TABLA DE CONTENIDO

1. OBJETIVO

Presentar el compromiso de la Dirección del Ministerio de Tecnologías de la Información y las Comunicaciones en cuanto a la gestión del riesgo bajo el marco que brinda el Manual Operativo del Modelo Integrado de Planeación y Gestión, en su dimensión y política de Control Interno, componente Evaluación del Riesgo del Modelo Estándar de Control Interno -MECI, y las directrices que se establecen en el estatuto anticorrupción establecido en la Ley 1474 de 2011.

Este documento es una guía para los líderes y gestores de los procesos y, colaboradores del Ministerio/Fondo Único de TIC, en la gestión del riesgo aplicada a todos los niveles de la organización.

Los lineamientos aquí establecidos para la Administración de Riesgos de Gestión, Corrupción, Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Ministerio, Seguridad y Salud en el Trabajo y Ambientales, buscan contribuir al fortalecimiento del Sistema Institucional de Control Interno -SICI y del Sistema Integrado de Gestión -SIG de la Entidad, facilitando el autocontrol, la autogestión, la autorregulación y la autoevaluación que generen una disminución considerable en la incertidumbre, en el cumplimiento de los objetivos institucionales y de igual forma hacer del cumplimiento de los mismos con eficiencia, eficacia y efectividad.

2. ALCANCE

El Manual para la Administración del Riesgo, aplica para la identificación, análisis, valoración, tratamiento, monitoreo, control y comunicación de los riesgos de Gestión, Corrupción, Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios del Ministerio, Seguridad y Salud en el Trabajo y Ambientales de la Entidad.

Aplica para los riesgos considerados en el mapa de riesgos institucional.

El presente Manual establece los lineamientos para la Administración de los riesgos más significativos de la Entidad, que debe ser aplicado bajo el enfoque por procesos alineado a las cadenas de valor del Modelo Integrado de Gestión - MIG, en el marco del Manual Operativo del Modelo Integrado de Planeación y Gestión - MIPG, guías y anexos complementarias, el componente establecido para el tema en el Modelo Estándar de Control Interno -MECI, la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad de la información - Versión 5 emitida por el Departamento Administrativo de la Función Pública - DAFP, Plan Institucional de Gestión Ambiental AGI-TIC-MA-002 y guía GTC 45 versión 2012.

3. DEFINICIONES

3.1. ACTIVO: Cualquier elemento que tiene valor para la organización, tales como elementos aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización en ejecución de sus funciones. La norma ISO/IEC 27000, define los siguientes tipos de activos: información;software, como un programa informático; fisico, como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; e intangibles, como reputación e imagen

3.2. ACTIVO DE INFORMACIÓN: Conocimiento o información que tiene valor para la organización.

3.3. ADMINISTRACIÓN DEL RIESGO: un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

3.4. AMENAZA: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.

3.5. AUTOCONTROL: la capacidad que tiene cada servidor público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades.

3.6. AUTOGESTIÓN: proporcionar una estructura de control de la gestión que especifique los elementos y parámetros necesarios para construir y fortalecer el Sistema Institucional de Control Interno -SICI.

3.7. AUTORREGULACIÓN: son todas las iniciativas que adopta la organización para regularse a sí mismas, mediante la fijación de estándares supervisiones y metas para poder reducir la contaminación.

3.8. AUTOEVALUACIÓN: proceso periódico, en el cual participan los servidores (colaboradores de la Entidad) que dirigen y ejecutan los procesos, programas y/o proyectos, según el grado de responsabilidad y autoridad para su operación.

3.9. CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

3.10. COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO - CICCI: Reglamentado en el MinTIC/Fondo Único de TIC, mediante la Resolución 033 de 2020.

3.11. 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

3.12. CONTEXTO EXTERNO: Ambiente externo en el cual la organización busca alcanzar sus objetivos.
3.13. CONTEXTO INTERNO: enfoque centrado en los aspectos que impactan directamente los objetivos del Ministerio
3.14. CONTEXTO DEL PROCESO: determina las características o aspectos esenciales del proceso y sus interrelaciones, teniendo en cuenta el nuevo modelo de operación por procesos
3.15. CONTROL: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
3.16. CONTROL DETECTIVO: Control que está diseñado para identificar un evento o resultado no previsto después de que se haya producido.
3.17. CONTROL PREVENTIVO: Control que está diseñado para evitar un evento no deseado en el momento en que se produce.
3.18. CONTROL CORRECTIVO: Aquellos que permiten, después de ser detectado el evento no deseado, el restablecimiento de la actividad.
3.19. DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
3.20. EVENTO: Ocurrencia o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000:2009]. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un "incidente" o "accidente".
3.21. EVENTO MATERIALIZADO: situación que evidencia la materialización del riesgo.
3.22. ESTABLECIMIENTO DEL CONTEXTO: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.
3.23. FACTOR DE RIESGO: toda característica proveniente del contexto cuya presencia o comportamiento incide en una mayor o menor probabilidad de materialización de una o varias causas asociadas a uno o varios riesgos.
3.24. FACTORES DE RIESGO DE FRAUDE: hechos o circunstancias que indiquen la existencia de un incentivo o elemento de presión para cometer fraude o que proporcionen una oportunidad para cometerlo.
3.25. FRAUDE: un acto intencionado realizado por una o más personas de la dirección, los responsables del gobierno de la entidad, los empleados o terceros, que conlleve la utilización del engaño con el fin de conseguir una ventaja injusta o ilegal.
3.26. FUENTES DE RIESGO EXTERNAS: son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.
3.27. GESTIÓN DEL RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
3.28. IDENTIFICACIÓN DEL RIESGO: etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias
3.29. INFORMACIÓN (ISO 9001): Datos que poseen significado.
3.30. IMPACTO: Se define como un resultado de los efectos de un proyecto, y la determinación que este exige el establecimiento de objetivos operacionales que permita vincular el proyecto con los efectos resultantes de su implementación.
3.31. LÍDER O RESPONSABLE DEL PROCESO:: persona con la responsabilidad y autoridad para gestionar un riesgo.
3.32. LÍNEAS DE DEFENSA DEL SICI: Esquema de responsabilidades del SICI, que proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionadas.
3.33. MAPA DE RIESGOS: documento con la información resultante de la gestión del riesgo.
3.34. MAPA DE RIESGOS INSTITUCIONAL: contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos (políticas operativas/procesos- Código de buen gobierno)
3.35. MAPA DE RIESGOS POR PROCESO: facilita la elaboración del mapa institucional, que se alimenta de éstos, teniendo en cuenta que solamente se trasladan al institucional aquellos riesgos que permanecieron en las zonas más altas de riesgo y que afecten el cumplimiento de la misión institucional y objetivos de la entidad.
3.36. MODELO ESTÁNDAR DE CONTROL INTERNO (MECI): Proporcionar una estructura de control de la gestión que especifique los elementos necesarios para construir y fortalecer el Sistema de Control Interno, a través de un modelo que determine los parámetros necesarios (autogestión) para que las entidades establezcan acciones, políticas, métodos, procedimientos, mecanismos de prevención, verificación y evaluación en procura de su mejoramiento continuo (autorregulación), en la cual cada uno de los servidores de la entidad se constituyen en parte integral (autocontrol).
3.37. PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal
3.38. PARTE INVOLUCRADA: persona u organización que puede afectar o verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Probabilidad: se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
3.39. PROBABILIDAD: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad
3.40. 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.
3.41. RIESGOS DE CUMPLIMIENTO: se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
3.42. RIESGOS 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 que afecta la confidencialidad, integridad o disponibilidad de la información.
3.43. RIESGO ESTRATÉGICO: se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
3.44. RIESGOS FINANCIEROS: se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
3.45. RIESGOS DE IMAGEN: están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
3.46. RIESGOS OPERATIVOS: comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
3.47. RIESGO DE GESTIÓN: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencia
3.48. RIESGO RESIDUAL: : Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
3.49. RIESGO DE SEGURIDAD DIGITAL: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas
3.50. RIESGOS DE TECNOLOGÍA: están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
3.51. SISTEMA DE INFORMACIÓN DEL MIG – SIMIG: Herramienta del MIG en la cual se gestiona y presenta la información relacionada con el enfoque de procesos del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, tales como: indicadores de gestión, riesgos, acciones de mejora, producto no conforme, documentación controlada de los procesos, entre otros.
3.52. SISTEMA INSTITUCIONAL DE CONTROL INTERNO -SICI: Estructurado bajo el MECI, es el conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y de los recursos, se lleven a cabo de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas

trazadas por la alta dirección y en atención a las metas u objetivos previstos.

3.53. STAKEHOLDERS: son las personas y las organizaciones quienes pueden ser afectadas, afectan o perciben que ellos mismos pueden ser afectados por una decisión o actividad. Se conocen también como "Partes Interesadas".

3.54. TOLERANCIA AL RIESGO: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

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

3.56. FUENTE DE AMENAZA: Se define como cualquier circunstancia o evento con el potencial para causar daños a un sistema o a una organización. Las fuentes comunes de amenazas de interrupción son las siguientes: • Amenazas naturales: Inundaciones, terremotos, deslizamientos de tierras, tormentas eléctricas y otros eventos similares. • Amenazas humanas: Eventos activados o causados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial). Incluye situaciones de alteración del orden público. • Amenazas ambientales: Eventos asociados a la polución, dispersión de líquidos y cambio climático (Escasez de recursos naturales) y enfermedades virales. • Amenazas Tecnológicas: Faltas prolongadas de energía eléctrica, fallas en hardware y fallas en redes de comunicaciones.

3.57. INTERRUPCIÓN: Evento bien sea anticipado o no anticipado, el cual causa una alteración no planeada, desviación negativa de la expectativa de entrega de productos o servicios de acuerdo con los objetivos organizacionales.

3.58. RIESGO DE INTERRUPCIÓN: Corresponde al evento de interrupción que se generaría por la no disponibilidad de algún activo de información, afectando las actividades del proceso. Lo anterior a causa de fuentes internas o externas.

3.59. 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.

3.60. 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: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas 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.

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

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

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

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

3.65. FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

3.66. 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.

3.67. 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.

3.68. 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.

3.69. 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.

3.70. 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 C340-07)

3.71. 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.

3.72. 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.

3.73. RECURSO PÚBLICO: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

3.74. 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.

3.75. 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.

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

3.77. TOLERANCIA DEL RIESGO: : Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

4. NORMATIVIDAD

Le aplican a este lineamiento el siguiente orden por jurisprudencia normativa:

Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011).]. En su artículo 2º, numeral f, establece dentro de uno de los objetivos del Sistema de Control Interno está la de definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presentan en la organización y que puedan afectar el logro de sus objetivos.

Ley 489 de 1998. Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno. En su artículo 27 crea el Sistema Nacional de Control Interno [6], conformado por el conjunto de instituciones, instancias de participación, políticas, normas, procedimientos, recursos, planes, programas, proyectos, metodologías, sistemas de información y tecnología aplicable, inspirado en los principios constitucionales de la función administrativa cuyo sustento fundamental es el servidor público.

Ley 1474 de 2011. Estatuto Anticorrupción. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción, y la efectividad del control de la gestión pública. Artículo 73. Plan Anticorrupcción y de Atención al Ciudadano.

Ley 1712 de 2012. Por la cual se crea la Ley de transparencia y del Decreto de Acceso a la Información Pública Nacional. Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales"

Decreto 1537 de 2001. Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del estado. El parágrafo del Artículo 4º señala los objetivos del sistema de control interno (...) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones (...) y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (...) que se enmarca en cinco tópicos (...) valoración de riesgos. Así mismo establece en su Artículo 4º la administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas

Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, Decreto Único Sectorial de Función Pública. Regula la organización de las Oficinas de Control Interno, su rol. Actualiza lo relativo al Comité Institucional de Coordinación de Control Interno en las entidades de la Rama Ejecutiva del orden nacional frente a las nuevas tendencias internacionales en materia de auditoría interna. Que como consecuencia del cambio de autoridad nominadora dada con la Ley 1474 de 2011, imparte directrices que permitan la interacción efectiva del Jefe de Control Interno. Actualiza el Título 25 de la Parte 2 del Libro 2 sobre el Premio Nacional de Alta Gerencia y el Banco de Éxitos conforme a las mejores prácticas internacionales.

Decreto 1499 de 2017. Por el cual modifica parcialmente 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.

Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción. Artículo 2 Objetivos del control interno: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. 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.

Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción. Decreto 2593 del 2000. Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.

Resolución 033 de 2020. Por la cual se conforma el Comité Institucional de Coordinación de Control Interno del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones. Define funciones para aprobación de la política de administración del riesgo, dar lineamiento sobre la administración de los riesgos y hacer seguimiento, en especial, a la prevención, detección de fraude y mala conducta.

Resolución 924 de 2020. Por la cual se adopta la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las comunicaciones y se definen lineamientos frente al uso y manejo de la información y deroga la Resolución 2007 de 2018.

Resolución 4870 de 2023.Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las comunicaciones/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2175 de 2022 y sus modificatorias.

Resolución 0448 de 2022. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se derogan la Resolución 2256 de 2020.

Norma Técnica Colombiana ISO 31000:2018. Describe los principios y directrices para la gestión del Riesgo de manera sistemática, transparente, creíble para cualquier alcance y contexto de una organización.

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5. Departamento Administrativo de la Función Pública - DAFP. - Diciembre de 2020.

Guía de estrategias para la construcción del plan anticorrupción y de atención al ciudadano. 2015. Departamento Administrativo de la Función Pública - DAFP.

CONPES 3854 de 2016, Política Nacional de Seguridad Digital.

CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital.

Modelo de Seguridad y Privacidad de la Información -MinTIC. Conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información.

LEY No. 2195 DE 2022. Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. Artículo 31. programas de transparencia y ética en el sector público.

5. DOCUMENTOS ASOCIADOS

- Activos de Información
- Manual de Activos de Información
- Gestión de Incidentes de Seguridad y Privacidad de la Información
- Gestión de Incidentes
- Plan Institucional de Gestión Ambiental (PIGA 2021-2024)
- Formulación, seguimiento y cierre de acciones de mejora
- Identificación de Peligros y Valoración de Riesgos Ocupacionales
- Gestión del Riesgo de Desastres- Plan de Emergencias MinTIC
- Investigación de Accidentes e Incidentes
- Manual del MIG
- Manual de Planeación Estratégica del Mintic-Futic
- Metodología de Gerencia de proyectos
- MIG-TIC-FM-022 Establecimiento del Contexto de Proceso.
- Mapa de riesgos de corrupción del proceso
- Formato Mapa de Riesgos SPI
- Manual del Sistema de Gestión Ambiental
- Procedimiento para la identificación de aspectos y valoración de impactos ambientales

Del listado maestro de documentos externos:

Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG - Vigente emitido por Departamento Administrativo de la Función Pública.

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Vigente emitido por Departamento Administrativo de la Función Pública.

Guía de estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Vigente emitido por Departamento Administrativo de la Función Pública

Guía de Fundamentos para la Dirección de Proyectos PMBOK Sexta edición.

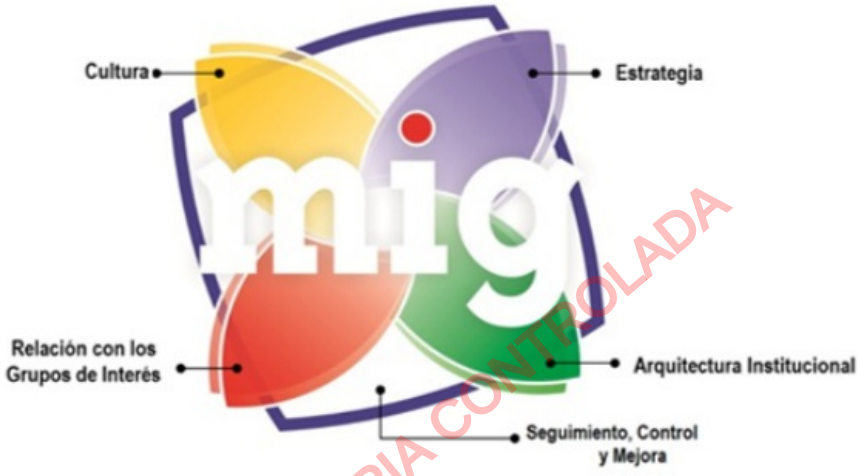
Instituto Colombiano de Normas Técnicas y Certificación- ICONTEC. (2018) Norma Técnica Colombiana NTC-ISO 31000:2018. Gestión del Riesgo. Principios y Directrices. Bogotá Colombia.

6. DESARROLLO

ALINEACIÓN DEL MODELO INTEGRADO DE GESTIÓN CON LA ADMINISTRACIÓN DEL RIESGO

El Modelo Integrado de Gestión MIG, es la estrategia utilizada por el Ministerio TIC para responder a los retos y exigencias del desarrollo organizacional en las entidades públicas. Su diseño, implementación y proceso de mejora, permite cumplir los requisitos de los diferentes sistemas de gestión que la administración pública exige.

Mediante la Resolución 4078 de 2023, se encuentra conformado el modelo y en él se distinguen cinco (5) dimensiones como lo expresa la figura.



A continuación, se describen las dimensiones en las cuales se aplica la administración del riesgo dentro de la Entidad:

***Dimensión Estrategia**

El Plan de Acción del Ministerio TIC, como elemento principal para establecer la estrategia y hacer seguimiento al cumplimiento de las metas de la Entidad, se sustenta bajo un análisis de riesgos a nivel de las iniciativas asociadas al Plan de Acción, registrado en el Aplicativo de Seguimiento al Plan de Acción – ASPA y en la Gerencia de Proyectos. El despliegue del análisis de los riesgos para la estrategia se realiza de forma anual, al plantear o actualizar las metas por iniciativa estratégica.

***Dimensión Cultura**

Desde la dimensión cultura a través de espacios de apropiación y formación en la gestión de los riesgos, se programan capacitaciones y mesas de trabajo a los colaboradores de la Entidad orientadas hacia Administración de Riesgos para fortalecer sus conocimientos y habilidades en la gestión de los riesgos.

***Dimensión Arquitectura Institucional**

Bajo la arquitectura de procesos, el Ministerio TIC establece los riesgos operativos asociados al cumplimiento de los objetivos de cada uno de los procesos establecidos dentro del mapa de macroprocesos de la Entidad. La administración de riesgos se realiza bajo la metodología establecida tanto en la Guía para la Administración del Riesgo de la Función Pública en el marco de la ISO 31000:2011 y en la Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República. La información derivada de la aplicación de estas metodologías se registra dentro de los respectivos procesos de la Entidad.

***Dimensión de Relación con Grupos de Interés**

Teniendo en cuenta los lineamientos definidos en Guía de estrategias para la construcción del plan anticorrupción y de atención al ciudadano, se divulga la propuesta del Mapa de Riesgos de Corrupción como ejercicio de participación en el marco de la elaboración del Plan Anticorrupción y de Atención al Ciudadano de la Entidad.

***Dimensión Seguimiento, Control y Mejora**

El conocimiento y apropiación de la política de administración del riesgo, la identificación de riesgos institucionales, el establecimiento, aseguramiento de controles, así como su seguimiento (visualizado en el mapa de riesgos), evitando así la materialización de los riesgos, se realizan aplicando los parámetros de esta dimensión ejerciendo el autocontrol y la autogestión, por medio de los Grupos Comités Primarios -GCP.

Por otra parte, y en desarrollo de su labor a través de los siguientes roles: Liderazgo estratégico, enfoque hacia la prevención y evaluación de la gestión del riesgo, la Oficina de Control Interno de la entidad realiza asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación y Estudios Sectoriales, monitoreo de la exposición de la entidad al riesgo, seguimiento a la implementación de la metodología de análisis de los riesgos y la pertinencia de los mismos con respecto a los objetivos de los procesos, proyectos y plan de acción de la entidad y realiza recomendaciones con alcance preventivo y sobre las responsabilidades en materia de riesgos.

