Manual metodológico para la administración integral de riesgos Instituto de Tránsito del Atlántico

V4 - 2021

Manual metodológico para la administración integral del riesgo

Instituto de Tránsito del Atlántico

V4 - 2021

Susana Cadavid
Director

Tabla de contenido

INTRODUCCIÓN 5

PRESENTACIÓN 6

CAPÍTULO 1. MARCO NORMATIVO 7

CAPÍTULO 2. MARCO CONCEPTUAL 8

CAPÍTULO 3. CONSIDERACIONES GENERALES 10

3.1. MAPA DE RIESGOS INSTITUCIONAL 10

3.2. PRIORIZACIÓN DE RIESGOS A CONTROLAR 10

3.3. SEGUIMIENTO Y MONITOREO 10

3.3.1. AUTOCONTROL 11

3.3.2. EVALUACIÓN INDEPENDIENTE 11

3.4. RECURSOS 11

3.5. DIVULGACIÓN 11

3.6. TIPOLOGÍA DEL RIESGO 12

CAPÍTULO 4. PROCEDIMIENTO PARA LA ADMINISTRACIÓN INTEGRAL DE LOS RIESGOS DE GESTIÓN, SEGURIDAD DE LA INFORMACIÓN Y DE CORRUPCIÓN 14

4.1. ANTES DE LA METODOLOGÍA 0

4.1.1. ALINEACIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN 0

4.1.2. ESQUEMA DE LÍNEAS DE DEFENSA 0

4.2. PASO 1: FORMULACIÓN DE LA POLÍTICA INSTITUCIONAL PARA LA ADMINISTRACIÓN INTEGRAL DEL RIESGO 1

4.3. PASO 2. IDENTIFICACIÓN DEL RIESGO 2

4.3.1. CONTEXTO ESTRATÉGICO 2

4.3.2. ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS 4

4.3.3. IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO 5

4.3.4. IDENTIFICACIÓN DE ÁREAS DE IMPACTO 6

4.3.5. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO 6

4.3.6. Descripción del riesgo 8

4.4. PASO 3. VALORACIÓN DE LOS RIESGOS 12
4.4.1. ANÁLISIS DEL RIESGO 13
4.4.2. EVALUACIÓN DEL RIESGO 20
4.3. ESTRATEGIAS PARA COMBATIR EL RIESGO 35
4.4. GESTIÓN DE EVENTOS 37
4.5. INDICADORES CLAVES DE RIESGO 37

Ilustración 1. Identificación del Contexto estratégico 3
Ilustración 2. Cadena de valor 5
Ilustración 3. Áreas de impacto 6
Ilustración 4. Estructura descripción del riesgo de gestión y seguridad de la información 9
Ilustración 5. Estructura propuesta riesgos de corrupción 9
Ilustración 6. Evaluación de los riesgos 13
Ilustración 7. Frecuencia actividades comunes gestión pública 14
Ilustración 8. Instrumento matriz de riesgos de gestión y seguridad de la información sección análisis del Riesgo inherente formato SIG-M06A 19
Ilustración 9. Instrumento matriz de riesgos de corrupción sección análisis del Riesgo inherente formato SIG-M06A 20
Ilustración 10. Figura 14 Matriz de calor (niveles de severidad del riesgo) 20
Ilustración 11. Estructura propuesta aplicación control 22
Ilustración 12. Ciclo del proceso y tipologia de controles 23
Ilustración 13. Definición controles riesgos de gestión y seguridad de la información 24
Ilustración 14. Definición controles riesgos de corrupción 26
Ilustración 15. Movimiento en la matriz de calor 30
Ilustración 16. Instrumento matriz de riesgos de gestión y seguridad de la información sección evaluación del riesgo - valoración de los controles formato SIG-M06A 31
Ilustración 17. Instrumento matriz de riesgos de corrupción sección evaluación del riesgo - valoración de los controles formato SIG-M06B 31
Ilustración 18. Instrumento matriz de riesgos gestión y seguridad de la información sección evaluación del riesgos - Nivel del riesgo residual ejemplo aplicado formato SIG-M06A 34
Ilustración 19. Instrumento matriz de riesgos de sección evaluación del riesgos - Nivel del riesgo residual riesgos de corrupción sección evaluación del riesgo – Nivel del riesgo residual formato SIG-M06B 34
Ilustración 20. Movimiento en la matriz de calor con el ejemplo propuesto 35
Ilustración 21. Instrumento matriz de riesgos de sección plan de acción o tratamiento, continuación ejemplo aplicado 36
Ilustración 22. Continuación ejemplo aplicado sección indicadores clave de riesgo 38

Tabla 1. Marco normativo Manual de administración integral del Riesgo 8

Tabla 2. Clasificación del riesgo de gestión 13
Tabla 3. Instrumento matriz de riesgos de gestión y seguridad de la información sección identificación del riesgo. Formato mapa de riesgos SIG-M06 10
Tabla 4. Instrumento matriz de riesgos de corrupción sección identificación del riesgo. Formato mapa de riesgos SIG-M06 11
Tabla 5. Criterios de probabilidad Riesgos de Gestión y Seguridad de la información 14
Tabla 6. Criterios de Probabilidad Riesgos de corrupción 14
Tabla 7. Tabla criterios de impacto de riesgos de gestión y seguridad de la información 17
Tabla 8. Tabla criterios de impacto riesgos de corrupción 19
Tabla 9. Atributos de para el diseño del control riesgos de gestión y seguridad de la información 26
Tabla 10. Variables y su ponderación en el diseño del control riesgos de corrupción 27
Tabla 11. Criterios calificación diseño del control de riesgos de corrupción 28
Tabla 12. . Criterios calificación ejecución del control de riesgos de corrupción 28
Tabla 13. Solidez individual controles riesgos de corrupción 29
Tabla 14. Solidez del conjunto de controles riesgos de corrupción 29
Tabla 15. Aplicación tabla atributos a ejemplo propuesto 31
Tabla 16. Aplicación de controles para establecer el riesgo residual riesgos se gestión y seguridad de la información 33
Tabla 17. Solidez conjunto de controles riesgos de corrupción 33

