiento y evaluación de las Oportunidades definidas por parte de los procesos institucionales.

En este sentido, para realizar el respectivo seguimiento a las Oportunidades, se debe diligenciar la siguiente información:

Tabla 29.
Factores de Evaluación de Oportunidades

CAMPO	DESCRIPCIÓN
Corte de seguimiento	Se refiere al período de seguimiento adelantado por parte del proceso de Direccionamiento Estratégico y Planeación, los cuales están definidos con una frecuencia cuatrimestral. Es por ello, que se debe seleccionar de la lista desplegable de este campo una de las opciones parametrizadas (I cuatrimestre, II cuatrimestre o III cuatrimestre).
No.	Corresponde al número consecutivo de Oportunidades definidas por parte del proceso responsable.
Oportunidad priorizada	En este campo, es preciso que se relacionen cada una de las descripciones de las diferentes oportunidades definidas por parte de los procesos institucionales, tal cual como se han descrito en la hoja Identificación Priorización de Oportunidades.
Acciones para abordar la Oportunidad	En este campo se deben listar el conjunto de actividades previamente definidas en la hoja Identificación Priorización de Oportunidades.
Responsables	En este campo se deben listar los responsables por cada actividad definida previamente en la hoja Identificación Priorización de Oportunidades.
Fecha de implementación	En este campo se deben listar las fechas de implementación de cada actividad definidas previamente en la hoja Identificación Priorización de Oportunidades.
Mecanismos de verificación	En este campo se deben listar los mecanismos de verificación de la ejecución de cada actividad definida previamente en la hoja Identificación Priorización de Oportunidades.
% de ejecución de las acciones	En este campo el proceso de Direccionamiento Estratégico y Planeación debe escribir el valor de avance, en porcentaje, de cada una de las actividades previamente definidas en el Plan de Acción.
Observación	En este campo se deben registrar los comentarios adicionales que el proceso de Direccionamiento Estratégico y Planeación haga respecto a la ejecución del Plan de Acción para abordar la Oportunidad.

Nota. Instituto Superior de Educación rural - ISER, proceso de Direccionamiento Estratégico, 2024.

9. ANEXOS

No aplica.

10. REFERENCIAS BIBLIOGRÁFICAS

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 04
Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, Versión 06
Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

11. HISTORIA DE MODIFICACIONES

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
03/03/2021	01	Actualización del documento por modificaciones al mapa de procesos.
01/12/2021	02	Actualización del documento por aprobación de la Política para la Administración del Riesgo, según guía del DAFP versión 05.
21/12/2023	03	Modificación del presente documento como consecuencia de la adopción de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 4. Actualización del instrumento la matriz de riesgos y oportunidades de la institución.
10/07/2024	04	Modificación del presente documento como consecuencia de la adopción de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 y la actualización del instrumento de la matriz de riesgos y oportunidades de la institución.

12. CONTROL DE CAMBIOS

Elaboró	Aprobó
Mónica Enith Salanueva Abril	Mónica Enith Salanueva Abril
Profesional Especializado adscrito al proceso de Direccionamiento Estratégico y Planeación	Profesional Especializado adscrito al proceso de Direccionamiento Estratégico y Planeación