7. CULTURA EN MATERIA DE ADMINISTRACIÓN DEL RIESGO

Es fundamental desarrollar al interior del MINTIC la cultura en materia de administración del riesgo, para esto, el Grupo Interno de Trabajo de Transformación

Organizacional debe definir y aplicar estrategias que promuevan la participación de los colaboradores de la Entidad en la identificación, medición y control de los riesgos. Desde la dimensión de Cultura del Modelo Integrado de Gestión a través de espacios de apropiación y formación en la gestión de los riesgos, se programan capacitaciones y mesas de trabajo a los colaboradores de la Entidad orientadas hacia Administración de Riesgos para fortalecer sus conocimientos y habilidades en la gestión de los riesgos.

8. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO

Para realizar un correcto análisis, valoración verificación y/o supervisión del riesgo que permita mitigar efectivamente los riesgos identificados, la entidad cuenta con su Sistema Institucional de Control Interno -SICI, bajo el MECI, modelo que contempla dos (2) elementos fundamentales, que trabajan de manera simultánea y articulada:

El primero, es una estructura de control basada en el esquema de COSO/INTOSAI, por 5 componentes, 17 principios y 81 requerimientos; resaltando el componente de Evaluación del Riesgo y sus 4 principios:

El segundo, es un esquema de asignación de roles y responsabilidades integradas por cuatro líneas de defensa, el cual se centra en la contribución para la gestión de riesgos hasta la obtención de objetivos, la creación, protección e incremento del valor público. Bajo este marco metodológico, las responsabilidades de la gestión de riesgos y del control están distribuidas en varias dependencias y no se concentran en la Oficina de Control Interno:

Línea Estratégica: Esta línea al ser una instancia decisoria dentro del SICI, está conformada por la Alta Dirección (Ministra y Grupo Directivo), el Comité Institucional de Coordinación de Control Interno –CICCI, el Comité Directivo y el Comité MIG. Su responsabilidad 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. Lo anterior enmarcado en la "Autorregulación" y le corresponde en materia de riesgo:

- Definir el marco general para la gestión del riesgo (política de administración del riesgo) y efectuar evaluación desde su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo y riesgos emergentes.
- Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, a través de la "Autorregulación".
- Verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea de defensa sea adecuada frente al logro de objetivos y metas estratégicos.
- Monitorear permanentemente los riesgos de corrupción.

- Monitorear al estado de los riesgos aceptados (apetito por el riesgo), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.
- Riesgos relacionados con el manejo de información clasificada o reservada.
- Verificación del avance y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones de la segunda línea de defensa.

Alta Dirección - Comité institucional de coordinación de control interno

Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad y evaluar su aplicación.

- Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.
- Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.
- Evaluar el estado del sistema de control interno, acorde con la información generada por parte de las instancias de 2ª línea identificadas y la actividad de control definida que materializa la línea de reporte en cada caso, acorde con el tema del cual son responsables, a fin de generar acciones y una toma de decisiones con enfoque preventivo.

Comité MIG (Comité de Gestión y Desempeño Institucional)

Asegurar la implementación y articulación de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales.

- Generar recomendaciones de mejora a la política de administración del riesgo para su inclusión y aprobación en el Comité Institucional de Coordinación de Control Interno.
- Realizar seguimiento y análisis periódico a los riesgos institucionales y proponer mejoras a su estructura.

Primera Línea de Defensa: Esta línea del SICI está bajo la responsabilidad principalmente de todos los Líderes de Programas y Proyectos y los Líderes y Gestores de Procesos, junto con sus equipos de trabajo, servidores en sus diferentes niveles. Se debe precisar que cuando se trate de cargos de responsabilidad (jefe, coordinadores) dentro de la estructura organizacional, aplican controles de gerencia operativa. Esta línea se encarga del mantenimiento efectivo de los controles, por consiguiente, identifica, evalúa, controla y mitiga los riesgos. Todo enmarcado a través del "Autocontrol" y le corresponde en materia de riesgo:

- La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.
- La generación de reportes periódicamente al CICCI, acerca del cumplimiento de la gestión integral del riesgo.
- Revisión de las exposiciones al riesgo con los grupos de interés o valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico).
- Verificación del diseño y ejecución de los controles que mitigan los riesgos estratégicos o institucionales.
- Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad.
- Verificación de que los responsables estén ejecutando los controles, tal como han sido diseñados.
- Verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción.
- Verificación del diseño y ejecución de los controles que mitigan los riesgos de fraude y corrupción.

Líderes de Procesos - Responsable del proyecto -Servidores en general

- Identificar y valorar los riesgos que pueden afectar el proceso, los programas, proyectos, planes y procedimientos a su cargo y actualizarlo cuando se requiera.
- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
- Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
- Informar a la Oficina Asesora de Planeación o quien haga sus veces (como 2ª línea de defensa) sobre los riesgos materializados en los procesos, programas, proyectos y planes a su cargo. En caso de la materialización de un riesgo no identificado, este debe ser incluido en el mapa de riesgo del proceso correspondiente.
- Establecer y aplicar las acciones de mejora requeridas frente al mapa de riesgos correspondiente, una vez se genera el informe de materialización del riesgo.

Segunda Línea de Defensa: Esta línea del SICI está bajo la responsabilidad, principalmente, del Jefe de la OAPES, Coordinadores de los Grupos Internos de Trabajo, Líderes de Sistemas de Gestión, Comité de Compras y Contratación, Subdirectores y Coordinadores de Contratación, Financiera y de TIC y sus equipos de trabajo., Esto le permite a la entidad hacer un seguimiento y/o autoevaluación permanente de la gestión de riesgos, de manera que pueda orientar y generar alertas a la 1ª línea de defensa, así como a la Línea Estratégica, todo lo anterior enmarcado en la "Autogestión" y le corresponde en materia de riesgo:

- Definir los objetivos con suficiente claridad para identificar y evaluar los riesgos relacionados: i) Estratégicos; ii) Operativos; iii) Legales y Presupuestales; iv) De Información Financiera y no Financiera.
- Identificación y análisis de riesgos (Analiza factores internos y externos; Implica a los niveles apropiados de la dirección; Determina cómo responder a los riesgos; Determina la importancia de los riesgos).
- Identificación y análisis de cambios significativos (Evalúa los cambios en el entorno externo; Evalúa cambios en la Alta Dirección)
- Evaluación del riesgo de fraude o corrupción. (Tiene en cuenta distintos tipos de fraude o corrupción; evalúa los incentivos y las presiones; evalúa las actitudes y justificaciones).
- Diseño, desarrollo y monitoreo de actividades de control (Integra el desarrollo de controles con la evaluación de riesgos; tiene en cuenta a qué nivel se aplican las actividades; facilita la segregación de funciones).
- Elaboración de autoevaluaciones de la gestión del riesgo de la entidad, de forma integral, con énfasis en: i) La exposición al riesgo, acorde con los lineamientos y la política institucional. ii) El cumplimiento legal y regulatorio. iii) Logro de los objetivos estratégicos o institucionales. iv) Confiabilidad de la información financiera y no financiera. v) Evaluación de la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora.
- Comunicación de las deficiencias oportunamente, generadas de los resultados de las autoevaluaciones de la gestión del riesgo de la entidad.
- Monitoreo de las acciones que subsanan las deficiencias detectadas, producto de las autoevaluaciones de la gestión del riesgo de la entidad, que encaminen a la mejora continua.
- Adicionalmente, asegura que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente,
- Asegura la implementación y eficacia de las prácticas de gestión de riesgo, ejercicio que implicará la implementación de actividades de control específicas que permitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos **.**

rmitan adelantar estos procesos de seguimiento y verificación con un enfoque basado en riesgos.

Oficina Asesora de Planeación

- Asesorar a la línea estratégica en el análisis del contexto interno y externo, para una adecuada definición de la política de administración del riesgo, el establecimiento de los riesgos al proceso de Direccionamiento acorde con el esquema de procesos actual, o bien el que lo actualice o sustituya cuando existan cambios en dicho esquema de operación.
- Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el CICCI y se adelanten los ajustes que correspondan a este aparte dentro de la presente política.
- Consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo periódicamente (establecer una periodicidad concreta) ante la Línea Estratégica para su análisis y toma de decisiones correspondiente.
- Informar a la 1ª línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado para que sea identificado e incluido en el mapa de riesgo del proceso correspondiente.

Oficial de Seguridad de la Información

- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de la Información en la entidad.
- Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información.
- Supervisar la respuesta a incidentes sobre violaciones de la seguridad, informando a la Línea Estratégica sobre sus consecuencias y acciones implementadas.
- Generar informes (establecer una periodicidad concreta) sobre fugas de información y los medios externos identificados.
- Proponer a la Línea estratégica medidas y mecanismos para mejorar la gestión de seguridad de la información.

Secretaria General en articulación con el Coordinador de Contratos

- El coordinador de contratos mensualmente, consolida los avances del Plan Anual de Adquisiciones, de acuerdo a cada modalidad de contratación, generando alertas en semáforo frente a retrasos o posibles incumplimientos en los planes, programas o proyectos a los cuales se encuentran asociados los contratos analizados. La fuente para el análisis se basa en los informes de supervisión o interventoría (según corresponda) de los contratos en ejecución.
- El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión de recursos.

Secretaria General en articulación con el Coordinador de Talento Humano

- El coordinador de TH, bimestralmente consolidará el avance sobre PIC, Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral, conflictos internos que no ha sido posible resolver y aquellos que llegan a instancia disciplinaria.
- El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión del Talento Humano.

Coordinador de Servicio al Ciudadano

- El coordinador del Grupo de Servicio al Ciudadano trimestralmente, evalúa la prestación del servicio a los grupos de valor, mediante el análisis de las PQRD y la evaluación de percepción de los usuarios por los diferentes medios de atención, generando alertas en semáforo sobre incumplimiento en términos, reiteraciones de consultas, quejas, denuncias y tutelas que se hayan presentado o que estén en curso. La fuente para el análisis es el sistema ORFEO y el sistema que consolida las encuestas de satisfacción aplicadas a los grupos de valor.
- El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Coordinador de Servicio al Ciudadano como líder del proceso de gestión del Servicio al Ciudadano.

Director Jurídico en articulación con el Coordinador Grupo Defensa Jurídica

- El coordinador del Grupo de Defensa Jurídica mensualmente, verifica el seguimiento a la gestión judicial adelantada por los abogados asignados, generando información sobre alertas en los procesos que se encuentran abiertos y las cuantías asociadas. La fuente de información es el sistema para la consulta de procesos de la Rama Juridicial, el sistema e-Kogui y los informes de los abogados responsables.
- El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Director Jurídico como líder del proceso de Defensa Jurídica.

Jefe de oficina de tecnologías de la información y las comunicaciones TIC en articulación con el Grupo de proyectos estratégicos de TIC

- El Jefe de oficina TIC mensualmente verifica el avance en los programas y proyectos desagregados por tema y recursos asociados, generando alertas sobre retrasos o posibles incumplimientos, a fin de tomar las acciones o intervenciones necesarias. La fuente para el análisis son los informes de los supervisores o interventores de los programas a proyectos (según corresponda).
- El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Jefe de TIC como líder del proceso de Tecnologías de la Información.

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 la 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de la 1ª línea de defensa que no se encuentren cubiertos, a través de los siguientes roles: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento y le corresponde en materia de riesgo:

- Da asesoría proactiva y estratégica a la Línea Estratégica y a la Primera Línea de Defensa del SICI, sobre las responsabilidades en materia de riesgos y control interno.
- Formar a la Línea Estratégica del SICI y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.
- Efectuar evaluaciones independientes que permiten determinar si se han definido, puesto en marcha y aplicado los controles establecidos por la entidad de manera efectiva. Su frecuencia depende de la importancia y respuesta al riesgo y de los resultados de las evaluaciones continuas o las autoevaluaciones de la entidad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Monitorea la exposición de la entidad al riesgo y realiza recomendaciones con alcance preventivo para mejorar la eficiencia y eficacia de los controles.
- Proporcionar seguridad razonable con respecto al diseño e implementación de políticas, procedimientos y otros controles.
- Evaluar si los procesos de gobierno de TI de la entidad apoyan las estrategias y los objetivos de la entidad.
- Proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos y, según sea apropiado, puede recomendar mejoras a las actividades de control específicas.
- Realizar seguimiento a las acciones establecidas para el mejoramiento de la administración del riesgo y emitir informes periódicos teniendo en cuenta los lineamientos que defina para ello el Gobierno Nacional.

- Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.
- Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías internas.
- Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.
- Informar al Comité Institucional de Coordinación de Control Interno sobre los cambios que podrían tener un impacto significativo en el SCI, identificados durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.
- Ejercer el rol de evaluación de la gestión del riesgo.
- Verificar y analizar que las actividades de control son una herramienta que garantiza la mitigación de riesgos, para la consecución de los objetivos estratégicos y de proceso.
- Verificar que los controles estén diseñados e implementados de manera efectiva y operen efectivamente para controlar los riesgos.
- Evaluar si los controles están presentes y funcionan adecuadamente para mitigar los riesgos.
- Comunicar a la Primera y la Segunda Línea de Defensa, aquellos aspectos que se requieren fortalecer relacionados con la información y comunicación de la administración de los riesgos.

Jefe Oficina Asesora de Control Interno o quien haga sus veces

- Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional Coordinador de Control Interno. Para esto tendrá en cuenta los resultados de los seguimientos aplicados por parte de la Oficina Asesora de Planeación, así como del oficial de seguridad, a fin de contar con información de base para sus evaluaciones y generar recomendaciones a estas instancias.
- Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados.
- Asesorar y acompañar a toda la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos corrupción, fiscales, de lavado de activos y otros que se definan en normas nacionales.

9. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Compromiso frente al Riesgo:

El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos, en las actividades desarrolladas por la Entidad asociadas con la responsabilidad de diseñar, adoptar, ejecutar y promover las políticas**,** planes, programas , iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados, de manera Integral, con la estrategia, la gestión, la transparencia y la ética, seguridad y privacidad de la información, seguridad digital y continuidad de la operación, riesgo fiscal aspectos ambientales y de seguridad y salud en el trabajo, que puedan afectar el cumplimento de los objetivos institucionales, el aprovechamiento al máximo los recursos destinados y la atención a nuestros grupos de interés.

10. ADMINISTRACIÓN DE RIESGOS

10.1 ADMINISTRACIÓN DE RIESGOS DE GESTIÓN

10.1.1. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, a través de su Modelo Integrado de Gestión, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, para de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

10.1.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

Las acciones que se tomarán en el desarrollo de esta política son:

- Regular los riesgos de los procesos mediante la administración de las acciones preventivas orientadas a reducir, evitar, asumir, compartir o transferir el riesgo, a fin de mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos.
- Generar estrategias para el monitoreo y revisión de la administración de riesgos, con el propósito que la Alta Dirección tome decisiones para la mejora continua del Modelo Integrado de Gestión y su articulación con el Modelo de Responsabilidad Institucional.
- Desarrollar al interior de la entidad una cultura organizacional que genere una gestión más preventiva y menos correctiva.
- Realizar la revisión o revaloración del riesgo como mínimo una vez al año.
- Las acciones formuladas para mitigar los eventos de riesgo deberán tener una vigencia máxima de un año y solo podrán ser cerradas si se ha cumplido con el total de actividades propuestas y cumple con lo mencionado en el MIG-TIC-PR-003 Formulación, seguimiento y cierre de acciones de mejora. En el caso de que no sea posible la mitigación dentro de la vigencia indicada anteriormente, será el Comité MIG tras una evaluación quién tome la decisión de prolongar las acciones de tratamiento de los riesgos.
- Verificar que los planes de mejoramiento derivados de la administración de riesgos (planes de tratamiento de riesgo, y acciones de mejora por eventos de riesgo materializados) tengan una vigencia máxima de un año y sean gestionados y cerrados en este período.
- Revisar y/o actualizar por lo menos una vez al año la política de gestión de riesgos.
- Generar y revisar los indicadores de gestión de los riesgos definidos en los procesos del sistema integrado de gestión mínimo una vez al año y actualizarlos cada vez que se requiera.

10.1.1.2. ALCANCE DE LA POLÍTICA

La política de riesgos es aplicable a todos los procesos que hacen parte del Sistema Integrado de Gestión del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones

10.1.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido que para los riesgos de gestión del Ministerio el nivel de aceptación se aplica a todos los riesgos que se ubiquen a nivel residual en una zona de riesgo bajo y moderado, ya que los controles son suficientes y el nivel de riesgo sería aceptable.

10.1.1.4. NIVELES PARA CALIFICAR LA PROBABILIDAD

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

Para la calificación de la probabilidad de los riesgos de gestión se establecen los siguientes 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%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10.1.1.5. NIVELES PARA CALIFICAR EL IMPACTO

Por "impacto" se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. Para la calificación del nivel de impacto se toma como referencia las consecuencias potenciales mencionadas en las siguientes tablas de niveles de impacto para cada tipo de riesgo que se esté calificando. El criterio se adaptará a la realidad del riesgo que se esté calificando.

El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

	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

Fuente: elaborado por el Ministerio TIC, tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5

10.1.1.6. TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Reducir el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación de este.

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

Transferir el riesgo: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

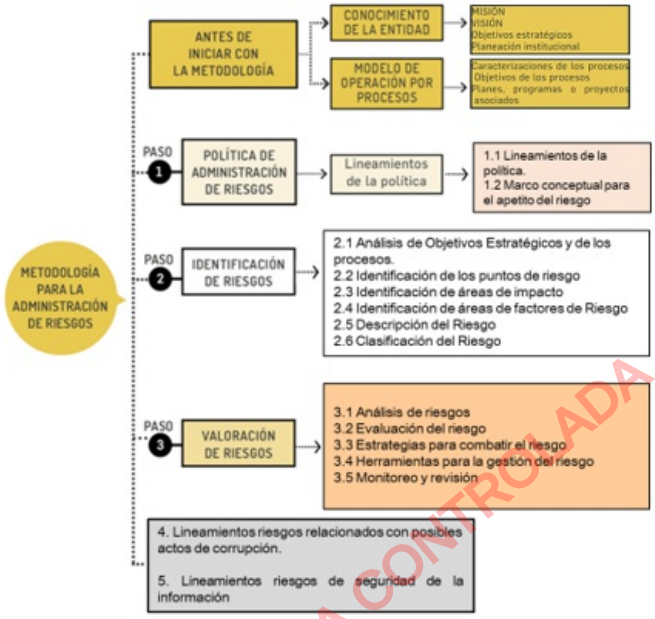
Mitigar: (Plan de Acción) Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

10.1.2. ESTRUCTURA PARA LA GESTIÓN DE RIESGOS

10.1.2.1 ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

En la Administración del riesgo el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones sigue las etapas de identificación, medición, control y monitoreo del riesgo en los procesos, teniendo como referencia Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública (DAFP) y para el manejo de los riesgos previsibles a la contratación pública adopta los lineamientos de la política de riesgos previsibles para la contratación estatal definidos en el Documento Conpes 3714 de 2012, que establece una serie de lineamientos básicos para el entendimiento del concepto de "riesgo previsible" en el marco en el marco de las adquisiciones sometidas al Estatuto General de Contratación de la Administración Pública, así como los instrumentos diseñados por Colombia Compra Eficiente, los cuales se encuentran en uso en el Ministerio para efectos de riesgos en procesos de compra, como instrumento válido.

A continuación, se presentan las etapas para la administración de los riesgos de gestión especificando los lineamientos adicionales que aplican en el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones.