INTRODUCCIÓN

El Instituto de Tránsito del Atlántico, adopta las políticas direccionadas para la administración integral del Departamento Administrativo de la Función Pública –DAFP– de acuerdo a la actualización de la "Guía para la administración y el diseño de controles en entidades públicas v5" de diciembre de 2020; para los riesgos de gestión y seguridad de la información y mantiene la metodología de la "Guía para la administración y el diseño de controles en entidades públicas v4" de octubre de 2018 para los riesgos de corrupción de la entidad.

Para su formulación, se desarrollaron dos matrices una donde se incluirán los riesgos de gestión y seguridad de la información y la otra, donde se incluirán los riesgos de corrupción asociados a los procesos institucionales.

PRESENTACIÓN

El presente documento es el manual operativo de administración integral del riesgo mediante el cual Instituto de Tránsito del Atlántico desarrolla la metodología para la administración y gestión de los riesgos de gestión, seguridad de la información y corrupción por procesos.

El presente documento se constituye en el documento técnico con el cual los funcionarios de la Entidad gestionarán y administrarán sus riesgo, entendidos estos como de gestión, seguridad de la información y corrupción, sus objetivos y los compromisos de la administración para su ejecución, el proceso para el diagnóstico, descripción, análisis, valoración y seguimiento de los riesgos y sus controles para mitigarlos, así como también , el marco legal y conceptual sobre el cual se soporta el mapa de riesgos institucional.

Se pretende que a partir de la identificación y valoración se generen estrategias y acciones preventivas a los riesgos, los cuales al ser controlados y mitigados permitan el cumplimiento de los objetivos misionales y los resultados esperados por cada una de las dependencias de la Entidad.

CAPÍTULO 1. MARCO NORMATIVO

Constitución Política 1991	*Adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno.*
Ley 87 de 1993	*Crea el Sistema Institucional de Control Interno y dota a la administración de un marco.*
Decreto 1537 de 2001	*Provee elementos técnicos y administrativos para fortalecer el Sistema de Control Interno (SCI) Establece la administración del Riesgo se contempla como parte integral del fortalecimiento de los SCI*
Decreto 1599 de 2005	*Adopta un marco general para el ejercicio del Control Interno, a través del Modelo Estándar de Control Interno –MECI y dota al Estado colombiano de una estructura única.*
Decreto 1599 de 2012	*Integra en un solo sistema todas aquellas herramientas de gestión, presenta a las entidades el Modelo Integrado de Planeación y Gestión, el cual recoge el Sistema de Desarrollo Administrativo en cinco políticas MECI se configura como la herramienta de seguimiento y control del Modelo.*
Ley 1523 de 2012	*Adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres*
Decreto 943 de 2014	*Actualiza el MECI a una versión más moderna y de fácil comprensión por parte de las entidades*
Decreto 1443 de 2014	*Implementación del sistema de seguridad y salud en el trabajo (SG-SST)*
Ley 1753 de 2015	*Integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998)*
Decreto 602 de 2017	*Adiciona la Parte 4 del Libro 2 del Decreto 1079 de 2015 y se reglamentan los artículos 84 de la Ley 1523 de 2012 y 12 y 63 de la Ley 1682 de 2013, en relación con la gestión del riesgo de desastres en el Sector Transporte*
Decreto 1499 de 2017	*Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG)*
Decreto 2157 de 2017	*Adopta directrices generales del Plan de Gestión de Riesgo de Desastres*
Guía 2018	*Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018,*
Manual 2019	*Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional Versión 4 -*

	Marzo 2021.
Guía 2020	*Guía de auditoría interna basada en riesgos para entidades públicas - Versión 4 - Julio de 2020.*
Guía 2020	*Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 Diciembre de 2020.*

Tabla 1. Marco normativo Manual de administración integral del Riesgo

CAPÍTULO 2. MARCO CONCEPTUAL[1]

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.

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.

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 es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

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.

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

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

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

[1] Función pública. Guía para la Administración de Riesgos y diseño de controles v5 - Diciembre de 2020

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

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

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

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

MIPG: Modelo Integrado de Planeación y Gestión

Continuidad: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis

Crisis (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata

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

Integridad: Propiedad de exactitud y completitud.

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

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.

Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección consideran que no sería posible el logro de los objetivos de la entidad.

CAPÍTULO 3. CONSIDERACIONES GENERALES

3.1. MAPA DE RIESGOS INSTITUCIONAL

El Mapa de Riesgos institucional contiene, a nivel estratégico, los mayores riesgos a los cuales se encuentra expuesta la entidad, permitiendo conocer las opciones inmediatas de respuesta ante éstos, tendientes a evitar, reducir, compartir o transferir el riesgo; o asumir el riesgo residual y la aplicación de acciones, así como los responsables, el cronograma y los indicadores.