Fuente: elaborado por el Ministerio TIC, tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5

10.1.2.1.1. ESTABLECIMIENTO DEL CONTEXTO

El contexto estratégico define los parámetros internos y externos que se deben tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Teniendo en cuenta que las organizaciones son dinámicas, es necesario analizar los datos históricos, teóricos, opiniones informadas y las necesidades de cada proceso. Para ello el Grupo Interno de Trabajo de Transformación Organizacional dispone de un instrumento para la recolección de la información relacionada con el contexto y la identificación de las partes interesadas que pueden afectar los procesos "Formato para el establecimiento del contexto", en el cual se analizan las siguientes temáticas:

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

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

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

NOTA: Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo. Es una referencia de información general para el Mintic y se alimenta de la información que requieran los diferentes sistemas de gestión para establecer su contexto.

Determinar los factores generadores de riesgos de corrupción (aplica para los riesgos de corrupción): ocasionados entre otras cosas por la misión, por las funciones que desarrolla y el sector al que pertenece la entidad

De acuerdo con lo anterior, el Contexto Estratégico del Ministerio TIC se encuentra enmarcado en los objetivos establecidos por la Ley de modernización TIC, a su vez se llevó a cabo el análisis de la información del Plan Estratégico y sus metas específicas.

	Amenazas	Oportunidades
Contexto Externo	*Cambios en las políticas de gobierno *Cambios en la normatividad y regulación del sector *Dificultades para la gestión del cambio dentro del gobierno y la población en general hacia la transformación digital. *Limitaciones presupuestarias para llevar a cabo iniciativas *Descentralización de los datos, que genera dificultad para reportes consolidados de los beneficiarios de programas implementados. *Brecha de conectividad digital en los territorios que limita el acceso a la oferta en las diferentes regiones y a diferentes grupos poblacionales *Bajo conocimiento de la oferta institucional en territorios *Falta de oportunidad de reporte de los datos por parte de operadores para la elaboración de los Boletines e informes. *Cambios políticos, económicos o sociales a nivel internacional que pueden afectar la cooperación y las relaciones internacionales, introduciendo incertidumbre en la implementación de proyectos. *Fallas en los aplicativos externos a la Entidad que pueden generar demoras en las gestiones presupuestales *Incumplimiento en las obligaciones y los acuerdos de nivel de servicio por parte de los terceros y/o operadores *Ciberataque, ciberterrorismo, hacktivismo. *Falta de cultura y apropiación en seguridad digital en el sector público y privado. *Bajo porcentaje de transformación digital en el gobierno. *Rotación de personal que genera inconvenientes por la curva de aprendizaje.	*Interés por promover la educación de calidad *Interés del país en la implementación de temas TIC *Desarrollo de nuevas soluciones de conectividad *Aplicabilidad de tecnologías emergentes en los diferentes sectores *Incremento en la demanda de profesionales con habilidades y formación en TIC *Ampliación en la conectividad del país. *Aplicabilidad de tendencias globales en temas TIC *Proyectos TIC con enfoque y relevancia en las regiones apartadas del país. *Promover la expansión de la infraestructura de comunicaciones *Digitalización de servicios. *Incorporación de herramientas tecnológicas que permitan hacer un seguimiento oportuno al cumplimiento de las obligaciones de los PRST, así como para el seguimiento a la planeación y control de los informes de visita y control de las etapas del proceso administrativo sancionatorio, para evitar caducidades. *Expansión en el país del 5G para facilitar el acceso a servicios digitales y promover tanto los procesos formativos de cualificación y el desarrollo económico en todas las regiones del país *Ampliar las alianzas estratégicas con actores que permitan tener una oferta diversa que apoye el crecimiento de la Economía digital del país. *Articulación con otros ministerios para el desarrollo de los programas *Propiciar espacios que faciliten un contacto directo con las comunidades que permitan potencializar su cultura a partir del uso de las TIC como herramienta para su productividad y desarrollo *Obtener mayores fuentes de recursos externos para financiar iniciativas y proyectos. *Acuerdos y convenios con otras Entidades estatales para potenciar la interoperabilidad de los sistemas de información.

	Debilidades	Fortalezas
Contexto Interno	*Falta de sistematización de la base de datos de contratación *Demoras en los procesos de contratación. *Desarticulación entre las iniciativas y proyectos de los Viceministerios que permitan mejorar las capacidades del país en materia TIC *Desarticulación entre los procesos transversales que conlleva al levantamiento reiterado de hallazgos por parte de los entes de control. *Poco uso de tecnologías emergentes, como la inteligencia artificial y robotización que permitan mejorar la eficiencia en diversos procesos y procedimientos *Falta articulación con los medios de comunicación *Insuficiente relación entre el Ministerio TIC y los territorios *Debilidad en la conservación de la información y el conocimiento de los colaboradores de la Entidad. *Falta de conocimiento de los procesos del Ministerio por parte de toda la Entidad. *Bajo aprovechamiento de las lecciones aprendidas de proyectos de vigencias anteriores. *Falta de estudios precisos sobre la caracterización de la población beneficiaria, especialmente en temas de brecha digital. *Falta de un sistema que permita la automatización en la Generación de la información Estadística. *Falta de adecuaciones para atención a la población en condición de discapacidad. *Falta de automatización de procesos *Falta de interoperabilidad en los sistemas de información internos de la Entidad. *Dificultad en la implementación de iniciativas de TI, por resistencia al cambio por parte de los colaborades de la Entidad en la adopción de nuevas tecnologías o procedimientos. *Riesgos relacionados con la calidad del servicio y los tiempos de respuesta por la dependencia de proveedores exclusivos para el soporte técnico y el mantenimiento de sistemas críticos. *Pérdida del gobierno de los datos y los sistemas de información por una alta dependencia con proveedores exclusivos.	*Líder en política TIC *Oferta de proyectos con cobertura nacional y con impacto social significativo. *Formalización y estructuración del equipo de CSIRT gobierno. *Liderar la política de Seguridad Digital y la definición de lineamientos de seguridad de la información a través de la experiencia. *Experiencia y conocimientos sólidos en la regulación de la industria de comunicaciones, lo que permite mantener un marco normativo eficiente y actualizado. *Amplia oferta de iniciativas y proyectos que permiten el fortalecimiento de la economía digital *Posicionamiento frente a instancias nacionales e internacionales como el CERT nacional. *Entidad con reconocimiento y participación en ámbitos internacionales. *red sólida de relaciones internacionales con organismos asociados al sector TIC y otras instancias, lo que facilita la cooperación y el intercambio de experiencias. *Capacidad para liderar iniciativas de innovación tecnológica a nivel gubernamental. *Competencia para generar alianzas estratégicas con actores del sector TIC *Análisis estadísticos a través de la validación de los datos históricos que permiten establecer diagnósticos, tendencias y proyecciones en la dinámica del sector. *Compromiso de la Entidad en la implementación de normas y estándares nacionales e internacionales *Estructura orgánica definida *Infraestructura física centralizada *Instalaciones óptimas *Adecuados procesos de seguridad y privacidad de la información y continuidad de la operación *Personal idóneo con conocimientos y capacidades para el desarrollo de las actividades requeridas por la Entidad *Equipo de alto desempeño con capacidad de innovar *Procesos definidos, estructurados y estandarizados para la entrega oportuna de productos *Alto posicionamiento en la calificación del FURAG para la Entidad *Líderes en la ejecución de recursos financieros dentro del gobierno nacional. *Alineación de la estrategia desde el PND hasta los planes Estratégicos y de Acción. *Contar con los diferentes instrumentos de planeación definidos el decreto 612 de 2018 *Tramites en línea y canales virtuales de atención al ciudadano. *Información clara y transparentes de cara a los grupos de interés.

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido para el análisis de su contexto para sus procesos, así como para el análisis de los riesgos la metodología DOFA (Debilidades – Oportunidades – Fortalezas – Amenazas), la cual consiste en identificar en tiempo real aquellas cuestiones del entorno (contexto externo): amenazas (Factores Negativos Externos) y oportunidades (Factores Positivos Externos) y al interior de la entidad (contexto interno): debilidades (Factores Negativos Internos) y fortalezas (Factores Positivos Internos). Esta actividad se realiza en forma participativa para todos los procesos de la Entidad.

10.1.2.1.2. IDENTIFICACIÓN DEL RIESGO

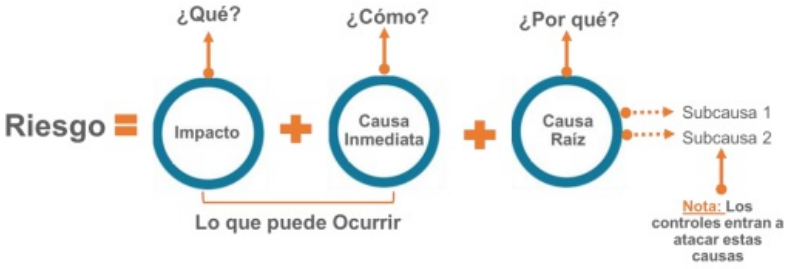
La identificación de riesgos se realiza con base en las actividades clave de éxito para cada proceso, que se enmarcan en la generación de cada uno de sus productos críticos. A estos productos críticos se les identificarán los riesgos de gestión con base en los hallazgos mencionados en los informes de auditorías internas y de la CGR, los eventos materializados de riesgo y otros temas relevantes mencionados en el contexto del proceso.

A partir de la identificación inicial de los riesgos en los procesos, se requiere realizar en forma anual una revisión, a fin de actualizar el perfil de riesgos de la Entidad e integrar los cambios que se hayan presentado en la estructura organizacional o contexto de la Entidad y en sus procesos y procedimientos. El resultado de esa identificación de riesgos quedará registrada en el formato MIG-TIC-FM-024 Formato Mapa de riesgos de gestión del proceso.

Es importante mencionar, que las etapas de Identificación y valoración de los riesgos se realizarán acorde a lo mencionado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 6.

Si durante la identificación de los riesgos o controles, se detecta uno que está fuera del alcance del proceso, pero dentro del alcance de otro proceso de la Entidad, ya sea por cambios de rediseño de la Entidad o por cambios administrativos, se procederá a realizar los ajustes en los mapas de riesgos respectivos.

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



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

Nota: Los riesgos del proceso de Direccionamiento Estratégico serán considerados como los "**Riesgos Estratégicos**" de la Entidad.

10.1.2.1.3. VALORACIÓN DEL RIESGO

La valoración de los riesgos de gestión se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada por el Ministerio para la gestión del riesgo y las tablas de impacto definidas para el Ministerio.

Es así como después de realizar el establecimiento del contexto y la identificación de los riesgos, se procede realizar en mesas de trabajo el análisis de la probabilidad y el impacto de los establecidos como valoración preliminar para generar el valor del riesgo inherente, se identifican sus causas y los controles para mitigar dichas causas. A estos controles se le definen las variables a evaluar para el adecuado diseño de controles como son: la asignación de un responsable, periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. La valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 del DAFP.

	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%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10.1.2.1.4. DEFINICIÓN Y APROBACIÓN DE PLANES DE ACCIÓN

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de gestión de la Entidad, el gestor del proceso procederá a cargar el documento interno llamado “Mapa de riesgos del proceso” para que surta el proceso de aprobación documental por parte del líder y de la Oficina Asesora de Planeación a través de la herramienta SIMIG.

Así mismo se deben clasificar aquellos riesgos cuya calificación residual se encuentren en zona Moderada, Alta o Extrema en el mapa de calor. En estos casos, los procesos en los cuales se obtenga dicha calificación residual deberán formular un plan de acción dentro del mapa de riesgos del proceso tal como lo menciona la Guía para la administración del riesgo emitida por el DAFP. El seguimiento al cumplimiento de las actividades propuestas será llevado para conocimiento al Comité MIG.

10.1.2.1.5. MATERIALIZACIÓN

Con el propósito de realizar una revisión objetiva de la valoración de los controles de los riesgos de gestión identificados, la entidad estimó conveniente diseñar un instrumento mediante el cual se registre dicha información, conformando una base de datos sobre eventos de riesgos materializados, la cual permitirá contar con información de tendencias y causas de aquellos presentados, para controlar la ocurrencia futura de los mismos.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Gestor de Procesos avalado por el Líder de Procesos al buzón MIG@mintic.gov.co, en el cuál debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado (opcionalmente), proceso en donde se identificó el suceso, impacto, acciones adelantadas y consecuencias. Este reporte debe realizarse mensualmente o cuando el evento de riesgo materializado se presente.

Partiendo del análisis de causas del evento materializado se debe formular un plan de mejora que indique la corrección o actividades que indiquen la acción de mitigación del mismo. Sólo para los casos en los cuales ya se tenga un plan de mejora formulado y las acciones correspondan directamente a la mitigación de las causas que motivaron a la materialización del riesgo, se homologará al ya existente y no requerirá formular un nuevo plan de mejora.

El Grupo Interno de Trabajo de Transformación Organizacional, debe validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos, y presentar en los casos requeridos, ante el Comité MIG aquellos que deban ser de su conocimiento, revisión y cierre.

La Oficina de Control Interno podrá reportar eventos materializados de riesgo a través de los informes o evaluaciones de auditoria a los diferentes procesos de la entidad. En tal caso el reporte quedará registrado en la matriz de eventos materializados de riesgo y el proceso deberá formular plan de mejora que indique la corrección y actividades que indiquen la acción de mitigación del mismo de tal forma que prevenga su reiteración en un término no superior a dos meses a partir de la identificación del evento.

10.1.2.1.6. MEDICIÓN

Se realiza medición a los avances en la realización de las actividades programadas para el fortalecimiento y apropiación de los lineamientos de riesgos de gestión a través del indicador de eficacia llamado “Cumplimiento del cronograma de gestión”, el cual se reporta en el aplicativo ASPA de la entidad.

El monitoreo y seguimiento de los riesgos de gestión del Ministerio aprobados por los procesos, así como de sus controles, se realiza por parte del grupo interno de trabajo de Transformación Organizacional, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de los controles y reporten las evidencias de los mismos, los profesionales del grupo interno de trabajo de Transformación Organizacional realizan la revisión y validación de esta información e informarán su oportuna gestión registrando su resultado a través del indicador N.211 llamado “Controles del Sistema Integrado de Gestión gestionados”, reportado en la herramienta SIMIG, que tiene como propósito medir el nivel de cumplimiento en la ejecución de los controles de los riesgos de gestión del Ministerio.

Los procesos que obtengan un rango bajo en la medición del indicador por no gestionar sus controles en la fecha límite informada para su gestión, deberán ir al Comité MIG a explicar las razones de su incumplimiento y formular el plan de mejora que evite que vuelva a suceder.

El Ministerio mantiene una base de datos de eventos materializados de riesgos a los cuales se les mide el cumplimiento de la gestión de los eventos materializados en la entidad mediante el indicador N.229 llamado “Eventos de riesgos que se materializaron gestionados” de manera mensual.

10.1.2.1.8.EXCEPCIONES DE LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS

- Se define como base de identificación de riesgos de gestión, los productos de la cadena de valor más críticos de cada proceso y aquellos hallazgos mencionados en los informes de auditorías internas y de la CGR y los eventos materializados de riesgo
- Un producto es considerado crítico para la entidad si su falta de disponibilidad o su mal funcionamiento tienen un impacto en los siguientes niveles:

Nivel económico y/o reputacional: un producto puede considerarse crítico si su falta de disponibilidad o su mal funcionamiento pueden tener un impacto significativo que representa una pérdida económica y/o reputacional para la entidad y su entrega se realiza en cumplimiento del objetivo del proceso. Ejemplos de productos críticos como incumplimiento de los compromisos y la entrega de productos a los grupos de interés (supervisión de la ejecución contractual), incumplimiento en los trámites, errores y demoras en las operaciones y/o gestión para el cumplimiento del objeto del proceso. La no entrega del mismo puede acarrear pago de sanciones, multas, demandas, inconformidad de los grupos de interés entre otros.

Nivel de dependencia: un producto puede considerarse crítico si hay una alta dependencia de él para la generación de otros productos dentro de la entidad o dentro del mismo proceso, de tal manera que su falta de disponibilidad o su mal funcionamiento pueden tener un impacto significativo en la calidad y entrega de otros productos. Ejemplos de productos críticos en este sentido podrían ser certificados de disponibilidad presupuestal, registros presupuestales puesto que de ellos depende la contratación o la realización de licitaciones entre otros.

Nivel de Regulación: El producto está sujeto a regulaciones gubernamentales estrictas dentro del cumplimiento del objeto del proceso. El producto debe generarse cumpliendo un requerimiento de ley. Cualquier incumplimiento de la ley podrá acarrear a la entidad sanciones económicas y/o impacto reputacional graves.

- Se retiran los riesgos que no se consideren críticos. Los riesgos transversales junto con sus controles se retiran del mapa de riesgos de los procesos.
- Se redacta el control en un párrafo como lo indica la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6, sin embargo, se conserva la hoja de controles con los 6 atributos.
- Los puntos de riesgo: deberán estar mencionados en la carta descriptiva de cada proceso y solo aparecerán en las actividades en donde se realicen, en la casilla "Descripción de la Actividad".
- Se ajusta la descripción de la escala del impacto inherente en el nivel Mayor 80%, mencionando adicionalmente que esta calificación aplica cuando se evidencien eventos materializados de riesgo.
- En cuanto a los riesgos de corrupción se decide: Se mantiene la estructura de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 4.
- En los casos en los cuales el riesgo de PQRSD se hayan visto en la vigencia anterior y la vigencia actual, materializados deberán establecer un indicador para su seguimiento. Esto aplica para aquellos temas de riesgos en el manejo de actividades transversales para la entidad como es la gestión de documentos, manejo de expedientes, cumplimiento en el reporte de indicadores y cumplimiento en lo formulado en los planes de acción, etc.
- Para el caso de las acciones, seguimiento a controles e indicadores la OAPES seguirá realizando los monitoreos y reporte de cumplimiento por parte de las áreas en los resultados del indicador que presenta al Comité MIG.
- Numeración los riesgos: sólo se asignará un nuevo número cuando se establezca un nuevo riesgo al mapa de riesgos del proceso, se aclara que ajustes o precisiones a los riesgos existentes no ameritan una nueva numeración del riesgo. Así mismo se eliminará un riesgo del mapa de riesgos cuando el proceso considere que el producto al cual iba enfocado el riesgo no es crítico o porque el enfoque y productos del proceso cambiaron.
- Valoración Riesgos fiscales: Para aquellos procesos que tengan bajo su supervisión contratistas por contratación de servicios tendrán un impacto bajo y por lo tanto un riesgo residual bajo. Para aquellos procesos que tengan contratos de naturaleza jurídica tendrán un impacto alto, especialmente los identificados para los procesos misionales cuyos contratos tienen montos muy significativos. Por lo anterior deberán definir un plan de acción con mínimo 2 actividades.

10.2. ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción.

Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción.

En materia de riesgos asociados a posibles actos de corrupción la identificación y valoración de los riesgos de corrupción se realizará acorde a lo mencionado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4.

Para los riesgos de corrupción en los trámites se tomará como referente el Anexo 3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios.

En cuanto a los riesgos de fraude se tendrán como referencia para este análisis los conceptos y controles establecidos en la Resolución 193 de 2016 emitida por la Contaduría General de la Nación y su anexo, referente al Control Interno Contable y lo mencionado en la estrategia de convergencia de la regulación contable pública hacia NIIF y NICSP, entre otros.

10.2. ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN

10.2.1 LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Ministerio de Tecnologías de la Información y las Comunicaciones genera un entorno permanente de lucha y cero tolerancia contra la corrupción, integrando sus procesos enfocados a la prevención y detección de hechos asociados a este fenómeno, tomando las medidas necesarias para combatirlo mediante, mecanismos, sistemas y controles adecuados que permiten la prevención, detección y respuesta a estas conductas.

10.2.1.1. OBJETIVO DE LA POLÍTICA

Los objetivos que se espera lograr con la implementación de la política de administración de riesgos de corrupción son:

- Gestionar los riesgos de corrupción procurando que no se materialicen.
- Generar compromiso y cultura frente a la lucha ante las prácticas corruptas.

La estrategia que de esta política es: combinar principios de transparencia activa y transparencia pasiva para evitar la materialización de hechos de corrupción en la Entidad a través de la generación de servidores públicos íntegros y transparentes.

Las acciones que se tomarán en el desarrollo de esta política son:

*Acciones generales:

- El Ministerio de Tecnologías de la Información y las Comunicaciones elaborará un plan Anticorrupción y de atención al ciudadano el cual deberá actualizarse anualmente o con la periodicidad que determine la ley.
- • El Plan Anticorrupción del Ministerio de Tecnologías de la Información y las Comunicaciones estará alineado al Sistema de Administración de Riesgos.
- • El Ministerio de Tecnologías de la Información y las Comunicaciones implementa instrumentos y actividades de prevención, detección y respuesta, así como

para la identificación, valoración, mitigación y control de riesgos de corrupción.
- El Ministerio de Tecnologías de la Información y las Comunicaciones programa actividades de capacitación y divulgación necesarias para fortalecer la cultura de prevención y control de la corrupción.

*Acciones específicas:

Realizar a través de un ejercicio participativo de los líderes de proceso y sus equipos de trabajo la gestión de los riesgos de corrupción.

Elaborar y consolidar el Mapa de Riesgos de Corrupción en el marco de un proceso participativo. Divulgar el mapa de riesgos de corrupción construido para consolidar el plan anticorrupción.

Efectuar el monitoreo y revisar el mapa de riesgo de Corrupción con los líderes de proceso y sus equipos.

Atender lo señalado por la Ley 1474 de 2011 en su artículo 73, la identificación, calificación, clasificación y valoración de los riesgos de corrupción se realizará siempre en el marco de los procesos, por lo cual los lineamientos metodológicos son aplicables para este tipo de riesgos.

Asegurar el seguimiento al Mapa de Riesgos de Corrupción. Esta acción será liderada por la oficina de Control Interno

10.2.1.2. ALCANCE DE LA POLÍTICA

La política de riesgos es aplicable a todos los procesos que hacen parte del Sistema Integrado de Gestión del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones

10.2.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido que los riesgos de corrupción del Ministerio no son aceptables. Por lo anterior los riesgos que a nivel residual queden en zona Moderada, Mayor o Extrema no son tolerables para la entidad.

10.2.1.4. NIVELES PARA CALIFICAR LA PROBABILIDAD

Los criterios para calificar la probabilidad para los riesgos de corrupción son:

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 el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último 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.

10.2.1.5. NIVELES PARA CALIFICAR ELIMPACTO

Acorde a lo mencionado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, para la calificación del impacto de los riesgos de corrupción la Matriz de Riesgos cuenta con un listado de preguntas que determinan el nivel de este.

Si el riesgo de corrupción se materializa podría…

1	¿Afectar al grupo de funcionarios del proceso?
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de misión de la Entidad?
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los 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?

Fuente: Guía para la Administración de los Riesgos de Gestión Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Publicas

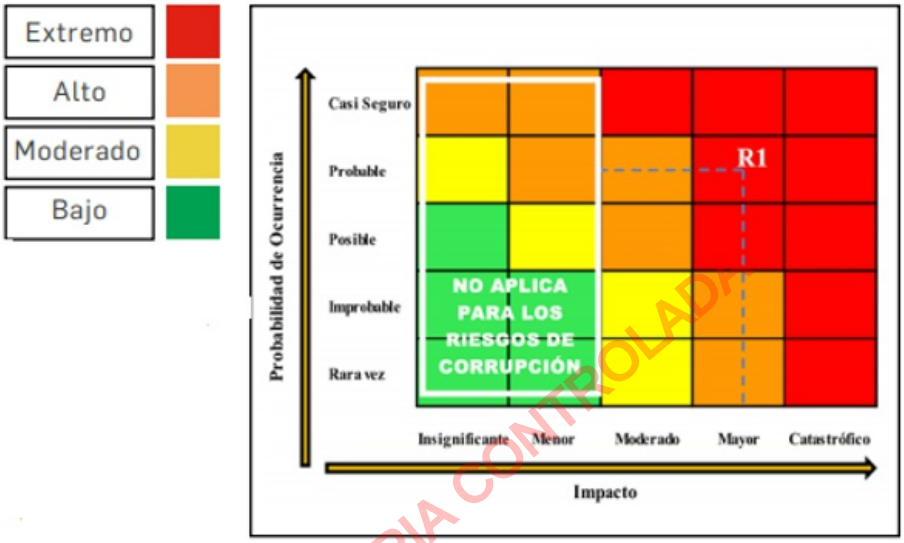
Importante: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla

de estas.

El impacto para los riesgos de corrupción se establece en la Matriz de Riesgos, de acuerdo con el número de respuestas afirmativas frente a las 19 preguntas mencionadas anteriormente, según los siguientes criterios:

RESPUESTAS AFIRMATIVAS	IMPACTO	DESCRIPCIÓN
1-5	Moderado	Afectación parcial al proceso o más procesos Genera medianas consecuencias para la entidad
6-11	Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.
12-19	Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.



10.2.1.5. TRATAMIENTO DE RIESGOS

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Reducir el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

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

Transferir el riesgo: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Mitigar: (Plan de Acción) Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

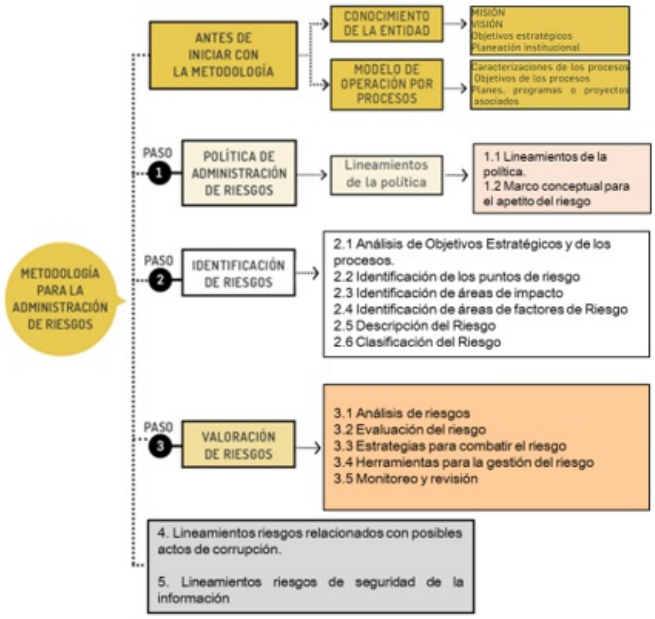
En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo, por ningún motivo para la Entidad se aceptan.

10.2.2. ESTRUCTURA PARA LA GESTIÓN DE RIESGOS

10.2.2.1. ETAPAS EN LA ADMINISTRACIÓN DELRIESGO

En la Administración del riesgo el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones sigue las etapas de identificación, medición, control y monitoreo del riesgo en los procesos, teniendo como referencia la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública (DAFP) y para el manejo de los riesgos previsibles a la contratación pública adopta los lineamientos de la política de riesgos previsibles para la contratación estatal definidos en el Documento Conpes 3714 de 2012, que establece una serie de lineamientos básicos para el entendimiento del concepto de “riesgo previsible” en el marco en el marco de las adquisiciones sometidas al Estatuto General de Contratación de la Administración Pública, así como los instrumentos diseñados por Colombia Compra Eficiente, los cuales se encuentran en uso en el Ministerio para efectos de riesgos en procesos de compra, como instrumento válido.

A continuación, se presentan las etapas para la administración de los riesgos de corrupción que aplican en el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones.



Fuente: elaborado por el Ministerio TIC, tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5

10.2.2.1. ESTABLECIMIENTO DEL CONTEXTO

El contexto estratégico define los parámetros internos y externos que se deben tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Teniendo en cuenta que las organizaciones son dinámicas, es necesario analizar los datos históricos, teóricos, opiniones informadas y las necesidades de cada proceso. Para ello el Grupo Interno de Trabajo de Transformación Organizacional dispone de un instrumento para la recolección de la información relacionada con el contexto y la identificación de las partes interesadas que pueden afectar los procesos, en el cual se analizan las siguientes temáticas:

Contexto Externo: se determinan las características o aspectos esenciales del entorno en el cual opera la Entidad. Se pueden considerar los siguientes factores: Legales, Políticos, Sociales, Tecnológicos, Financieros y Sectoriales. Así como aquellos impulsores claves y tendencias que tengan impacto a la organización, relaciones con las partes involucradas, sus percepciones y valores.

Contexto Interno: se determinan las características o aspectos esenciales del ambiente en la cual la organización busca alcanzar sus objetivos. Se pueden considerar los siguientes factores: Talento Humano, Infraestructura, Planeación, Recursos financieros, entre otros.

Contexto del Proceso: se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como: Objetivo, alcance, interrelación con otros procesos, procedimientos y responsables.

Determinar los factores generadores de riesgos de corrupción (aplica para los riesgos de corrupción): ocasionados entre otras cosas por la misión, por las funciones que desarrolla y el sector al que pertenece la entidad

10.2.2.1.2. IDENTIFICACIÓN DEL RIESGO

La identificación y valoración de los riesgos de corrupción se realizará acorde a lo mencionado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4. Así mismo el diseño de sus controles.

Para los riesgos de corrupción en los trámites se tomará como referente el Anexo 3. Protocolo para la identificación de riesgos de corrupción asociados a la prestación de trámites y servicios.

En cuanto a los riesgos de fraude se tendrán como referencia para este análisis los conceptos y controles establecidos en la Resolución 193 de 2016 y su anexo, referente al Control Interno Contable y lo mencionado en la estrategia de convergencia de la regulación contable pública hacia NIIF y NICSP, entre otros. El resultado de esa identificación de riesgos quedará registrada en el Formato Mapa de riesgos de corrupción del proceso.

10.2.2.1.3. VALORACIÓN DEL RIESGO

La valoración de los riesgos de corrupción se realizará acorde a lo metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada por el Ministerio para la gestión del riesgo y las tablas de impacto definidas para el Ministerio.

Es así como después de realizar el establecimiento del contexto y la identificación de los riesgos, se procede realizar en mesas de trabajo el análisis de la probabilidad y el impacto de los establecidos como valoración preliminar para generar el valor del riesgo inherente, se identifican sus causas y los controles para mitigar dichas causas. A estos controles se le definen las variables a evaluar para el adecuado diseño de controles como son: la asignación de un responsable, segregación y autoridad del responsable, periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. La valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP.

10.2.2.1.4. DEFINICIÓN Y APROBACIÓN DE MAPAS DE RIESGO Y PLANES DE TRATAMIENTO DE RIESGOS.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de corrupción de la Entidad, el gestor del proceso procederá a

cargar el documento interno llamado “Mapa de riesgos del proceso” para que surta el proceso de aprobación documental por parte del líder y de la Oficina Asesora de Planeación a través de la herramienta SIMIG. Así mismo, se clasifican aquellos riesgos cuya calificación residual se encuentren en zona Alta o Extrema en el mapa de calor y para estos casos, la Oficina Asesora de Planeación, en conjunto los procesos en los cuales se obtenga dicha calificación residual y con el acompañamiento del líder de transparencia de la entidad, formularán un plan de tratamiento para los riesgos de corrupción que contenga las acciones requeridas para mitigar su ocurrencia e impacto dentro de la Entidad, y presentarlo para conocimiento y aprobación ante el Comité Institucional de Control Interno de la entidad.

10.2.2.1.5. MATERIALIZACIÓN

El reporte de los eventos de riesgos de corrupción o cualquier sospecha de evento de riesgo de corrupción o conflicto de interés, debe ser realizado a través de su buzón soytransparente@mintc.gov.co que se encuentra en la página web de la Entidad.

Estos eventos reportados son recibidos y analizados directamente al Grupo Interno de Trabajo de Control Interno Disciplinario quien realizará la investigación y tratamiento correspondiente acorde a la normatividad vigente.

10.2.2.1.6. MEDICIÓN

El monitoreo se realiza en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizan monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

Adicionalmente, el monitoreo y seguimiento de los riesgos de corrupción del Ministerio aprobados por los procesos, así como de sus controles, se realiza por parte del grupo interno de trabajo de Transformación Organizacional, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de los controles y reporten las evidencias de los mismos, los profesionales del grupo interno de trabajo de Transformación Organizacional realizan la revisión y validación de esta información, con el fin de reportar la medición trimestral de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de corrupción del Ministerio.

Los procesos que obtengan un rango bajo en la medición del indicador por no gestionar sus controles en la fecha límite informada para su gestión, deberán ir al Comité MIG a explicar las razones de su incumplimiento y formular el plan de mejora que evite que vuelva a suceder.

10.3 ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS.

10.3.1. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) le permite al Ministerio realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La aplicación de la administración de riesgos se alinea con la Guía para la administración del riesgo y el diseño de controles en entidades públicas y el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD).

La administración de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

Sólo se identificarán riesgos de Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios (riesgos de Interrupción) para aquellos activos cuyo nivel de criticidad sea alto, o que en su identificación se evidencie falta de controles de seguridad de la información.

10.3.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada gestión de los riesgos de Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios (riesgos de interrupción) del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

Gestionar los riesgos asociados a los activos de información críticos de los procesos, con el objetivo de identificarlos, clasificarlos y valorarlos de acuerdo con la importancia que tengan para el funcionamiento óptimo de los procesos del MINTIC.

10.3.1.2. ALCANCE DE LA POLÍTICA

Los presentes lineamientos aplican a la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) a los que podrían estar expuestos todos los procesos que hacen parte del Modelo de operación del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones.

10.3.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido para los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios (riesgos de interrupción), el nivel de aceptación se aplica a todos los riesgos que se ubiquen en un nivel residual bajo. Para los riesgos que se ubiquen en un nivel diferente se deberá realizar un plan de tratamiento que permita reducir el nivel del riesgo.

10.3.1.4. NIVELES PARA CALIFICAR EL IMPACTO

Para la calificación del impacto de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios (riesgos de interrupción) se tendrá en cuenta los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Como recomendación y en la medida en que aplique se deberá tener en cuenta de manera cualitativa el impacto a nivel de integridad, disponibilidad o confidencialidad de la información.

10.3.1.5. TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso como dueño del riesgo junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Reducir el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

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

Transferir el riesgo: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Mitigar: (Plan de Acción) Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

10.3.2. 1.ETAPAS EN LA ADMINISTRACIÓN DEL RIESGO

En la Administración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios (riesgos de interrupción) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones se siguen las etapas de identificación, medición, control y monitoreo del riesgo en los procesos, teniendo como referencia la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública (DAFP).

10.3.2.1.1. ESTABLECIMIENTO DEL CONTEXTO

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios (riesgos de interrupción) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

10.3.2.1.2. IDENTIFICACIÓN DEL RIESGO

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios (riesgos de interrupción) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar en el formato del mapa de riesgos: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), dueño del riesgo (líder del proceso), activo de información afectado, amenazas, vulnerabilidades y consecuencias.

Para determinar los activos afectados es necesario validarlos dentro del inventario de activos de información del proceso en donde en su valoración se estableció la criticidad, la clasificación de la información y otros atributos importantes a tener en cuenta en el análisis del posible riesgo. Es importante mencionar que la identificación de los activos de información se realizó de acuerdo con los lineamientos establecidos por la entidad en los documentos GDO-TIC-MA-014 manual de activos de información y el GDO-TIC-PR-019 Procedimiento Activos de Información.

Por otra parte, la identificación de las posibles amenazas y vulnerabilidades es apoyada por el catálogo definido en el anexo 4 “Lineamientos para la gestión del riesgo en entidades públicas” las cuales son analizadas, validadas y complementadas en las mesas de trabajo con los diferentes procesos, y de acuerdo con éstas se establecen las posibles consecuencias.

Adicionalmente, para los riesgos de interrupción se establece:

- Su actualización está sujeta por la actualización de la documentación correspondiente al Plan de Continuidad del Negocio (BCP) y específicamente al documento del Análisis de Impacto al Negocio (BIA).
- Una nueva categoría o tipología denominada **Interrupción,**
- Un campo asociado al **Custodio del Activo,** que corresponde al proceso o al tercero responsable por el activo ante la Entidad. Cuando el custodio del activo es un proceso diferente al proceso que identifica el riesgo o es un tercero, los controles y planes de tratamiento deben establecerse de manera conjunta.
- **Fuente o Tipo de amenaza**, que corresponde a los tipos de amenaza establecidos en la metodología. Estos pueden ser Naturales, Humanos, Ambientales, Tecnológicos o De terceros.

Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

10.3.2.1.3. VALORACIÓN DEL RIESGO

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios (riesgos de interrupción) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada por el Ministerio para la gestión del riesgo y las tablas de impacto definidas para el Ministerio.

Es así como en mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus amenazas, vulnerabilidades y consecuencias e identificando los controles asociados al anexo A de la Norma ISO 27001 para mitigarlas. A estos controles se le identifican las variables a evaluar para su adecuado diseño como son: la asignación de un responsable, segregación y autoridad del responsable, tipo de control (preventivo, detectivo o correctivo), implementación (manual o automático), periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. La valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo.

Para los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo.

10.3.2.1.4. DEFINICIÓN Y APROBACIÓN DE MAPAS DE RIESGOS Y PLANES DE TRATAMIENTO.

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) del Ministerio, los líderes de los procesos apoyados por los gestores, deberán realizar a través de la plataforma de formalización de documentación definida por el Ministerio, el proceso de aprobación de los mapas de riesgos y de los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

10.3.2.1.5. MATERIALIZACIÓN

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

10.3.2.1.6. MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) del Ministerio aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del equipo de Seguridad y Privacidad de la Información teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados así como el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, los profesionales del proceso de Seguridad y Privacidad de la Información realizan la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el seguimiento a la ejecución de los controles de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios del Ministerio.

Los procesos que obtengan un rango bajo en la medición del indicador por no gestionar sus controles en la fecha límite informada para su gestión, deberán ir al Comité MIG a explicar las razones de su incumplimiento y formular el plan de mejora que evite que vuelva a suceder.

10.4 ADMINISTRACIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO – SGSST

La administración de riesgos en Seguridad y Salud en el Trabajo tiene como objetivo la protección de las personas, gestionando y estableciendo los controles para minimizar la materialización de los peligros identificados que pueden generar consecuencias en las personas tanto a nivel físico como psicológico, teniendo en cuenta las diferentes actividades, funciones u obligaciones laborales tanto en las instalaciones de la entidad como en actividades de comisión, teletrabajo o trabajo en casa.

Lo anterior enfocado en la prevención de incidentes, accidentes de trabajo y enfermedades laborales, orientando la gestión a toda la población de la entidad, independiente del tipo de vinculación, atendiendo lo estipulado normativamente y basándose en la metodología establecida mediante la Guía Técnica Colombiana GTC-45.

10.4.1 LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

10.4.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada gestión de los riesgos de Seguridad y Salud en el Trabajo del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en Guía GTC 45 versión 2012, orientando a la toma de decisiones oportunas y minimizando accidentes de trabajo o enfermedades laborales al interior de la Entidad.

10.4.1.2. ALCANCE DE LA POLÍTICA

Los presentes lineamientos aplican a la gestión de los riesgos de Seguridad y Salud en el Trabajo a los que podrían estar expuestos todos colaboradores de los procesos que hacen parte del Sistema Integrado de Gestión del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones.

10.4.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

En el Sistema en Seguridad y Salud en el Trabajo de la entidad, la aceptación del riesgo se identifica en la guía GTC 45 versión 2012, acogiendo y adoptando las tablas y rangos mencionados en dicha referencia.