3.2. PRIORIZACIÓN DE RIESGOS A CONTROLAR

El mapa de riesgos institucional se consolidará a partir de aquellos riesgos que muestren una calificación más alta en los mapas de riesgos por proceso, es decir, aquellos riesgos cuya valoración se encuentra en ZONA DE RIESGO ALTA Y EXTREMA, independientemente de la naturaleza de estos. Todos los riesgos de corrupción se incluirán en el mapa de riesgos institucional. Su consolidación se desarrollará en Formato Mapa de riesgos institucional Riesgos de Gestión y seguridad de la información SIG – M06a. En el Formato SIG – M06b se consolidarán los riesgos de corrupción identificados en los procesos institucionales.

3.3. SEGUIMIENTO Y MONITOREO

El seguimiento y monitoreo a la administración del riesgo se encuentra conformado por dos componentes: el primero mediante el autocontrol realizado por los líderes de los procesos y el segundo, mediante la evaluación Independiente realizada por la Oficina Asesora de Control Interno.

3.3.1. AUTOCONTROL

Para realizar el seguimiento a las acciones de respuesta y su efectividad el líder del proceso tendrá en cuenta lo definido en el mapa de riesgos de su proceso, y los indicadores claves de riesgo, el seguimiento se realizarán mensual y bimestralmente de acuerdo al nivel de severidad del riesgo residual.

3.3.2. EVALUACIÓN INDEPENDIENTE

La Oficina Asesora de Control Interno desarrollará el seguimiento y evaluación a los mapas de riesgos de los procesos del Instituto de Tránsito del Atlántico, teniendo en cuenta los procedimientos definidos para tal fin.

3.4. RECURSOS

En cada uno de los elementos de administración de riesgos se contemplarán los recursos necesarios para la definición, implementación y efectividad de las acciones que permitan un tratamiento adecuado de los riesgos, teniendo en cuenta la viabilidad financiera para aplicar dichas acciones conforme a los lineamientos del ordenador del gasto. En el marco del Comité Institucional de Coordinación de Control Interno se aprobarán los recursos requeridos para la implementación de los diferentes planes de acción.

3.5. DIVULGACIÓN

La Política de Administración Integral de Riesgos, el Mapa de Riesgos Institucional, los mapas de riesgos por procesos y el Mapa de Riesgos de Corrupción, se divulgarán a todos los servidores públicos de la Entidad a través de los diferentes medios de comunicación, cada vez que se presente una actualización, conforme con los lineamientos de la estrategia de gobierno en línea.

3.6. TIPOLOGÍA DEL RIESGO

Teniendo en cuenta la naturaleza de la entidad se han determinado los siguientes tipos de riesgos: de gestión, de seguridad de la información y de corrupción.

RIESGOS DE GESTIÓN

Están asociados a la interferencia que puede ocasionar la materialización de una acción que pueda afectar negativamente el logro de los objetivos de los procesos institucionales. Estos riesgos se identifican y/o validan en cada vigencia por los líderes de proceso junto a sus respectivos equipos de trabajo y se clasifican en:

CLASIFICACIÓN	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.

Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Tabla 2. Clasificación del riesgo de gestión

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.

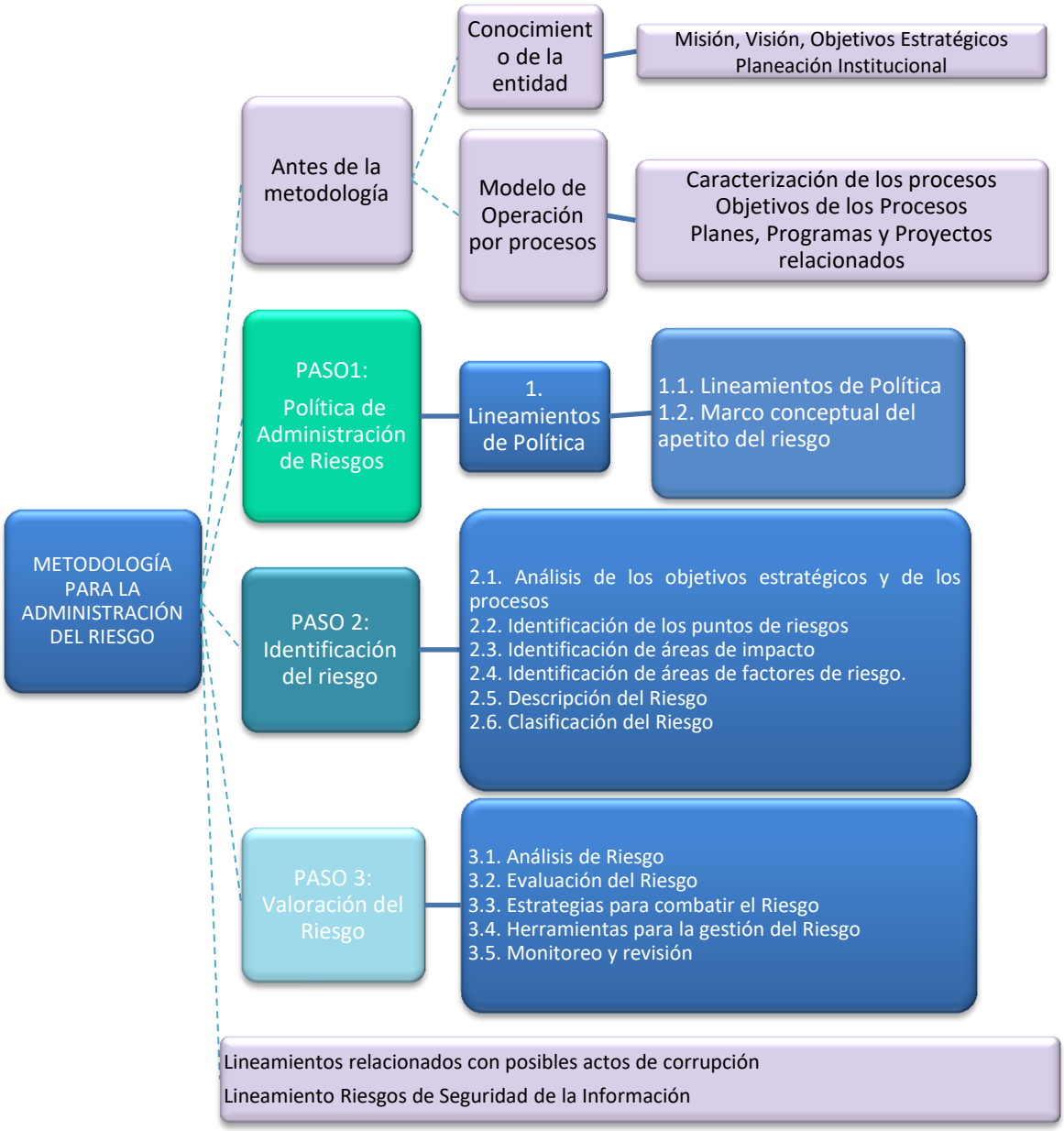
RIESGO DE SEGURIDAD DE LA INFORMACIÓN

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

- Pérdida de la Confidencialidad: cuando la información es divulgada a individuos, entidades o procesos no autorizados
- Pérdida de la Integridad: Cuando la información es manipulada y/o alterada por personas o procesos no autorizados.
- Pérdida de la Disponibilidad: Cuando la información y los sistemas no están disponibles para las personas autorizadas en el momento que así lo requieran.

CAPÍTULO 4. PROCEDIMIENTO PARA LA ADMINISTRACIÓN INTEGRAL DE LOS RIESGOS DE GESTIÓN, SEGURIDAD DE LA INFORMACIÓN Y DE CORRUPCIÓN

La administración integral de los riesgos se desarrollará de acuerdo a la siguiente metodología:



4.1. ANTES DE LA METODOLOGÍA

4.1.1. ALINEACIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN

Mediante Decreto 1499 de 2017 se adopta el Modelo Integrado de Planeación y Gestión, el cual articula el sistema de gestión de la entidad y el sistema de control interno a través de siete (7) dimensiones y diecinueve (19) políticas. Sin embargo, para poder identificar cómo se gestionan los riesgos en las entidades se debe entender cuál es su relación directa con MIPG. Teniendo en cuenta lo anterior podemos identificar esa relación de acuerdo al esquema presentado a continuación:

ELEMENTO	DIMENSIÓN	ASPECTOS A TENER EN CUENTA
Planeación Institucional: Misión, Visión, Objetivos Estratégicos	DIRECCIONAMIENTO ESTRATÉGICO Y LA PLANEACIÓN	A partir de la dimensión de direccionamiento estratégico y la planeación se definen los siguientes aspectos: Se genera la política de Administración Integral del Riesgo y se definen los siguientes aspectos claves para la generación de la administración de los riesgos: ✓ Evaluación de Factores de riesgos (análisis interno y externo de la entidad) atendiendo el diagnóstico de capacidades y entornos. ✓ Los riesgos son de la entidad por eso se analizan con base en el mismo entorno. ✓ Planeación estratégica de la Entidad. ✓ Plan anticorrupción y Atención al ciudadano. Dimensión de gestión de riesgos de corrupción.
Caracterización de los procesos Objetivos de los Procesos Planes, Programas, Proyectos relacionados	GESTIÓN CON VALORES PARA RESULTADO	A partir de la dimensión de gestión con valores para resultado se definen los siguientes aspectos: Existen dos políticas que tiene relación directa con la gestión del riesgo. ✓ Política de Fortalecimiento Institucional y gestión de trámites: Los riesgos los identificamos a los procesos, por ello es necesario tener una buena estructura de procesos, procedimientos, políticas, planes, programas y proyectos entre otras herramientas, temas concebidos en cascada desde la misión, visión y objetivos estratégicos ✓ Política de seguridad de la información, debemos identificar los riesgos de seguridad de la información debido a que todos los procesos generan información a través de instrumentos y herramientas de tecnología de la información y comunicaciones para la mejora de procesos ✓ Generar mecanismos para proteger la información, siendo TIC la responsable de la metodología, sin embargo, la información es responsabilidad de todos los servidores y colaboradores de la entidad.
Lineamientos para el diseño y ejecución del control Líneas de defensa	CONTROL INTERNO	A partir de la dimensión de control interno se definen los siguientes aspectos: ✓ Esquemas de las líneas de defensa para la definición de roles y responsabilidades de la gestión del riesgo y del control. ✓ A través de los componentes del MECI. Se evalúa la efectividad de los controles (diseño y ejecución de los controles) específicamente a través del ambiente de control, evaluación del riesgo y actividades de control frente a la gestión y dentro de la gestión lo que va a asegurar que los líderes de procesos puedan identificar desviaciones que aseguren el cumplimiento de los objetivos de procesos y los objetivos institucionales.

EJE ARTICULADOR DEL SISTEMA DE GESTIÓN Y EL SISTEMA DE CONTROL INTERNO = MODELO ESQUEMA LÍNEAS DE DEFENSA

4.1.2. ESQUEMA DE LÍNEAS DE DEFENSA

MIPG se constituye en el sistema de gestión de calidad de la entidad ya que articula el sistema de gestión y el sistema de control interno a través dimensiones y políticas que contienen los parámetros de calidad que se deben ejecutar de manera de adecuada para dar respuesta a nuestros grupos de valor y la dimensión de control interno a través del manejo de los riesgos y de los controles aseguran razonablemente el cumplimiento de los objetivos institucionales.