10.4.1.4. NIVELES PARA CALIFICAR EL IMPACTO

En el Sistema en Seguridad y Salud en el Trabajo de la entidad, los niveles para calificar el impacto, se basan en la guía GTC 45 versión 2012, acogiendo y adoptando las tablas y rangos mencionados en dicha referencia.

10.4.1.5. TRATAMIENTO DE RIESGOS

En el Sistema en Seguridad y Salud en el Trabajo de la entidad, el tratamiento de los riesgos, se basan en la guía GTC 45 versión 2012, acogiendo y adoptando las tablas y rangos mencionados en dicha referencia.

10.4.2. ESTRUCTURA PARA LA GESTIÓN DE RIESGOS

10.4.2.1. ETAPAS EN LA ADMINISTRACIÓN DEL RIESGO

10.4.2.1.1. ESTABLECIMIENTO DEL CONTEXTO

El contexto para la gestión de riesgos en Seguridad y Salud en el Trabajo se basa en la identificación de los peligros presentes en cada uno de los procesos que se desarrollan en el Ministerio de Tecnologías de la Información y las Comunicaciones, generando su valoración y estableciendo los controles necesarios y apropiados para evitar que los mismos generen accidentes de trabajo o enfermedades laborales.

10.4.2.1.2. IDENTIFICACIÓN, VALORACIÓN DEL RIESGO Y APROBACIÓN DE PLANES DE TRATAMIENTO

La identificación se genera mediante la recolección de información sobre inspecciones de las áreas, entrevistas al personal y matrices de riesgos de Seguridad y Salud en el Trabajo de años anteriores; de esta forma, se identifican condiciones inseguras, actos inseguros y los controles existentes, relacionando todos los controles que la entidad ha implementado para reducir el riesgo asociado a cada peligro.

La valoración se basa fundamentalmente en la metodología establecida en la Guía Técnica Colombiana GTC-45, determinando los niveles de probabilidad y consecuencia de cada riesgo, generando la respectiva valoración o nivel de riesgo.

Los planes de tratamiento consideran los costos relativos, la respectiva disponibilidad y aprobación dentro del Plan Anual de Adquisiciones de la entidad, los beneficios de la reducción de riesgos, y la confiabilidad de las opciones disponibles en el siguiente orden de eliminación, sustitución, controles de ingeniería, controles administrativos, señalización, advertencias y equipos o elementos de protección personal.

Lo anterior descrito se encuentra en el procedimiento GTH-TIC-PR-023 Identificación de Peligros y Valoración de Riesgos Ocupacionales.

10.4.2.1.3. MATERIALIZACIÓN

En el caso de materializarse un riesgo, se seguirá lo establecido en el Manual GTH-TIC-MA-007 Gestión del Riesgo de Desastres- Plan de Emergencias MinTIC y en el procedimiento GTH-TIC-PR-024 Investigación de incidentes y accidentes de trabajo.

10.4.2.1.4. MEDICIÓN

El monitoreo y seguimiento de los riesgos en Seguridad y Salud en el Trabajo se realiza identificando y midiendo los peligros presentes en cada uno de los procesos que se desarrollan en el Ministerio de Tecnologías de la Información y las Comunicaciones, generando su valoración y estableciendo los controles necesarios y apropiados para evitar que los mismos generen accidentes de trabajo o enfermedades laborales.

Los Controles están orientados bajo un orden jerárquico de intervención para cada uno de los peligros identificados, buscando eliminar, sustituir, establecer controles de ingeniería o controles administrativos para gestionar dichos peligros. La gestión de las medidas de intervención se basa y se controla con la ejecución de los planes, programas, procedimientos o lineamientos que se generan de Seguridad y Salud en el Trabajo de la entidad.

10.5. ADMINISTRACIÓN DE RIESGOS DEL SISTEMA DE GESTIÓN AMBIENTAL

La administración de riesgos ambientales se realiza teniendo en cuenta los aspectos e impactos significativos identificados y sus requisitos legales asociados. Lo anterior, de acuerdo con el AGI-TIC-PR-009 Procedimiento para la identificación de aspectos y valoración de impactos ambientales y lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública.

Lo anterior permite identificar los riesgos ambientales que podrían generar un impacto afectando no sólo al medio ambiente sino también al Ministerio y sus diferentes grupos de interés.

10.5.1. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

10.5.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada gestión de los riesgos ambientales del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo lo establecido en el Plan Institucional de Gestión Ambiental AGI-TIC-MA-002 y la matriz de impactos y aspectos ambientales AGI-TIC-DI-006, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión ambiental institucional, y por lo tanto, dar cumplimiento a la normatividad asociada.

10.5.1.2. ALCANCE DE LA POLÍTICA

Los presentes lineamientos aplican a la gestión de los riesgos ambientales a los que podrían estar expuestas las actividades administrativas realizadas en la única sede del MinTIC, que hacen parte del Sistema Integrado de Gestión del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones.

10.5.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

El Sistema de Gestión Ambiental ha establecido para los riesgos ambientales un nivel de aceptación/tolerancia para aquellos riesgos ubicados en un nivel residual bajo

10.5.1.4. NIVELES PARA CALIFICAR EL IMPACTO

En el Sistema de Gestión Ambiental de la entidad se tienen variables para valorar o calificar el impacto ambiental, las cuales se encuentran relacionadas en el Procedimiento para la identificación de aspectos y valoración de impactos ambientales; con base en esto, se identifican aquellos aspectos con una clasificación de importancia alta y se analiza su capacidad de generar un riesgo ambiental para la Entidad.

10.5.2. ESTRUCTURA PARA LA GESTIÓN DE RIESGOS

10.5.2.1. ETAPAS EN LA ADMINISTRACIÓN DEL RIESGO

En la Administración de riesgos ambientales, el Ministerio/Fondo único de Tecnologías de la Información y las Comunicaciones sigue las etapas definidas en el Procedimiento para la identificación de aspectos y valoración de impactos ambientales, aplicada a las actividades administrativas del Ministerio, realizando un análisis de la situación ambiental de la entidad, con el fin de determinar los aspectos ambientales por los cuales se puede presentar algún riesgo para la Entidad.

10.5.2.1.1. ESTABLECIMIENTO DEL CONTEXTO

El contexto se define a partir de las condiciones ambientales internas y externas de la Entidad, el cual se encuentra descrito en el Plan Institucional de Gestión Ambiental AGI-TIC-MA-002 en el ítem número 3. Planificación, así mismo, se tiene en cuenta el contexto de cada uno de los procesos institucionales partiendo de la recolección de información realizada a partir del *Formato para el Establecimiento del Contexto*, en el cual se incluyen preguntas de carácter ambiental que permiten

identificar aquellos procesos relacionados con aspectos ambientales significativos y/o requisitos legales ambientales.

10.5.2.1.2. IDENTIFICACIÓN DEL RIESGO

La identificación de los riesgos del Ministerio de Tecnologías de la Información y Comunicaciones se debe realizar mediante un análisis interpretativo de la situación ambiental de la entidad, identificando las actividades y productos (bienes y/o servicios) que interactúan con el ambiente en diferentes escenarios, y de esta forma estableciendo los aspectos e impactos ambientales, así como también, los requisitos legales que en materia ambiental le apliquen a la Entidad, y con los cuales, se pueda ver comprometida su capacidad para cumplir la política ambiental adoptada.

Cabe mencionar que los riesgos asociados al Sistema de Gestión Ambiental, deberán estar relacionados en el AGI-TIC-MA-007 Manual del Sistema de Gestión Ambiental.

10.5.2.1.3. VALORACIÓN DEL RIESGO

Una vez identificado el contexto, e identificados y evaluados los aspectos e impactos ambientales junto con los requisitos legales ambientales aplicables, para la vigencia, se procede a valorar el riesgo ambiental correspondiente teniendo en cuenta la metodología definida para la determinación de riesgos de gestión; toda vez que, con los riesgos de carácter ambiental se encuentran estrechamente ligados a la gestión que realiza la Entidad en materia ambiental institucional y por ende, no sólo se busca mitigar/evitar los posibles impactos ocasionados directamente al ambiente, sino también los impactos que puedan ocasionarse a la Entidad en materia económica y/o reputacional.

10.5.2.1.4. DEFINICIÓN Y APROBACIÓN DE PLANES DE TRATAMIENTO DE RIESGOS

- Riesgos asociados con aspectos ambientales significativos con rango de importancia moderada y requisitos legales relacionados: cuando se obtenga esta interpretación el líder del proceso a cargo del Sistema de Gestión Ambiental debe establecer controles operacionales (prácticas, actividades, procedimientos, etc).
- Riesgos asociados con aspectos ambientales significativos con rango de importancia alta y requisitos legales relacionados: cuando se obtenga esta interpretación el líder del proceso a cargo del Sistema de Gestión Ambiental y de los procesos que se vean relacionados con su posible materialización, deben establecer mecanismos de mejora, control y seguimiento.

10.5.2.1.5. MATERIALIZACIÓN

Cuando se genera la materialización de un evento con impacto ambiental, éstos deberán ser inmediatamente reportados al correo: sgambiental@mintic.gov.co, con el propósito de tomar las acciones correspondientes de manera oportuna informando la descripción de la situación presentada.

Una vez materializado el evento se deberá proceder con la formulación del plan de mejora correspondiente, de acuerdo con lo establecido en el procedimiento Formulación, seguimiento y cierre de acciones de mejora.

10.5.2.1.6. MEDICIÓN

La medición de los riesgos ambientales estará enfocada en determinar el porcentaje gestionado de los controles establecidos de acuerdo con su programación para lo cual se estableció la siguiente formula:

$$\frac{No.\,de\ controles\ gestionados\ en\ el\ periodo}{No.\,de\ controles\ identificados\ en\ el\ periodo} * 100$$

Cuando se evidencie que se incumple con el indicador, se debe formular un plan de mejora que indique la corrección o actividades que nos permitirán cumplir con este. En caso de que el incumplimiento obedezca a factores externos que no puedan ser controlados por el proceso, se debe relacionar la debida justificación.

10.6. ADMINISTRACIÓN DE RIESGOS DE INICIATIVAS Y PROYECTOS

10.6.1 LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

10.6.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada administración de los riesgos identificados y registrados en el aplicativo ASPA que puedan afectar el logro de los objetivos de cada iniciativa o proyecto de cada una de las áreas de la entidad que conforma el Plan de Acción de cada vigencia para el Ministerio/Fondo Único de Tecnologías de la Información y las comunicaciones.

10.6.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA AL RIESGO

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido que para los riesgos de iniciativas y proyectos como nivel tolerable, serán aceptados los riesgos que se ubiquen en una zona baja y moderada.

10.6.1.4. NIVELES PARA CALIFICAR EL IMPACTO

Por impacto se entienden las consecuencias que le pueden ocasionar en el logro de los objetivos de la iniciativa o proyecto la materialización del riesgo, para su determinación se utiliza la siguiente tabla:

Tabla No.2 Criterios para Calificar el Impacto		
CRITERIOS PARA CALIFICAR EL IMPACTO		
NIVEL	NIVEL	IMPACTO
5	Critico	Se ve afectada la imagen de la entidad ante grupos de interés y ciudadanía, presunción de hechos de corrupción y/o indebidas actuaciones. Incumplimiento en las metas y objetivos institucionales afectando de forma grave los objetivos estratégicos propuestos del sector TIC.
4	Mayor	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento de las metas del gobierno y estrategia del sector TIC, materialización de hallazgos y observaciones de índole administrativo o fiscal.
3	Moderado	Incumplimiento de los objetivos de las iniciativas y proyectos a nivel operativo y táctico, posibles reclamaciones o quejas por los diferentes grupos de interés y ciudadanía. Inoportunidad en la información ocasionando retrasos en la ejecución de la iniciativa.
2	Menor	Solicitudes de cambio no significativos en los ajustes de los proyectos sin afectar los objetivos del proyecto, El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno.
1	Leve	No afecta el desarrollo de la iniciativas y proyectos que conforman el plan de acción, el riesgo afecta la imagen de alguna área de la organización.
Fuente: GIT de Planeación y Seguimiento		

10.6.1.5. TRATAMIENTO DE RIESGOS

De acuerdo con lo establecido en la metodología PMIBOOK implementar las respuestas al riesgo: Consiste en implementar las estrategias de tratamiento a los riesgos los cuales deben ser documentados en una carpeta propia en cada dependencia para efectos de auditoría y gestión del conocimiento, el beneficio clave es asegurar que las estrategias de tratamiento a los riesgos se ejecuten tal como se planificaron.

La implementación de respuesta a los riesgos de las iniciativas y proyectos, debe realizar cada dependencia del MinTIC con el líder de la iniciativa, el responsable del proyecto y su equipo.

El líder de las iniciativas y proyectos junto con sus equipos deben estar atentos a los eventos identificados en los riesgos de forma tal que determinen las acciones que permitan controlar evitar la materialización del riesgo o su mitigación a través de las acciones de mitigación en caso de que se haya materializado el riesgo.

Las acciones y actividades realizadas deben registrarse en el seguimiento que se hace mensualmente a los riesgos en el aplicativo ASPA, y los soportes que dan cuenta de estas acciones, deben almacenarse en un repositorio dentro de la carpeta de entregables de la iniciativa a que pertenece.

10.6.2. ESTRUCTURA PARA LA GESTIÓN DE RIESGOS

10.6.2.1. ETAPAS EN LA ADMINISTRACIÓN DELRIESGO

10.6.2.1.1. PLANIFICAR LA GESTION DE LOS RIESGOS:

Define cómo realizar las actividades de gestión de riesgo del proyecto. En el Ministerio se realiza utilizando como entradas el acta de constitución del proyecto cuando aplique, documentos del proyecto tales como la plantilla PES, repositorio de lecciones aprendidas de anteriores proyectos y similares, otros factores de la Entidad que pueden influir en la administración del riesgo. Adicionalmente se utilizan herramientas y técnicas para planificar la gestión de riesgos tales como: reuniones durante la jornada de planeación estratégica las cuales se realizan con los líderes de las iniciativas, la Ministra y el Comité Directivo; Reuniones a través de mesas de trabajo con los enlaces de las Iniciativas y Proyectos que conforman el plan de acción; o el Análisis de datos: de las Lecciones aprendidas de la ejecución de los proyectos anteriores y los que están en curso, solicitudes de cambio de iniciativas y proyectos, análisis de proyectos similares y análisis de los riesgos materializados identificados en las solicitudes de cambio.

10.6.2.1.2. IDENTIFICAR LOS RIESGOS:

Consiste en identificar y determinar los riesgos que pueden afectar el proyecto, así como las fuentes de riesgo general del proyecto y documentar sus características.

En esta etapa se identifican los riesgos determinando las causas con base en el contexto interno y externo, igualmente se establecen las consecuencias en caso de materialización.

Para su análisis se pueden utilizar herramientas o técnicas tales como: datos históricos, opiniones informadas y expertas, las necesidades de las partes involucradas, lecciones aprendidas y las solicitudes de cambio que están registradas en el Aplicativo de Seguimiento al Plan de Acción “ASPA”. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan las iniciativas y proyectos (líderes de la iniciativa, funcionarios y/o contratistas encargados de registrar la información en el Aplicativo de Seguimiento al Plan de Acción “ASPA”).

La identificación de los riesgos es un proceso recurrente porque se da a lo largo de todo el proyecto, se debe tener en cuenta que los riesgos se transforman y hay riesgos que surgen durante la vida de la iniciativa y el proyecto, en su desarrollo y ejecución. Es importante que en cada comité primario las dependencias que tienen iniciativas asignadas analicen los riesgos impredecibles, monitoreen y evalúen los existentes puesto que la amenaza puede desaparecer al dejar de existir el evento generador.

Es recomendable realizar la identificación de los riesgos durante los ejercicios anuales de Planeación Estratégica en las que participan el responsable del registro de la información en el aplicativo, el líder de la iniciativa y los colaboradores del MinTIC involucrados en el proyecto, con el fin de identificar y discutir cuáles son los riesgos que pueden afectar positiva o negativamente los objetivos de las iniciativas o proyectos.

Para la identificación de los riesgos de las iniciativas y proyectos se recomienda crear un listado de riesgos que se documenta en una hoja de Excel y se debe asociar la categoría, identificar la causa, mencionando si corresponde a un riesgo negativo o positivo. Si es riesgo de un proyecto se debe relacionar la fase en la que se pueda presentar el riesgo (Planeación, Ejecución o Seguimiento).

Tener en cuenta que de acuerdo con la Política de seguridad de la información en la gestión de proyectos contenida en la resolución No.0448 de 2022, se debe identificar riesgos asociados a seguridad y privacidad de la información. EL Oficial de Seguridad y Privacidad de la información o a quien este delegue de acuerdo con la especificidad técnica, apoyará cuando se requiera en la evaluación de los riesgos de seguridad y privacidad de la información en una fase inicial del proyecto para identificar los controles necesarios, de acuerdo con el tipo de proyecto.

10.6.2.1.2.1. ESTABLECIMIENTO DEL CONTEXTO

En esta etapa se definen los parámetros tanto internos como externos que debemos tener en cuenta para la administración del riesgo

10.6.2.1.2.1.1. ESTABLECIMIENTO DEL CONTEXTO EXTERNO

Se determinan las características esenciales del entorno en el cual opera la entidad, como son los factores Legales, Políticos, Sociales, Tecnológicos, Financieros y Sectoriales. Así como aquellos impulsores claves y tendencias que tengan impacto a la organización, relaciones con las partes involucradas, sus percepciones y valores.

10.6.2.1.2.1.2. ESTABLECIMIENTO DEL CONTEXTO INTERNO

Se determinan las características esenciales del ambiente en el cual el Ministerio TIC busca alcanzar sus objetivos, como son su estructura organizacional, sus objetivos, sus recursos económicos, tecnológicos, sus procesos.

10.6.2.1.2.2. REDACCIÓN Y DESCRIPCIÓN DEL RIESGO

Los riesgos deben quedar bien redactados deben ser claros, simples de entender, no ambiguos, ni generales. Para la definición del riesgo, se podrán utilizar palabras que denoten la situación indeseada tales como: Imposibilidad, Fallas, Errores, Inadecuado, Conflictos, Ausencia, Fraude, Inexactitud, Duplicación, Falta de autorización, Incumplimiento, Incorrecta, Imprecisión, Pérdida, Inoportunidad, Indisponibilidad, Dificultad.

10.6.2.1.2.3. DESCRIPCIÓN DEL RIESGO

Para la descripción de un riesgo se recomienda como una mejor práctica seguir la siguiente estructura:

Debido a la (Causa) puede ocurrir (Riesgo), lo que provocaría el (Consecuencia) en el proyecto, por ejemplo:

Riesgo: Modificación del cronograma de ejecución del proyecto

Causa del Riesgo: Continuos ajustes al Plan Anual de Adquisiciones

Consecuencias del Riesgo: Dificultad en el cumplimiento de los objetivos definidos en el proyecto.

Descripción del Riesgo: Los continuos ajustes al Plan Anual de Adquisiciones, originan modificaciones al cronograma de ejecución del proyecto ocasionando una dificultad en el cumplimiento de los objetivos definidos en el proyecto.

10.6.2.1.2.4. ANÁLISIS DE CAUSA

Uno de los componentes más importantes del riesgo es la causa que lo genera, por esto es muy significativo enfocarse en gestionar las razones por las cuales podría ocurrir un riesgo.

La causa debe ser coherente con el riesgo, por ejemplo: “La resistencia al cambio de la ciudadanía es alta, si no se gestionan bien sus necesidades y expectativas, puede provocar que los usuarios rechacen la iniciativa”.

Una vez depurada la lista que se obtuvo en la etapa de identificación de los riesgos, se procede a identificar las causas de riesgo.