Por ello, el eje articulador entre el sistema de gestión de la entidad y el sistema de control interno es a través del esquema de las líneas de defensa, las cuales son cuatro:

ESTRUCTURA INTERNA PARA LA ADMINISTRACIÓN INTEGRAL DEL RIESGO

4.2. PASO 1: FORMULACIÓN DE LA POLÍTICA INSTITUCIONAL PARA LA ADMINISTRACIÓN INTEGRAL DEL RIESGO

La formulación de la política está a cargo del representante legal de la entidad en cabeza de la oficina asesora de Planeación y contará con la participación del Comité Institucional de Coordinación de Control Interno. Se deberán tener en cuenta los objetivos estratégicos de la entidad, niveles de responsabilidad frente al manejo de los riesgos, el mapa de riesgos de las vigencias anteriores y los mecanismos para dar a conocer la política a todos los niveles de la entidad.

La política define que debe hacerse para efectuar el control y la implementación de la misma, basándose en los planes estratégicos y los objetivos institucionales o por procesos.

La política es diseñada por la Oficina Asesora de Planeación y aprobada en el marco del Comité Institucional de Coordinación de Control Interno. La política deberá ser aprobada cada vigencia a más tardar el 31 de enero del año en curso y será actualizada de acuerdo a los lineamientos y/o actualizaciones emitidas por el Departamento Administrativo de la Función Pública y demás normas a las que haya lugar.

ASPECTOS QUE DEBE CONTENER:

- El objetivo de la política y su alienación con los objetivos estratégicos.
- El alcance de la política
- Los niveles de aceptación del riesgo.
- Niveles para calificar el impacto.
- Periodicidad del seguimiento según el riesgo residual y evaluación a la implementación y efectividad de los controles.

Ver Política de Administración Integral de Riesgo del Instituto de Transito del Atlántico

4.3. PASO 2. IDENTIFICACIÓN DEL RIESGO

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

4.3.1. CONTEXTO ESTRATÉGICO

Para la identificación de los riesgos se hace necesario evaluar factores externos e internos, a través del análisis diferentes fuentes de información e indagación con los funcionarios de los procesos, los cuales serán tenidos en cuenta para el adecuado análisis de las causas y consecuencias del riesgo en cada proceso y la gestión del mismo:

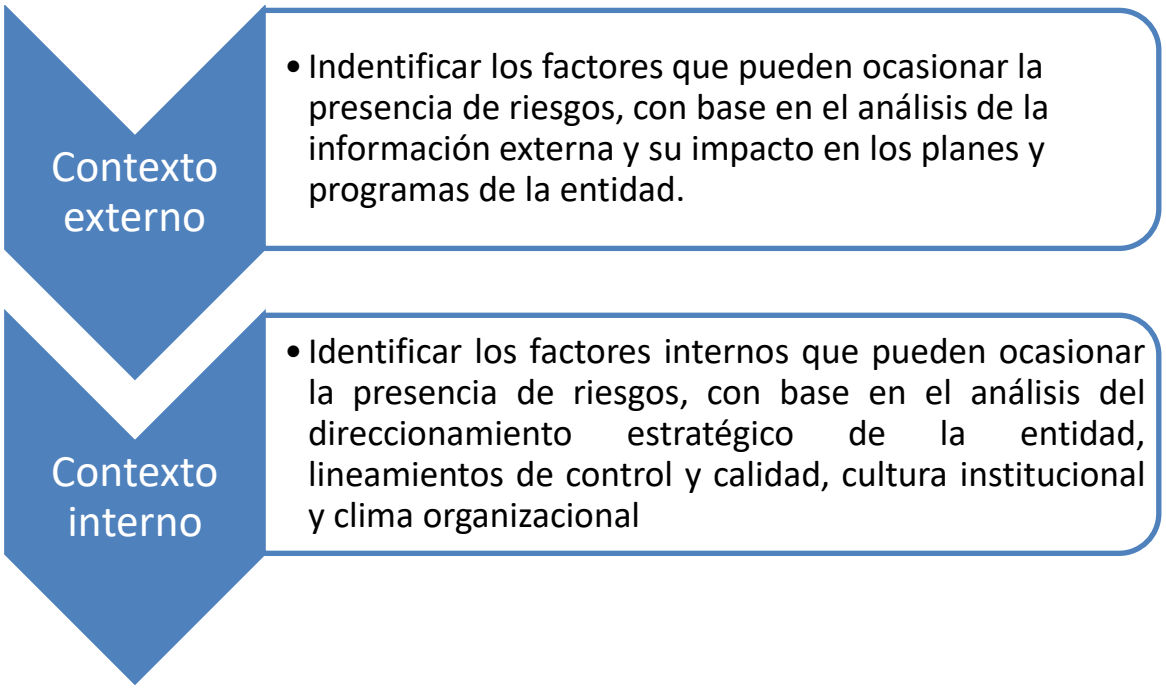


Ilustración 1. Identificación del Contexto estratégico

Analizando el entorno de la del Instituto de Tránsito del Atlántico, se han identificado los siguientes factores a considerar para el adecuado análisis de las causas de los riesgos en cada proceso y la gestión de los mismos:

FACTORES EXTERNOS	FACTORES INTERNOS
Económicos: Disminución del presupuesto por austeridad en el gasto con base en las políticas del Gobierno.	Financieros: Bajo presupuesto de funcionamiento que impide el desarrollo de proyectos.
Medioambientales: catástrofes naturales	Talento humano: Desmotivación de los servidores; Falta de incentivos; Alta rotación, carrera administrativa sin posibilidades de ascenso, falta de capacitación para mejorar la gestión institucional y la innovación en la prestación del servicio.
Políticos: Cambio de gobierno con nuevos planes y proyectos; Falta de continuidad en los programas y proyectos establecidos en la entidad.	Procesos: Desconocimiento de los procesos y procedimientos por parte de los servidores, incoherencia entre procesos establecidos y ejecutados; desactualización de documentos; desconocimiento de la Entidad por parte de otros órganos de gobierno.
SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.	Tecnología: Falta de optimización de sistemas de gestión, falta de coordinación de necesidades de tecnología. Poca implementación de políticas de seguridad de la información
Tecnológicos: Falta de interoperabilidad con	Estratégicos: Falta de lineamientos y demoras

otros sistemas, Fallas en la infraestructura tecnológica, falta de recursos para el fortalecimiento tecnológico	en la Planeación; Desconocimiento y falta de aplicación de políticas de operación por parte de los servidores, no utilización de los indicadores para la toma de decisiones; falta de cultura de planeación al interior de cada unidad; desconocimiento y falta de aplicación de políticas de operación por parte de los servidores y colaboradores.
Comunicación externa: Pocos canales para comunicación externa teniendo en cuenta la cobertura de servicios institucional.	Comunicación Interna: Falta de planeación de las comunicaciones internas. Poca visibilidad del proceso como prioritario por parte de los servidores y colaboradores; baja efectividad en los canales internos; Falta de control sobre los canales establecidos; Ausencia de registros de control de comunicaciones; Información dispersa; Falta de control sobre los canales establecidos, Falta de registros de resultados de reuniones, demoras en bajar la información, poca efectividad en los canales internos.

4.3.2. ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

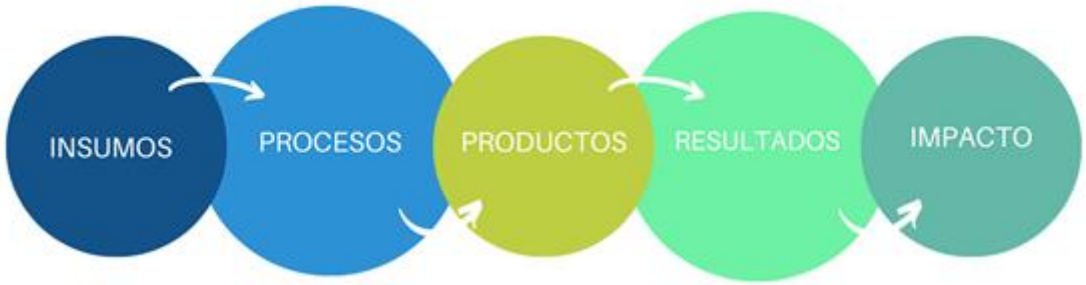
La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucional, así como su desdoble hacia los objetivos de los procesos. Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos. Además de analizar los puntos anteriores con referencia a los objetivos de procesos se debe analizar si estos contribuyen a los objetivos estratégicos.

Es necesario revisar que los objetivos estratégicos y de procesos estén formulados de manera adecuada, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo. SMART.

La entidad debe identificar los posibles riesgos que puedan afectar el cumplimiento de los objetivos estratégicos y que puedan ocasionar su éxito o su fracaso.

4.3.3. IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO

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



Recursos financieros, humanos y materiales empleados para generar los productos.	Actividades realizadas para transformar los insumos en productos.	Bienes y servicios elaborados que requiere la población para satisfacer una demanda o dar respuesta a las causas correctas de un problema.	Cambios en el comportamiento o en el estado de los beneficiarios como consecuencia de recibir los bienes o servicios.	Cambios en las condiciones de vida de la población objetivo. Mayor valor público en términos de bienestar, prosperidad general y calidad de vida de la población

Ilustración 2. Cadena de valor

Los puntos de riesgo pueden identificarse dentro de los procedimientos con aquellas actividades que se desarrollan con el fin de identificar posibles desviaciones y que son catalogadas como puntos de control dentro del procedimiento.

4.3.4. IDENTIFICACIÓN DE ÁREAS DE IMPACTO

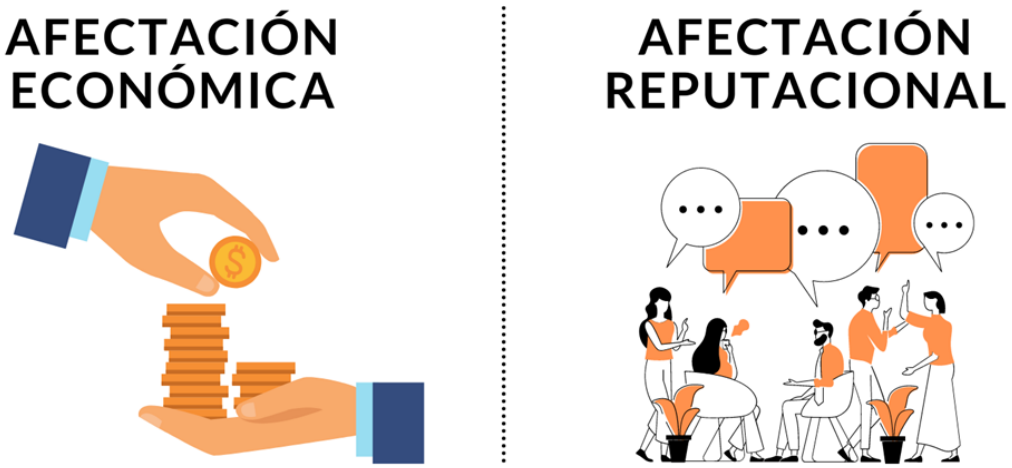


Ilustración 3. Áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional debido a que la entidad puede verse impactada negativamente de dos formas o por disminución de su presupuesto como consecuencia de la materialización de algún riesgo o su imagen frente a la gestión desarrollada.