Hay varias herramientas que nos pueden ayudar a identificar las causas de riesgo que afectan negativamente el objetivo de nuestras iniciativas o proyectos, para el ejercicio se recomiendan tres herramientas como son: los talleres de identificación de riesgos, la tormenta o lluvia de ideas y análisis FODA en esta última técnica se identifican las fortalezas y debilidades de la entidad luego identifica las oportunidades para el proyecto teniendo en cuenta las fortalezas y luego las amenazas que resulte de las debilidades.

Los talleres de identificación de riesgos son reuniones de identificación de las causas de riesgos, que se desarrollan en ejercicios de planeación estratégica, o en los grupos primarios donde el líder, el colaborador encargado de registrar la información en el aplicativo “ASPA”, o con el equipo de trabajo del área, identifican cuáles son las causas que pueden generar los riesgos identificados en la primera parte del proceso de identificación de riesgos.

La ventaja de esta herramienta es que permite identificar muchas causas y efectos de forma rápida, fácil y creativa. Es posible que se genere una larga lista de causas, por tanto, se deben seleccionar las causas más significativas, tal como se realizó en la etapa de identificación del riesgo, esta herramienta permite involucrar el equipo y tener una retroalimentación directa e inmediata.

10.6.2.1.2.5. CLASIFICACIÓN DE RIESGOS EN PROYECTOS

Existen diferentes clasificaciones a tener en cuenta a la hora de gestionar riesgos en las iniciativas y proyectos:

Clasificación de riesgos en Proyectos según su impacto

Riesgos conocidos: Son aquellos que han sido identificados y analizados, por lo que se puede planificar una acción preventiva.

Riesgos desconocidos: Son aquellos que no han sido identificados en la fase de “identificación de riesgos”. Por este motivo, no pueden ser tratados de forma proactiva

Los riesgos de las iniciativas y proyectos pueden provenir de fuentes externas o internas

10.6.2.1.2.6. TIPOLOGÍA DEL RIESGO

Definir la tipología del riesgo tiene como propósito establecer en que ámbito el riesgo se va a desarrollar, para lo cual se definen las siguientes:

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

Para realizar la identificación de los riesgos de corrupción es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCION U OMISIÓN+USO DEL PODER+DESVIACION DE LA GESTION DE LO PUBLICO+BENEFICIO PRIVADO

Con el fin de facilitar la identificación de los riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición.

De acuerdo con la matriz que se detalla a continuación, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un 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

Fuente: Secretaría de Transparencia de la Presidencia de la República.

Al realizar la identificación de riesgos de corrupción para iniciativas y proyectos, el líder de la iniciativa verificará si estos riesgos se encuentran identificados en el Mapa de Riesgos Institucional, en caso contrario se deben incluirlos.

Los líderes de las iniciativas y proyectos junto con su equipo deben realizar monitoreos mensuales y evaluación permanente a la gestión de riesgos de corrupción.

Es importante que los riesgos de corrupción siempre sean gestionados. En caso de que se materialice un riesgo de corrupción el líder de la iniciativa o del proyecto debe reportar los eventos de riesgos de corrupción o cualquier sospecha de evento de riesgo de corrupción o conflicto de interés, a través de un buzón soytransparente@mintc.gov.co que se encuentra en la página web de la Entidad.

Estos eventos reportados son recibidos y analizados directamente al Grupo Interno de Trabajo de Control Interno Disciplinario quien realizará la investigación y tratamiento correspondiente acorde a la normatividad vigente.

Para los proyectos o iniciativas que componen el plan de acción de la entidad, los lideres deberán validar si sus proyectos cumplen con uno o más de los criterios que se detallan a continuación, lo cual los hace susceptibles a riesgos de corrupción, por tanto, deben identificarlos:

1. Cuando el proyecto requiera de una contratación derivada. Es decir, cuando un contratista tiene previsto contratar a terceros para el desarrollo del contrato
2. Proyectos donde tengan interventoría o aprobaciones de pago por parte de terceros.
3. Durante la ejecución del proyecto se evidencie cambios en la forma de pago pactada inicialmente.
4. Cuando se evidencie retrasos en la ejecución del cronograma sin previa justificación.
5. Cuando se presenten posibles deficiencias en los productos o servicios adquiridos.

Riesgos de cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

Riesgos estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos de imagen: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas. Relación con la percepción y la confianza de la ciudadanía hacia la gestión de la institución.

Riesgos operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad. Comprende los riesgos que provienen del funcionamiento y operatividad del sistema de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica. Está relacionado con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la Misión.

Riesgos de seguridad y privacidad 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 que afecta la confidencialidad, integridad, privacidad o disponibilidad de la información.

Para gestionar estos riesgos las dependencias del MinTIC se deberán apoyar en el Oficial de Seguridad y Privacidad de la información o quien haga sus veces y su equipo de trabajo, siguiendo los lineamientos del SPI-TIC-DI-009 Plan de Tratamiento a Riesgos.

10.6.2.1.2.7. IDENTIFICACIÓN DE RIESGOS POSITIVOS O NEGATIVOS Y LA FASE EN LA QUE SE ENCUENTRAN

Para realizar una mejor identificación de los riesgos se debe establecer si el riesgo es negativo o positivo y asociar la fase del proyecto en la que se encuentra el riesgo de acuerdo con las establecidas para los proyectos: planeación, ejecución y seguimiento.

Riesgos positivos: un riesgo puede ser positivo al proporcionar una oportunidad para el proyecto y la organización, que puede ser reflejado en la reducción de costos, simplificación de tareas, obtención de beneficios a los grupos de interés, entre otros. De esta forma el equipo del proyecto puede mejorar su probabilidad de que se materialicen los riesgos de iniciativas y proyectos.

[JAN1]Se incluye la frase "los riesgos de iniciativas y proyectos"

Riesgo negativo: Un riesgo negativo es una amenaza, que cuando ocurre, se transforma en un problema, porque puede impactar negativamente los objetivos y el desarrollo del proyecto.

Fases del proyecto en la que se puede asociar el riesgo

Planeación: la fase de planeación del proyecto incluye las acciones requeridas para establecer el alcance, el costo, las adquisiciones, los interesados y los riesgos del proyecto. Está compuesta por las sub-fases de preparación de la planeación, programación e inicio definidas en la Metodología de Gerencia de Proyectos.

Ejecución: La fase de ejecución inicia posteriormente a la fase de planeación donde se dirige y gestiona el trabajo del proyecto que implica ejecutar las actividades programadas a fin de completar los entregables y alcanzar los objetivos establecidos.

Seguimiento: En la fase de seguimiento se realiza el monitoreo, revisión e información del avance general a fin de cumplir con los objetivos establecidos para el proyecto. Busca analizar y regular el progreso y desempeño del proyecto para identificar los cambios presentados respecto a su planeación. Se cataloga como una fase transversal a las fases de planeación y ejecución.

10.6.2.1.3. REALIZAR EL ANALISIS CUALITATIVO O CUANTITATIVO DE LOS RIESGOS

En esta etapa se busca establecer cuáles son los riesgos más relevantes que al momento de su materialización que afecten significativamente los objetivos de las iniciativas o proyectos, cuál es la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial y cómo abordarlos.

Para este análisis se utiliza en primera instancia el análisis cualitativo para las iniciativas y proyectos, el análisis cuantitativo se realiza sólo si es necesario en los proyectos que conforman la iniciativa.

En el análisis cualitativo de las Iniciativas y proyectos se deben analizar los riesgos evaluando la probabilidad de ocurrencia, y el impacto que causaría su materialización. De la lista de riesgos identificados y priorizados en la etapa de identificación, se debe realizar el respectivo análisis cualitativo con el equipo, el líder de la iniciativa y el responsable del proyecto, este análisis es obligatorio para determinar cuál es la probabilidad de ocurrencia de cada riesgo y cuál sería su impacto.

El análisis cuantitativo solo se utiliza sobre los riesgos de la lista que necesitan un análisis mayor por su complejidad o impacto en el proyecto. Este permite tomar decisiones en caso de incertidumbre de una manera más precisa y debe repetirse también después de la planificación de la respuesta a los mismos, para determinar si el riesgo general del proyecto ha sido reducido satisfactoriamente. Se sugiere al responsable del proyecto considerar el juicio de expertos para determinar la necesidad y la viabilidad del análisis cuantitativo de riesgos.

Una vez analizados los riesgos cualitativamente se obtiene una lista corta de riesgos priorizados los cuales deben ser identificados y registrados en el aplicativo "ASPA".

Valoración de riesgos:

La valoración de los riesgos principalmente consiste en establecer la probabilidad de ocurrencia del riesgo, así como el impacto que causaría en la consecución del objetivo de la iniciativa o proyecto en caso de su materialización. Los cuales fueron identificados previamente durante el ejercicio anual de Planeación Estratégica.

Es así como después de realizar el establecimiento del contexto y la identificación de los riesgos, se procede a realizar el análisis de la probabilidad y el impacto.

10.6.2.1.3.1. PROBABILIDAD DE OCURRENCIA DEL RIESGO

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado

Se deben analizar los riesgos de las iniciativas o proyectos evaluando la probabilidad de ocurrencia, y el impacto que causaría su materialización, de la lista de riesgos identificados y priorizados en la etapa anterior.

En un principio se debe analizar el número de eventos asociados al riesgo en un determinado periodo de tiempo en los cuales se ha materializado el riesgo.

Para su determinación se utiliza la siguiente tabla para calificar la probabilidad de ocurrencia de los riesgos identificados para las iniciativas y proyectos:

Tabla 1 CRITERIOS PARA CALIFICAR LA PROBABILIDAD

CRITERIOS PARA CALIFICAR LA PROBABILIDAD		
NIVEL	**DETALLE**	**DESCRIPCION**
5	**Muy alta**	Se espera que el evento ocurra en la mayoria de las circunstancias, por regla general el evento ocurre.
4	**Alta**	Es viable que el evento ocurra siempre o casi siempre
3	**Moderada**	El evento podrá ocurrir en algún momento o algunas ocasiones
2	**Baja**	El evento es poco frecuente o rara vez que pueda ocurrir
1	**Muy Baja**	El evento puede ocurrir solo en circunstancias excepcionales (Poco comunes o anormales)

Fuente: Grupo Planeacion y Seguimiento OAPES

10.6.2.1.3.2. NIVEL DE IMPACTO DEL RIESGO

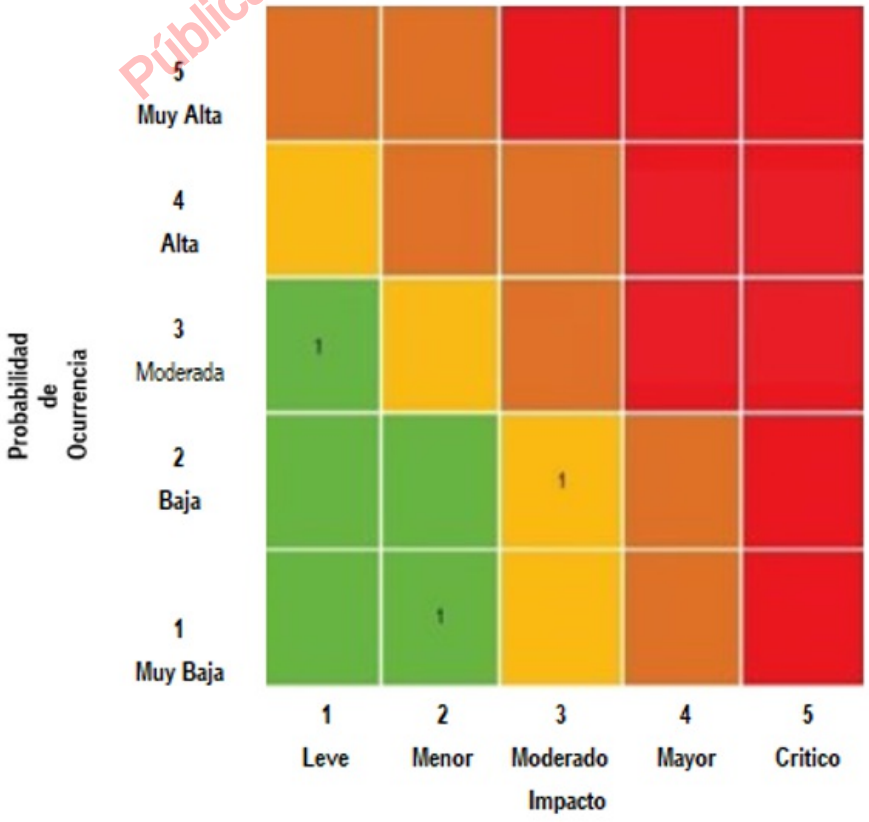
Por impacto se entienden las consecuencias que le pueden ocasionar en el logro de los objetivos de la iniciativa o proyecto la materialización del riesgo, para su determinación se utiliza la siguiente tabla

Tabla No.2 Criterios para Calificar el Impacto		
CRITERIOS PARA CALIFICAR EL IMPACTO		
NIVEL	NIVEL	IMPACTO
5	Critico	Se ve afectada la imagen de la entidad ante grupos de interés y ciudadanía, presunción de hechos de corrupción y/o indebidas actuaciones. Incumplimiento en las metas y objetivos institucionales afectando de forma grave los objetivos estratégicos propuestos del sector TIC.
4	Mayor	Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento de las metas del gobierno y estrategia del sector TIC, materialización de hallazgos y observaciones de índole administrativo o fiscal.
3	Moderado	Incumplimiento de los objetivos de las iniciativas y proyectos a nivel operativo y táctico, posibles reclamaciones o quejas por los diferentes grupos de interés y ciudadanía. Inoportunidad en la información ocasionando retrasos en la ejecución de la iniciativa.
2	Menor	Solicitudes de cambio no significativos en los ajustes de los proyectos sin afectar los objetivos del proyecto, El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno.
1	Leve	No afecta el desarrollo de la iniciativas y proyectos que conforman el plan de acción, el riesgo afecta la imagen de alguna área de la organización.
Fuente: GIT de Planeación y Seguimiento		

10.6.2.1.3.3. MATRIZ DE RIESGOS

Mapa de riesgos (Matriz de probabilidad e impacto de riesgos): permite clasificar y visualizar el estado de los riesgos en cada una de las iniciativas y proyectos con el fin de tomar decisiones sobre los aspectos críticos identificados. Para estimar el nivel de riesgo se toman los valores determinados para la probabilidad y el impacto o consecuencias y se cruzan en la siguiente matriz de riesgo, determinando así su ubicación dentro de la zona de riesgo. El mapa de riesgos es un reporte que se extrae de la herramienta ASPA y se consolida con la matriz de riesgos institucional.

En el mapa de calor en general se usan los colores para representar la prioridad de los riesgos y las zonas tolerables de los riesgos, el mapa de calor es una matriz cinco por cinco, Si los riesgos son Críticos los más altos se usa el color rojo, si son mayores se utiliza el color naranja, si son moderados se utiliza el color amarillo, y si son menores o leves se utiliza el verde.



Fuente: grafica Aplicativo ASPA mapa de calor

10.6.2.1.4. PLANIFICAR LA RESPUESTA A LOS RIESGOS:

La planificación de respuesta a los riesgos esta orientadas a definir acciones preventivas orientadas a las estrategias para amenazas u oportunidades que permitan abordar la exposición general al riesgo del proyecto.

Acción Preventiva: La identificación de las acciones preventivas lo realiza el líder del proyecto con su equipo de trabajo a través de reuniones, mesas de trabajo, datos históricos y lecciones aprendidas acordes con los objetivos de la Iniciativa y tiempos estimados del proyecto. Todas las acciones preventivas se deben monitorear de acuerdo con la periodicidad establecida por cada dependencia. Las acciones preventivas se deben registrar en el módulo de seguimiento al plan de acción por parte del enlace o colaborador autorizado, Una vez publicado el plan de acción y registradas las iniciativas y proyectos con sus riesgos se sugiere establecer las actividades de seguimiento en las acciones preventivas del primer corte que realizaran el líder del proyecto y su equipo de trabajo.

Acción de Mitigación: La mitigación de riesgos es el proceso de desarrollo de opciones y acciones que, al ser implementadas, mejorarán las oportunidades y reducirán el impacto negativo o la probabilidad de ocurrencia de un evento en particular.

La mitigación es la aplicación de acciones para reducir la vulnerabilidad frente a ciertas amenazas. Esto significa que el riesgo sigue existiendo y seguimos expuestos a él. Pero en un escenario controlado y bajo unas condiciones que nos permiten reducir la exposición y esperar un impacto negativo bajo.

Existen estrategias que podemos usar para prevenir que los riesgos ocurran, o para responder ante ellos, para el caso de los riesgos negativos podemos considerar aplicar las siguientes estrategias (Escalarlos, evitarlos, transferirlos, mitigarlos o aceptarlos) para los riesgos positivos u oportunidades (escalarlos, explotarlos, compartirlos, mejorarlos, aceptarlos).

A continuación, se describen las estrategias para amenazas como para las oportunidades que de acuerdo con los riesgos presentados a lo largo del proyecto se pueden aplicar según lo consideren el líder del proyecto con su equipo para sacar avante el proyecto.

Estrategias para amenazas.: Se pueden considerar cinco estrategias para hacer frente a las amenazas de la siguiente manera:

ü Escalar: Escalar respuesta al riesgo se realiza cuando el equipo del proyecto concluye que el riesgo está fuera del alcance del proyecto. También podría ocurrir que el riesgo esté en el alcance pero que las acciones de respuesta estén más allá de la autoridad del líder de proyectos, en este caso el riesgo debe ser escalado. Los riesgos escalados se gestionan a nivel de programa, portafolio o el área organizacional apropiada que no esté a nivel del proyecto. Es recomendable que el gerente del proyecto obtenga la confirmación de aceptación del riesgo escalado por parte de la unidad organizacional que recibe.

ü Evitar: Es una estrategia de respuesta a los riesgos según la cual el equipo del proyecto actúa para eliminar la amenaza o para proteger al proyecto de su impacto. Por lo general implica cambiar el plan para la dirección del proyecto, a fin de eliminar por completo la amenaza.

ü Transferir: La transferencia implica el cambio de titularidad de una amenaza a un tercero para que maneje el riesgo y para que soporte el impacto si se produce la amenaza, la transferencia puede ser lograda por una gama de acciones que incluye entre otras el uso de seguros, garantías de cumplimiento, fianzas, certificados de garantías para transferir a un tercero la responsabilidad de riesgos específicos, se pueden utilizar acuerdos.

ü Mitigar: En la mitigación de riesgos se toman medidas para reducir la probabilidad de ocurrencia y/o el impacto de una amenaza, las acciones de mitigación tempranas son muy efectivas, que tratar de reparar el daño después que se ha producido la amenaza.

ü Aceptar: La Aceptación del riesgo reconoce la existencia de una amenaza, pero no se toman medidas proactivas, esta estrategia puede ser apropiada para las amenazas de baja prioridad, y también puede ser adoptada cuando no es posible o rentable hacer frente a una amenaza de ninguna otra manera, la aceptación puede ser activa o pasiva, cuando la aceptación es activa es establecer una reserva para contingencias que incluya la cantidad de tiempo, dinero o recursos necesarios para manejar la amenaza si esta se presenta, la aceptación pasiva no implica ninguna acción proactiva, aparte de la revisión periódica de la amenaza para asegurarse que no cambie significativamente.

Estrategias para oportunidades: Se pueden considerar cinco estrategias para hacer frente a las oportunidades de la siguiente manera:

ü Escalar: Esta estrategia de respuesta a los riesgos es apropiada cuando el equipo del proyecto está de acuerdo en que una oportunidad se encuentra fuera del alcance del proyecto o que la respuesta propuesta excedería la autoridad del director del proyecto, las oportunidades escaladas se gestionan a nivel del programa, nivel de portafolio, u otra parte relevante de la organización y no al nivel de los proyectos. El director del proyecto determina quién debería ser notificado acerca de la oportunidad y comunica los detalles a la organización. Es importante que la responsabilidad de las oportunidades escaladas sea aceptada por la parte relevante de la organización. Las oportunidades son por lo general escaladas al nivel que coincide con los objetivos que se verían afectados si se produjera la oportunidad. Las oportunidades escaladas ya no son monitoreadas por el equipo del proyecto después del escalamiento, aunque pueden ser registradas en el registro de riesgos para propósitos de información.