4.3.5. IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos. Durante el desarrollo del análisis del contexto interno se deben tener en cuenta para facilitar la descripción de aquellos hechos generadores de riesgos que se constituyen finalmente en las causas y subcausas del riesgo.

Podemos ver la relación entre la clasificación de los riesgos descritos en el punto 3.6 y los factores de riesgos que se identificarán durante el ejercicio de análisis del contexto externo e interno en la siguiente ilustración:

4.3.6. Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder 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:

- **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.

Ilustración 4. Estructura descripción del riesgo de gestión y seguridad de la información

Para los riesgos de corrupción se propone se tendrá en cuenta la siguiente estructura:

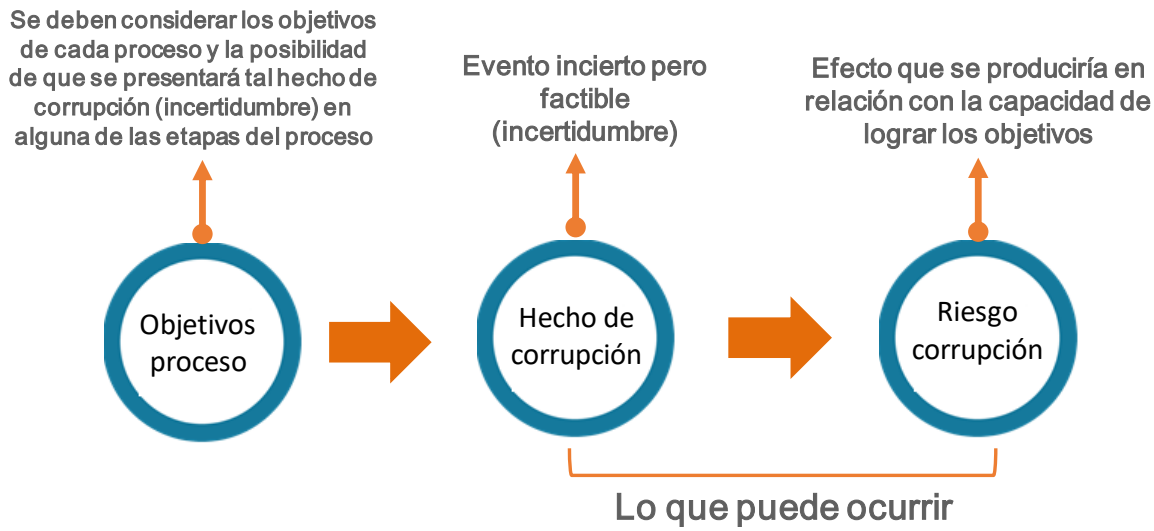


Ilustración 5. Estructura propuesta riesgos de corrupción

PROCESO	HECHO GENERADOR	RIESGO
Realizar un estudio documental y jurídico de las solicitudes de modificación y elaborar la respectiva minuta.	Aceptar modificaciones al contrato que reduzcan las obligaciones o especificaciones, con el interés de favorecer un interés particular.	Posibilidad de afectación económica generando un impacto fiscal para la entidad.

Premisas para una adecuada redacción del riesgo

No describir como riesgos omisiones ni desviaciones del control.

Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos

Ejemplo: inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control.

Ejemplo: retrasos en la prestación del servicio por no contar con digiturno para la atención.

No existen riesgos transversales, lo que pueden existir son causas transversales.

Ejemplo: pérdida de expedientes.

Identificación del riesgo								
Referencia	Impacto ¿Qué?	Causa Inmediata ¿Cómo?	Causa Raíz ¿Por qué?	Descripción del Riesgo	Tipología del riesgo	Clasificación del Riesgo	Activo de Información	Frecuencia con la cual se realiza la actividad
1	Económico y reputacional	Por multa o sanción del ente regulador e investigaciones disciplinarias	presentación extemporanea de informes de Ley como producto de la inoportunidad de la información requerida a las diferentes áreas de la entidad	Posibilidad de afectación económica y reputacional por Por multa o sanción del ente regulador e investigaciones disciplinarias	Gestión	Ejecución y Administración de Procesos	n/a	40

Tabla 3. Instrumento matriz de riesgos de gestión y seguridad de la información sección identificación del riesgo SIG-M06A

Identificación del riesgo			
Referencia	Hecho de corrupción (Causas)	Descripción del Riesgo	Frecuencia
1	En desarrollo del ejercicio auditor a cargo del proceso de evaluación y control se omite, la realización de actuaciones y se ajustan o alteran	Posibilidad de Pérdida de confianza de la comunidad por investigaciones administrativas y disciplinarias debido al incumplimiento del código ético del auditor y estatuto de auditoria interna.	El evento puede ocurrir en algún momento. Al menos una vez en los últimos 5 años

Tabla 4. Instrumento matriz de riesgos de corrupción sección identificación del riesgo SIG-M06B

4.4. PASO 3. VALORACIÓN DE LOS RIESGOS

Se tendrá en cuenta el siguiente esquema:

Análisis de riesgo: busca establecer la probabilidad de ocurrencia de los riesgos y sus consecuencias o impacto. El análisis del riesgo dependerá de la información obtenida en la identificación de riesgos, la disponibilidad de datos históricos y aportes de los servidores públicos de la entidad.