ü Explotar: La estrategia de explotar se puede seleccionar para oportunidades con alta prioridad, cuando la organización quiere asegurarse que la oportunidad se haga realidad, esta estrategia busca capturar el beneficio asociado con la oportunidad especial garantizando que sin duda suceda, lo que aumenta la probabilidad de ocurrencia al 100%. Algunas respuestas de explotación asignación al proyecto de los recursos más talentosos de una organización para reducir el tiempo hasta la conclusión o el uso de nuevas tecnologías o mejoras tecnológicas para reducir el costo y la duración.

ü Compartir: Implica la transferencia de la propiedad de una oportunidad a un tercero para que éste comparta alguno de los beneficios si se produce la oportunidad. Es importante seleccionar con cuidado el nuevo dueño de la oportunidad compartida, de tal modo que sea el más capacitado para capturar la oportunidad para el beneficio del proyecto. Compartir un riesgo a menudo implica el pago de la primera de riesgo a la parte que asume la oportunidad. Un ejemplo de acciones de compartir incluye la conformación de asociaciones de riesgo compartido, equipos, compañías de propósito especial o empresas conjuntas.

ü Mejorar: La estrategia de mejorar se utiliza para aumentar la probabilidad y/o el impacto de una oportunidad, las acciones de mejoramiento tempranas son a menudo más efectivas que tratar de mejorar el beneficio después de que se ha producido la oportunidad. La probabilidad de ocurrencia de una oportunidad puede ser aumentada al centrar la atención sobre sus causas. Cuando no es posible aumentar la probabilidad, una respuesta de mejora podría aumentar el impacto centrándose en los factores que impulsan el tamaño de los beneficios potenciales. Entre los ejemplos de mejorar oportunidades se cuenta con la adición de más recursos a una actividad para terminar más pronto.

ü Aceptar: La aceptación de una oportunidad reconoce su existencia, pero no se toman medidas proactivas. Esta estrategia puede ser apropiada para las oportunidades de baja prioridad, y también puede ser adoptada cuando no es posible o rentable hacer frente a una oportunidad de ninguna manera. La aceptación puede ser activa o pasiva. La estrategia de aceptación activa más común consiste en establecer una reserva para contingencias, que incluya la cantidad de tiempo, dinero o recursos necesarios para aprovechar la oportunidad si ésta se presenta. La aceptación pasiva no implica ninguna acción proactiva, aparte de la revisión periódica de la oportunidad para asegurarse de que no cambie significativamente.

Las Estrategias anteriormente descritas, se deben registrar en las acciones preventivas en el campo de descripción de la acción en el aplicativo aspa, indicando de forma concreta la forma como se va a desarrollar la estrategia, se debe registrar de la siguiente manera: estrategia + acción preventiva. Ejemplo:

- Riesgo: Omisión de la inspección, vigilancia y control de las obligaciones a cargo de los vigilados.
- Estrategia para desarrollar: Mitigar

- Acciones de respuesta a la estrategia (Acción Preventiva): Revisión y actualización de las matrices de obligaciones pertenecientes a los sectores de móvil, no móvil, televisión, radiodifusión sonora y servicios postales, Verificar que se realicen los ajustes correspondientes a la planeación de la verificación del cumplimiento (cuando aplique). Verificar la gestión de los contratos que se suscriban en el marco de la vigilancia e inspección.

Estas estrategias deben quedar registradas para cada riesgo especificando en forma concreta cuales son las acciones que deben realizarse durante la gestión del proyecto de modo que durante el seguimiento y monitoreo de cada riesgo se tenga presente.

Nota: Para el caso de los riesgos de corrupción no pueden ser aceptados, los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

10.6.2.1.5. IMPLEMENTAR LA RESPUESTA Y SEGUIMIENTO A LOS RIESGOS

De acuerdo con lo establecido en la metodología PMIBOOK implementar las respuestas al riesgo: Consiste en implementar las estrategias de tratamiento a los riesgos los cuales deben ser documentados en una carpeta propia en cada dependencia para efectos de auditoría y gestión del conocimiento, el beneficio clave es asegurar que las estrategias de tratamiento a los riesgos se ejecuten tal como se planificaron.

La implementación de respuesta a los riesgos de las iniciativas y proyectos lo debe realizar cada dependencia del MinTIC con el líder de la iniciativa, el responsable del proyecto y su equipo.

Las acciones y actividades realizadas deben registrarse en el seguimiento que se hace mensualmente a los riesgos en el aplicativo ASPA, y los soportes que dan cuenta de estas acciones, deben almacenarse en un repositorio dentro de la carpeta de entregables de la iniciativa a que pertenece.

Materialización del Riesgo:

Se considera materialización cuando ya el riesgo ha pasado de ser un riesgo o una posibilidad de que ocurra a un hecho o acontecimiento ya ocurrido.

Las solicitudes de cambio se pueden dar por acciones preventivas con el fin de prevenir y evitar que se materialice el riesgo, como una actividad anticipada a su ocurrencia, teniendo en cuenta el seguimiento permanente y atento que se le hace a los riesgos del proyecto por el líder junto con su equipo a cargo. También se puede dar por acciones de mitigación cuando el riesgo se ha materializado y con urgencia se requieren hacer cambios, modificaciones en el proyecto (Cronograma, indicadores, modalidad de contratación, emergencia económica y ambiental, y cumplimiento de metas etc.). se establecen e implementan los controles para evitar nuevamente su ocurrencia.

El proceso de Monitorear los Riesgos puede dar lugar a una solicitud de cambio de las líneas base de costos o del cronograma o de otros componentes del plan para la dirección del proyecto. Las solicitudes de cambio se procesan para su revisión y tratamiento por medio del procedimiento DES-TIC-PR-010 Control de cambios del componente del plan de acción a cargo de la OAPES.

Cuando la situación que generó la solicitud de cambio está relacionada con un riesgo no contemplado en el mapa de riesgos de la iniciativa relacionada, se debe implementar la presente metodología - planificar la gestión de riesgos, identificación del riesgo, Análisis cuantitativo o cualitativo planificación e implementación de respuesta y monitoreo de los riesgos. igualmente se debe actualizar el mapa de riesgos en caso de que sea un riesgo nuevo, formular la acción correctiva y/o formular una acción preventiva nueva. registrar mensualmente por parte del colaborador en el módulo de seguimiento a riesgos del ASPA indicando que medidas o acciones se tomaron para corregir esa acción, y como se va a realizar el seguimiento al riesgo materializado para evitar que vuelva a ocurrir, continuar haciendo seguimiento para verificar que las acciones tomadas han sido efectivas.

Cuando se materialice un riesgo de cada una de las iniciativas y proyectos: documente y registre en el formato de Lecciones Aprendidas que tiene el aplicativo ASPA, las razones por las cuales el riesgo se materializó, describa las acciones aplicadas, los nuevos controles implementados y llevados a cabo para evitar nuevamente su materialización, realice un breve resumen como solucionó, si los controles fueron efectivos y que experiencia describen para que sea útil y tomados en cuenta en futuros proyectos.

Actualizaciones a los documentos del proyecto:

Registro de Incidentes: Es un documento del proyecto en el que se registra y da seguimiento a todos los incidentes ocurridos durante la ejecución del proyecto al realizar este registro se debe registrar tipo de incidente, quien planteo el incidente y cuando, descripción, prioridad y quien está asignado al incidente, fecha, estado y solución final. El registro de incidentes ayuda al líder de la iniciativa a realizar seguimiento y gestionar los incidentes.

Registro de lecciones aprendidas: estas se deben registrar en el módulo de lecciones aprendidas de la herramienta seguimiento al plan de acción conforme avanza al proyecto, En el registro de lecciones aprendidas se actualiza la información sobre las dificultades encontradas al implementar respuesta a los riesgos y cómo podrían haberse evitado, así como los enfoques que han funcionado bien para implementar la respuesta a los riesgos. Se documentan en el modelo de seguimiento al plan de acción siguiendo el instructivo DES-TIC-IN-003 Instructivo de lecciones aprendidas.

Asignaciones del equipo del proyecto: El líder del proyecto le indicara a su equipo de trabajo las actividades para realizar la respuesta a los riesgos, la asignación de recursos a cada acción asociada a un plan de respuesta a los riesgos y personas encargadas de realizar e informar al enlace de las actividades realizadas en el mes para que este diligencie en el aplicativo de manera mensual en los tiempos indicados en este manual.

Registro de Nuevos Riesgos: cuando se identifique un nuevo riesgo hay que documentarlo en la herramienta de seguimiento al plan de acción en el módulo de seguimiento a riesgos como lo indicado previamente en el capítulo de Identificación de riesgos.

Informe de Riesgos: El registro a los riesgos debe ser actualizado para reflejar cualquier cambio de respuesta previamente acordada para la exposición general al riesgo del proyecto que se realiza posteriormente como resultado de implementar la respuesta a los riesgos.

Registro de Riesgos: Se designa el colaborador responsable de registrar el seguimiento a las actividades de control. El colaborador es seleccionado por el líder de la iniciativa quien registra en el aplicativo "ASPA" en registro de riesgos – Usuario responsable. La periodicidad de realizar el seguimiento a los controles de las iniciativas y proyectos con el fin de evitar o minimizar la materialización de los riesgos debe ser como mínimo una vez al mes y gestiona de manera directa el día a día de los riesgos identificados para la iniciativa a su cargo.

Informe a los Riesgos: Este informe lo realiza la Oficina Asesora de Planeación de manera mensual donde consulta el ASPA en el módulo seguimiento a Riesgos y genera un reporte de riesgos de las iniciativas y proyectos que componen el Plan de Acción con el objetivo de verificar cuales riesgos se han materializado bien sea dentro de la ejecución o por solicitudes de cambio. Verifica que los nuevos riesgos que surgen a lo largo de la ejecución de las Iniciativas y Proyectos que conforman el plan de Acción de nuestra Entidad estén registrados con la información completa, verifica que todos los enlaces responsables del registro hayan cumplido con esta tarea cada mes, por último, el profesional del GIT de Planeación y Seguimiento elabora un informe mensual de lo hallado y registrado en el ASPA.

Los activos de los procesos de la organización que pueden influir en el proceso de implementar la respuesta a los riesgos incluyen entre otros el repositorio de lecciones aprendidas de proyectos terminados y similares que indican la efectividad de determinadas respuestas a los riesgos.

El seguimiento a los riesgos lo registra el enlace autorizado por el líder de la iniciativa en el mes que realizó la modificación objeto de solicitud de cambio, como riesgo

materializado, diligenciando el módulo que trae el aplicativo designado como “seguimiento” describiendo las acciones correctivas que implementaran para evitar que el riesgo vuelva a materializarse y hacerle el correspondiente seguimiento.

10.6.2.1.6. MONITOREAR Y CONTROLAR LOS RIESGOS:

Consiste en monitorear y hacer seguimiento a los riesgos identificados, analizar e identificar nuevos riesgos y evaluar la efectividad de la gestión de riesgos a lo largo de las iniciativas y proyectos que conforman el plan de acción, permite que las decisiones de los proyectos se basen en la información sobre la exposición al riesgo de los diferentes proyectos que se están ejecutando. El proyecto debe ser monitoreado continuamente en busca de riesgos nuevos, cambiantes y obsoletos y de cambios en el nivel del riesgo general del proyecto.

El control de los riesgos de las iniciativas y proyectos lo debe realizar cada dependencia del MinTIC con el líder de la iniciativa, el responsable del proyecto y su equipo. Se identifican las acciones preventivas y se implementa la respuesta a los riesgos, se realiza el seguimiento a los riesgos identificados, se monitorean los riesgos, se identifican los nuevos riesgos dentro de la ejecución de las iniciativas y proyectos, y se evalúa la efectividad de la de gestión de los riesgos.

Para registrar el resultado de la evaluación de la efectividad de la gestión del riesgo en cada dependencia se define el colaborador responsable de registrar el seguimiento a las actividades de control. El colaborador asignado para registrar el seguimiento al control debe ser seleccionado por el líder de la iniciativa y se debe registrar en el aplicativo ASPA en registro de riesgos – Usuario responsable teniendo siempre la precaución de no eliminar la trazabilidad que trae la iniciativa y proyecto. La periodicidad de realizar el seguimiento a los controles de las iniciativas con el fin de evitar o minimizar la materialización de los riesgos debe ser como mínimo una vez al mes y debe gestionar de manera directa el día a día de los riesgos identificados para la iniciativa a su cargo.

En el control de los riesgos debe dejar evidencia de ejecución, esta evidencia debe reposar en los archivos del área correspondiente con el fin de ser presentadas cuando las circunstancias lo requieran, igualmente debe ser registrado este seguimiento en el aplicativo ASPA en: Registro ASPA – Seguimiento, y diligenciar completamente la información que el aplicativo solicita.

Las herramientas más usadas para controlar los riesgos son las reuniones del proyecto, revaluación de riesgos, autoevaluación a los riesgos, indicadores, el estado de avance del proyecto y registro de riesgos materializados. Estas herramientas se aplicarán según lo estime el responsable del proyecto, las cuales se describen a continuación:

a) Reuniones: la gestión de los riesgos debe ser un punto del orden del día en las reuniones periódicas sobre el estado de las iniciativas y proyectos que pueden ser tratadas en los grupos primarios estas son efectivas allí se discute cómo va el proyecto frente a lo que planificó, dado que permite involucrar al equipo y tener una retroalimentación directa e inmediata. El tiempo requerido para tratar este asunto variará en función de los riesgos que se hayan identificado, su prioridad y la dificultad de respuesta. La gestión de riesgos se torna más sencilla conforme se practica con mayor frecuencia. Los debates frecuentes sobre los riesgos aumentan las posibilidades de que las personas identifiquen los riesgos y las oportunidades.

b) Revaluación de riesgos: Esta técnica significa volver a evaluar los riesgos durante la ejecución del proyecto, se recorre riesgo a riesgo se evalúan nuevamente ya que estos no son estáticos pueden volverse más o menos importantes, cambiar de prioridad, puede dar lugar a nuevos riesgos se utilizan las mismas herramientas que se utilizaron para evaluar los riesgos la primera vez. Al utilizar esta técnica aseguramos que el riesgo siga vigente.

c) Autoevaluación a los riesgos: se puede realizar las autoevaluaciones de riesgos y, si es el caso, deben realizarse con una frecuencia adecuada, Estas se pueden incluir en las reuniones de rutina de revisión de las iniciativas y proyectos, o bien, pueden celebrarse reuniones específicas de autoevaluación de riesgos si el equipo así lo decide. Permite al líder de la iniciativa junto con su equipo adoptar medidas y tomar decisiones enfocadas en cumplir con los objetivos establecidos. Esta técnica permite identificar y medir su propia exposición a efectos de corregir de manera oportuna las deficiencias.

d) Indicadores: se sugiere como buena práctica hacer análisis del comportamiento y tendencia de los indicadores asociados al proyecto para determinar la existencia de la materialización de un riesgo.

e) Estado de avance de las iniciativas y proyectos: el responsable del proyecto junto con el equipo deberá tener conocimiento del estado de avance del proyecto a través del cumplimiento de indicadores, actividades y entregables. Esto para cada uno de los proyectos que contemplan las iniciativas.

f) Riesgos materializados: La posibilidad de materialización de un riesgo siempre está presente, así que permanentemente se debe revisar los procesos y medidas de contingencia para validar su pertinencia en las circunstancias actuales, se debe actuar lo más pronto posible para mitigar el impacto que éste genera y evitar su repetición.

La revisión de la gestión de los riesgos lo realizará la Oficina Asesora de Planeación y Estudios Sectoriales- OAPES.

Durante el ciclo de vida del proyecto se debe realizar monitoreo a los riesgos identificados y a los controles definidos a través de reuniones de seguimiento y el monitoreo de la gestión de riesgo efectuadas por las dependencias registradas en el aplicativo ASPA.

Este monitoreo se registra en el aplicativo ASPA, en el módulo “Seguimiento” durante los cinco primeros días calendario del mes siguiente. En caso de no cumplirse con esta actividad el colaborador de la OAPES, solicita dentro de los dos días calendario al vencimiento del primer plazo, la realización de dicha actividad mediante correo electrónico al colaborador responsable del área de registrar este seguimiento con copia al líder de la iniciativa; si persiste el incumplimiento, el colaborador comunica al coordinador de planeación y seguimiento, para que este reitere mediante correo electrónico el registro de la información; si persiste el incumplimiento y no se ha recibido comunicación o registro de seguimiento en el ASPA, el Jefe de la OAPES solicitará mediante oficio el cumplimiento de esta actividad dentro de los tres días al recibo de la comunicación.

10.7. ADMINISTRACIÓN DE RIESGOS FISCALES

10.7.1. LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

El Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, a través de su Modelo Integrado de Gestión, se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida, enfocado en la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6)

10.7.1.1. OBJETIVO DE LA POLÍTICA

Establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

Las acciones que se tomarán en el desarrollo de esta política son:

- Generar estrategias para el monitoreo y revisión de la administración de riesgos fiscales, con el propósito que la Alta Dirección tome decisiones para la mejora

continua del Modelo Integrado de Gestión y su articulación con el Modelo de Responsabilidad Institucional.

- Desarrollar al interior de la entidad una cultura organizacional que genere una gestión más preventiva y menos correctiva. Realizar la revisión o revaloración del riesgo como mínimo una vez al año.
- Las acciones formuladas para mitigar los eventos de riesgo deberán tener una vigencia máxima de un año y solo podrán ser cerradas si se ha cumplido con el total de actividades propuestas y cumple con lo mencionado en el MIG-TIC-PR-003 Formulación, seguimiento y cierre de acciones de mejora. En el caso de que no sea posible la mitigación dentro de la vigencia indicada anteriormente, será el Comité MIG tras una evaluación quién tome la decisión de prolongar las acciones de tratamiento de los riesgos.
- Verificar que los planes de mejoramiento derivados de la administración de riesgos (planes de tratamiento de riesgo, y acciones de mejora por eventos de riesgo materializados) tengan una vigencia máxima de un año y sean gestionados y cerrados en este período.

10.7.1.2. ALCANCE DELAPOLÍTICA

La política de riesgos es aplicable a todos los procesos que hacen parte del Sistema Integrado de Gestión del Ministerio/Fondo de Tecnologías de la Información y las comunicaciones

10.7.1.3. NIVELES DE ACEPTACIÓN O TOLERANCIA ALRIESGO

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido que para los riesgos de gestión del Ministerio el nivel de aceptación se aplica a todos los riesgos que se ubiquen a nivel residual en una zona de riesgo bajo y moderado, ya que los controles son suficientes y el nivel de riesgo sería aceptable.

10.7.1.4. NIVELES PARA LA CALIFICAR LA PROBABILIDAD

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

Para la calificación de la probabilidad de los riesgos de gestión se establecen los siguientes 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%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10.7.1.5 NIVELES PARA CALIFICAR ELIMPACTO

Por "impacto" se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo. Para la calificación del nivel de impacto se toma como referencia las consecuencias potenciales mencionadas en las siguientes tablas de niveles de impacto para cada tipo de riesgo que se esté calificando. El criterio se adaptará a la realidad del riesgo que se esté calificando.

El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Para la calificación del impacto de los riesgos de gestión se tiene la siguiente tabla de Criterios:

	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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10.7.1.1. TRATAMIENTODERIESGOS

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Reducir el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

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

Transferir el riesgo: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

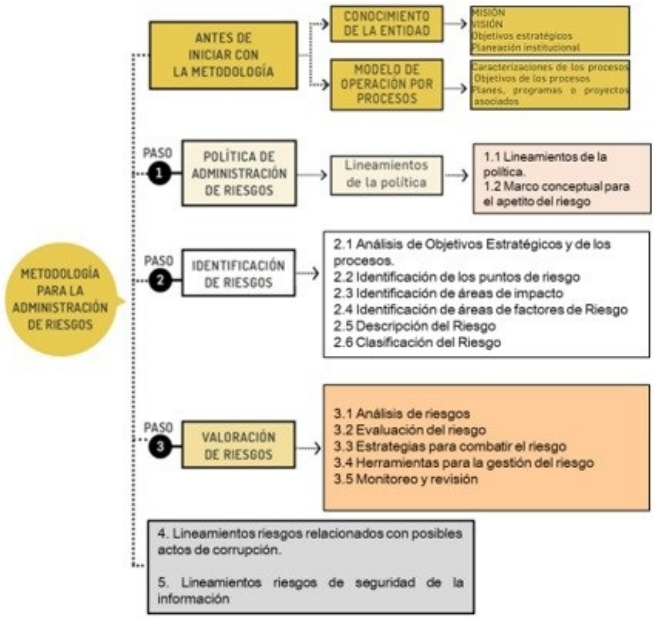
Mitigar: (Plan de Acción) Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

10.7.2. ESTRUCTURAPARALAGESTIÓNDERIESGOS

10.7.2.1 ETAPAS PARALAADMINISTRACIÓNDELRIESGO

En la Administración del riesgo el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones sigue las etapas de identificación, medición, control y monitoreo del riesgo en los procesos, teniendo como referencia Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública (DAFP).

A continuación, se presentan las etapas para la administración de los riesgos de gestión especificando los lineamientos adicionales que aplican en el Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones.



Fuente: elaborado por el Ministerio TIC, tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5

10.1.2.1.1. ESTABLECIMIENTO DELCONTEXTO

El contexto estratégico define los parámetros internos y externos que se deben tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Teniendo en cuenta que las organizaciones son dinámicas, es necesario analizar los datos históricos, teóricos, opiniones informadas y las necesidades de cada proceso. Para ello el Grupo Interno de Trabajo de Transformación Organizacional dispone de un instrumento para la recolección de la información relacionada con el contexto y la identificación de las partes interesadas que pueden afectar los procesos "Formato para el establecimiento del contexto", en el cual se analizan las siguientes temáticas:

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

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

NOTA: Los factores relacionados son una guía, cada entidad puede analizar los que considere de acuerdo con la complejidad propia de cada entidad y con sector en el que se desenvuelve, entre otros aspectos que puedan llegar a ser pertinentes para el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo. Es una referencia de información general para el Mintic y se alimenta de la información que requieran los diferentes sistemas de gestión para establecer su contexto.

Determinar los factores generadores de riesgos de corrupción (aplica para los riesgos de corrupción): ocasionados entre otras cosas por la misión, por las funciones que desarrolla y el sector al que pertenece la entidad.

El Ministerio de Tecnologías de la Información y las Comunicaciones ha establecido para el análisis de su contexto para sus procesos, así como para el análisis de los riesgos la metodología DOFA (Debilidades – Oportunidades – Fortalezas – Amenazas), la cual consiste en identificar en tiempo real aquellas cuestiones del entorno (contexto externo): amenazas (Factores Negativos Externos) y oportunidades (Factores Positivos Externos) y al interior de la entidad (contexto interno): debilidades (Factores Negativos Internos) y fortalezas (Factores Positivos Internos). Esta actividad se realiza en forma participativa para todos los procesos de la Entidad.

10.1.2.1.1. IDENTIFICACIÓN DELRIESGO

Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

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. Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

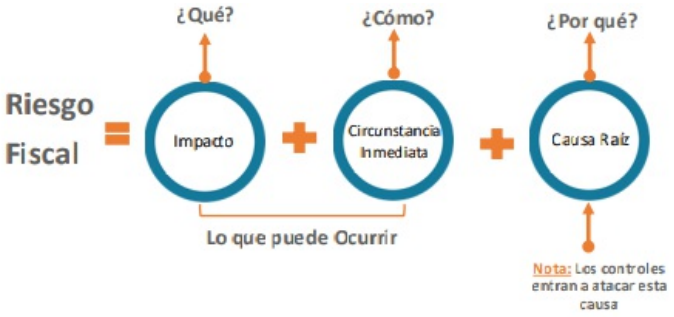
Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias Inmediatas. Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal. Para las circunstancias inmediatas, se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Descripción del Riesgo Fiscal A continuación, se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos.

Para redactar un riesgo fiscal se debe tener en cuenta:



✓ Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.

✓ Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

✓ Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.

✓ Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se general. De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

¿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

10.7.2.1.3. VALORACIÓN DELRIESGO

Evaluación de riesgos Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes. **Probabilidad** La probabilidad es 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 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal. Teniendo esto de presente, para definir el nivel de probabilidad, se ha de tener en cuenta la siguiente tabla definida:

	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%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá 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, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la siguiente tabla definida en el numeral 3.1 de la presente guía

	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

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

10.7.3. VALORACIÓN DELRIESGO

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. Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

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. (ver Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP - última versión).

10.1.2.1.4. DEFINICIÓN Y APROBACIÓN DE PLANES DE ACCIÓN

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de fiscales de la Entidad, el gestor del proceso procederá a cargar el documento interno llamado “Mapa de riesgos del proceso” para que surta el proceso de aprobación documental por parte del líder y de la Oficina Asesora de Planeación a través de la herramienta SIMIG.

Así mismo se deben clasificar aquellos riesgos cuya calificación residual se encuentren en zona Media, Alta o Extrema en el mapa de calor. En estos casos, los procesos en los cuales se obtenga dicha calificación residual deberán formular un plan de acción dentro del mapa de riesgos del proceso tal como lo menciona la Guía para la administración del riesgo emitida por el DAFP. El seguimiento al cumplimiento de las actividades propuestas será llevado para conocimiento y análisis al Comité MIG.

10.1.2.1.5. MATERIALIZACIÓN

Con el propósito de realizar una revisión objetiva de la valoración de los controles de los riesgos de gestión identificados, la entidad estimó conveniente diseñar un instrumento mediante el cual se registre dicha información, conformando una base de datos sobre eventos de riesgos materializados, la cual permitirá contar con información de tendencias y causas de aquellos presentados, para controlar la ocurrencia futura de los mismos.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Gestor de Procesos avalado por el Líder de Procesos al buzón MIG@mintic.gov.co, en el cuál debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado (opcionalmente), proceso en donde se identificó el suceso, impacto, acciones adelantadas y consecuencias. Este reporte debe realizarse mensualmente o cuando el evento de riesgo materializado se presente.

El Grupo Interno de Trabajo de Transformación Organizacional, debe validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos, y presentar en los casos requeridos, ante el Comité MIG aquellos que deban ser de su conocimiento, revisión y cierre.

La Oficina de Control Interno podrá reportar eventos materializados de riesgo a través de los informes o evaluaciones de auditoria a los diferentes procesos de la entidad. En tal caso el reporte quedará registrado en la matriz de eventos materializados de riesgo y el proceso deberá formular plan de mejora que indique la corrección y actividades que indiquen la acción de mitigación del mismo de tal forma que prevenga su reiteración en un término no superior a dos meses a partir de la identificación del evento.

10.1.2.1.6. MEDICIÓN

Se realiza medición a los avances en la realización de las actividades programadas para el fortalecimiento y apropiación de los lineamientos de riesgos de gestión a través del indicador de eficacia llamado “Cumplimiento del cronograma de gestión”, el cual se reporta en el aplicativo ASPA de la entidad.

El monitoreo y seguimiento de los riesgos de gestión del Ministerio aprobados por los procesos, así como de sus controles, se realiza por parte del grupo interno de trabajo de Transformación Organizacional, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de los controles y reporten las evidencias de los mismos, los profesionales del grupo interno de trabajo de Transformación Organizacional realizan la revisión y validación de esta información e informarán su oportuna gestión registrando su resultado a través del indicador

N.211 llamado “Controles del Sistema Integrado de Gestión gestionados”, reportado en la herramienta SIMIG, que tiene como propósito medir el nivel de cumplimiento en la ejecución de los controles de los riesgos de gestión del Ministerio.

Los procesos que obtengan un rango bajo en la medición del indicador por no gestionar sus controles en la fecha límite informada para su gestión, deberán ir al Comité MIG a explicar las razones de su incumplimiento y formular el plan de mejora que evite que vuelva a suceder.

El Ministerio mantiene una base de datos de eventos materializados de riesgos a los cuales se les mide el cumplimiento de la gestión de los eventos materializados en la entidad mediante el indicador N.229 llamado “Eventos de riesgos que se materializaron gestionados” de manera mensual.

El monitoreo se realiza dentro de la entidad teniendo en cuenta las líneas de defensa mencionados en el numeral 8. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO.

11. OPORTUNIDAD DE MEJORA

El Ministerio/Fondo de Tecnologías de la Información y las comunicaciones no sólo deberá centrarse en los riesgos encontrados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

12. CAPACITACIÓN Y APROPIACIÓN

El Grupo Interno de Trabajo de Transformación Organizacional debe liderar la formulación y ejecución de las capacitaciones a impartir a los colaboradores de la Entidad sobre la administración de riesgos, para lo cual puede apoyarse en proveedores o expertos externos o internos.

Es responsabilidad del Grupo Interno de Trabajo de Transformación Organizacional la ejecución de las actividades de capacitación sobre la administración de riesgos.

Los líderes de proceso están a cargo de divulgar al interior de sus equipos de trabajo las políticas, procedimientos y responsabilidades propias de la administración de riesgos, los mapas de riesgo de sus procesos, monitoreo a los controles para mitigar dichos riesgos y sus correspondientes planes de tratamiento; y también son responsables de promover su cumplimiento.

Los líderes de proceso deben promover y permitir la asistencia a las capacitaciones que se programen en el proceso de implementación y mantenimiento de la administración de riesgos

13. AUDITORIA INTERNA

Como resultado de las evaluaciones programadas, se debe diseñar un informe detallado que incluya el producto de la planeación versus lo ejecutado, haciendo énfasis en las recomendaciones y hallazgos. Con base en este informe detallado, se diseña un informe ejecutivo en el que se resuman los aspectos más importantes de la evaluación (especificando si la misma se hizo por proceso o tarea). Este esquema es ejecutado por la Oficina de Control Interno en ejecución de sus funciones.

Clasificación de la Información:Pública

VERSIÓN	FECHA	DESCRIPCIÓN
1	16/Abr/2014	Adopción.
2	28/Feb/2017	Cambio de la denominación del manual de "Política de Administración de Riesgos" a "Lineamientos para la Administración de Riesgos". Se actualizó el contenido del documento de acuerdo a la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República. Se elimina el mapa de riesgos que se encontraba consignado en la versión anterior.
3	10/Oct/2017	Se actualiza la introducción y objetivo, se modifica el pie de página 1 "Las políticas de administración de riesgos de gestión y corrupción relacionadas en este documento se encuentran en aprobación", por "Las políticas de administración de riesgos de gestión y corrupción fueron aprobadas mediante la Resolución 548 de 2017". Se ajusta el numeral Registro de Eventos de Riesgos de Gestión.
4	28/Mar/2018	Se articulan los lineamientos de la administración de riesgos de la Entidad, con el MiPG, MECI y el manual DES-TIC-MA-008 Metodología de Gerencia de Proyectos. Se incluye la política y metodología de administración de riesgos de proyectos.
5	30/Nov/2018	Se incluye la política y metodología de administración de riesgos de Seguridad de la Información
6	30/Jul/2019	Se incluye los lineamientos acorde a la nueva Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital y los lineamientos aquí establecidos para la Administración de Riesgos de Gestión, Corrupción, Proyectos y de seguridad y privacidad de la información, seguridad digital y continuidad de la operación.
7	28/Ago/2020	Se retiran lineamientos referentes a los riesgos de Gerencia de Proyectos, Se menciona una política integral de riesgos. Se mencionan excepciones a la Guía para la administración de riesgos y diseño de controles del DAFP. Se agregan lineamientos específicos para los riesgos de Seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios y se agregan las tablas de impacto. Se actualiza definiciones, normatividad, documentos asociados, la dimensión de seguimiento, control y mejora, las responsabilidades en la gestión del riesgo de la entidad en el marco del esquema de las líneas de defensa del Sistema Integral de Control Interno.
8	24/Jun/2021	Se ajusta la política de riesgo enfocado al Sistema Integrado de Gestión, enfoque al tema el aprovechamiento al máximo los recursos, prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos. Se incluye la metodología de riesgos para el sistema de seguridad y salud en el trabajo y sistema de gestión ambiental. Se define la estructura para la gestión del riesgo particular para cada sistema de gestión acorde a lo mencionado en la resolución 1092 de 2021 - Establece el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones.
		. Se actualizó parcialmente el objetivo

9	23/Dic/2021	. Se incorporó nuevas definiciones. . Se ordenó por jurisprudencia normativa, el ítem de normatividad . Se actualizó el capítulo "Roles y responsabilidades en la gestión del riesgo"
10	11/Abr/2022	Ajuste en el alcance, normatividad y documentos asociados. Ajuste en los capítulos 10.1. ADMINISTRACIÓN DE RIESGOS DE GESTIÓN y 10.3. ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS. Inclusión de formatos para contexto y mapas de riesgos que apoyarán la implementación de los lineamientos que aprueba el Comité.
11	13/Jun/2022	1.En la sección 3. Definiciones, se adicionó la definición de Fuente de amenaza, Interrupción y Riesgo de interrupción. 2.Se especificó la palabra riesgos de interrupción en las siguientes secciones: 10.3.1. Lineamientos de la política de administración de riesgos 10.3.1.1. Objetivo de la política 10.3.1.2. Alcance de la política 10.3.1.3. Niveles de aceptación o tolerancia al riesgo 10.3.1.4. Niveles para calificar el impacto 10.3.2.1. Etapas en la administración del riesgo 10.3.2.1.1. Establecimiento del contexto 10.3.2.1.2. Identificación del riesgo 10.3.2.1.3. Valoración del riesgo 10.3.2.1.4. Definición y aprobación de mapas de riesgos y planes de tratamiento 10.3.2.1.6. Medición 3.En la sección 10.3.2.1.2. Identificación del riesgo, se establece la nueva categoría de interrupción y se definen campos específicos para este tipo de riesgo 4.En la sección 10.3.2.1.3. Valoración del riesgo, se adiciona un párrafo mencionando la particularidad de los controles partiendo del del criterio denominado custodio del activo
12	29/Nov/2022	. Se actualiza la política de riesgos enfocando a los riesgos de gestión y a la ejecución de los políticas, planes, programas y proyectos, y se cambia el término corrupción por Transparencia y Ética. . Se agregan excepciones a la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5. . Se actualiza el capítulo 10.6 riesgos de proyectos e iniciativas, normatividad, concepto de acción de mitigación y eliminación del término disparador.
13	26/May/2023	. Se enfocan los lineamientos a la Guía para la administración del riesgo y el diseño de controles en entidades públicas - V6. . Se menciona la aprobación de los mapas de riesgos por parte del líder se realizará por medio flujo de aprobación documental de la herramienta SIMIG. Y para el caso en el cual el riesgo quede en zona alta o extrema se generan planes de acción cuyo seguimiento al cumplimiento se presenta ante el Comité MIG, tanto para los riesgos de gestión como para los riesgos de corrupción. . Se incluye dentro de la materialización de los riesgos de gestión, que la Oficina de Control Interno tiene la potestad de registrar eventos materializados de riesgos a cualquier proceso como resultado de una evaluación o auditoria, ante lo cual el proceso se verá obligado a presentar el plan de mejora que corrija y evite de nuevo su materialización en un término no superior a 1 mes. . Se aclaran los criterios específicos para definir un producto como crítico para la entidad en la identificación de riesgos, en el numeral de excepciones de la guía.
14	29/Ago/2023	Se especifican las líneas de defensa según los lineamientos DAFP. Se crea el capítulo N.10.7 en donde se especifica cómo se identifican, valoran y controlan los riesgos fiscales. Se actualiza el glosario y normatividad con enfoque a los riesgos fiscales. En el tema de seguridad y privacidad de la información. se realizan los siguientes ajustes: 1. Se complementó la sección de Identificación del riesgo, Adicionando los aspectos importantes a tener en cuenta para determinar cuáles son los activos de información afectados, siguiendo los lineamientos de los documentos GDO-TIC-MA-014 Manual de Activos de Información y el GDO-TIC-PR-019 Procedimiento Activos de Información, Adicionando que la identificación de las posibles amenazas y vulnerabilidades es apoyada por el catálogo definido en el anexo 4 "Lineamientos para la gestión del riesgo en entidades públicas", Precisando que la actualización de los riesgos de interrupción está sujeto por la actualización de la documentación correspondiente al Plan de Continuidad del Negocio (BCP) y específicamente al documento del Análisis de Impacto al Negocio (BIA). Se complementó la sección de valoración del riesgo especificando que los controles definidos para mitigarlos deben estar asociados a los controles determinados en el anexo A de la ISO 27001 y complementando las variables que debe tener un control (tipo de control: preventivo, detectivo o correctivo e implementación: manual o automático). Se ajustó la sección definición y aprobación de mapas de riesgos y planes de tratamiento donde de acuerdo con los lineamientos de la OAPES se determinó que el proceso de aprobación de los mapas de riesgos se debe realizar a través de SIMIG y no por memorando como inicialmente se venía realizando.
15	17/Ene/2024	* Se actualiza Resolución del MIG No. 2175 de 2022 por la Resolución No. 4870 de 2023. * Se ajusta el numeral 10.1.2.1.8. EXCEPCIONES DE LA GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS. * Se incluye en la nota en el Numeral 10.1.2.1.2. IDENTIFICACIÓN DELRIESGO. Los riesgos del proceso de Direccionamiento Estratégico serán considerados como los "Riesgos Estratégicos"de la Entidad.

ELABORÓ	REVISÓ	APROBÓ
	Nombre: Carolina Castañeda de Avila **Cargo:** Coordinador	**Nombre:** Juddy Alexandra Amado Sierra **Cargo:** Jefe de Oficina

		Fecha:	12/Abr/2024	**Fecha:**	22/Abr/2024
		Nombre:	Giovanni Andres Espitia Roa	**Nombre:**	Carolina Castañeda de Avila
		Cargo:	Contratsta	**Cargo:**	Coordinador
		Fecha:	11/Abr/2024	**Fecha:**	19/Abr/2024
		Nombre:	Diego Mauricio Reyes Vargas	**Nombre:**	Angela Janeth Cortes Hernandez
		Cargo:	Profesional Especializado	**Cargo:**	Oficial de Seguridad y Privacidad de la Información
Nombre:	Susen Dayana Mateus Vargas	**Fecha:**	11/Abr/2024	**Fecha:**	15/Abr/2024
Cargo:	PROFESIONAL UNIVERSITARIO	**Nombre:**	Laura Maria Melendez Galvis	**Nombre:**	Cesar Giovanni Artunduaga Higuera
Fecha:	26/Mar/2024	**Cargo:**	Contratista	**Cargo:**	Subdirector para la Gestion de Talento Humano
		Fecha:	10/Abr/2024	**Fecha:**	12/Abr/2024
		Nombre:	Esmeralda Carolina Orduz Olaya	**Nombre:**	Sohe Munoz Orozco
		Cargo:	Contratista	**Cargo:**	Subdirector Administrativo
		Fecha:	07/Abr/2024	**Fecha:**	12/Abr/2024
		Nombre:	Ahimer Andres Pardo Moreno		
		Cargo:	Contratista		
		Fecha:	27/Mar/2024		