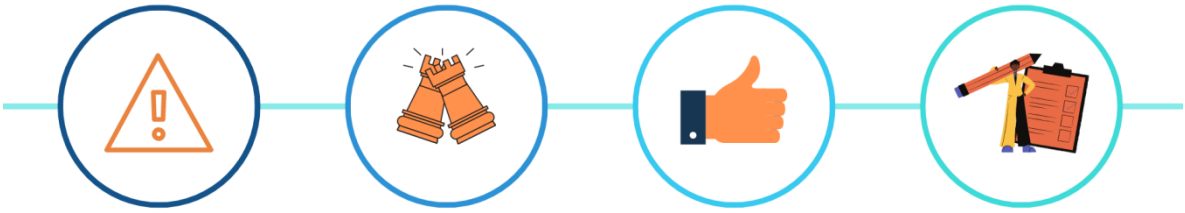
Evaluación del Riesgo Inherente: Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo ante de los controles aplicados; de esta forma es posible distinguir entre los riesgos que son tolerables, moderados e importantes y fijar las prioridades de las acciones requeridas para su tratamiento.

Tratamiento del riesgo: El procedimiento de tratamiento del riesgo involucra la selección de una o más opciones para transformar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

El tratamiento del riesgo implica un proceso cíclico de:

- Valoración del tratamiento del riesgo
- Decisión sobre si los niveles de riesgo residual son tolerables
- Si no son tolerables; generación de un nuevo tratamiento para el riesgo
- Valoración de la eficacia de dicho control.

DEFINICIONES A TENER EN CUENTA:



RIESGO INHERENTE	CONTROLES	RIESGO RESIDUAL	TRATAMIENTO
Riesgo propio de la actividad desarrollada	Controles existentes desarrollados para mitigar el riesgo.	Producto de la valoración de la eficiencia de los controles existentes	Acciones adicionales a implementar una vez se evalúa la efectividad de los controles.

4.4.1. ANÁLISIS DEL RIESGO

Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias e impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE) dentro de una escala de severidad. La primera se entiende como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, teniendo en cuenta el número de veces que se realiza la actividad. Por Impacto se entiende las consecuencias que puede ocasionar a la entidad la materialización del riesgo y se logra a través de la combinación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo.

Ilustración 6. Evaluación de los riesgos

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

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubica dos en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Probabilidad Riesgos de Gestión y Seguridad de la información

	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%

Tabla 5. Criterios de probabilidad Riesgos de Gestión y Seguridad de la información

Probabilidad Riesgos de corrupción

	Descriptor	Frecuencia de la Actividad	Probabilidad
Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.	20%
Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años.	40%
Posible	El evento podrá ocurrir en algún momento.	Al menos una vez en los últimos 2 años.	60%
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año.	80%
Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.	100%

Tabla 6. Criterios de Probabilidad Riesgos de corrupción

A modo de ejemplo, a continuación se observa ejemplo de la frecuencia de actividades comunes desarrolladas en las diferentes entidades del sector público:

Ilustración 7. Frecuencia actividades comunes gestión pública

4.4.1.2. Determinar el impacto

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

Para la definición de los impactos relacionados con afectación económica se contemplará todo lo referente a:

- Afectaciones a la ejecución presupuestal.
- Pagos por sanciones económicas.
- Indemnizaciones a terceros.
- Sanciones por incumplimientos de tipo legal.

Para la definición de los impactos relacionados con Afectación reputacional se tendrá en cuenta los criterios:

Afectación de la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles se debe tomar el nivel más alto.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis. En la tabla siguiente tabla se establecen los criterios para definir el nivel de impacto:

Impacto Riesgos de Gestión y seguridad de la información

	Económica	Reputacional	Nivel de severidad
CATASTRÓFICO	Impacto que afecte la ejecución presupuestal mayor a 500 SMLMV: • Pérdida de recursos por la no captación de recursos en los servicios de trámites mayor a 500 SMLMV. • Pago de indemnizaciones y/o acciones legales que afecten el presupuesto de la entidad mayor a 500 SMLMV. • Pago sanciones económicas por incumplimiento fiscal y normativo mayor a 500 SMLMV.	Imagen institucional afectada a nivel nacional, con efecto publicitario sostenido a nivel país. • Interrupción en los servicios de la entidad por más de 5 días. • Intervención por parte de los entes de control u otro ente regulador. • Pérdida de información crítica para la entidad. • Incumplimiento en las metas y objetivos institucionales afectando el presupuesto de la entidad. • Pérdida grave de la disponibilidad, integridad o confidencialidad de la información.	100%

MAYOR	Impacto que afecte la ejecución presupuestal entre 100 y 500 SMLMV: • Pérdida de recursos por la no captación de recursos en los servicios de trámites entre 100 y 500 SMLMV. • Pago de indemnizaciones y/o acciones legales que afecten el presupuesto de la entidad entre 100 y 500 SMLMV. • Pago sanciones económicas por incumplimiento fiscal y normativo entre 100 y 500 SMLMV.	Imagen institucional afectada con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal: • Interrupción en los servicios de la entidad por más de 2 días. • Sanción por parte de los entes de control u otro ente regulador. • Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento de las metas departamentales. • Imagen institucional afectada en el orden nacional o regional por hechos o actos de corrupción comprobados. • Pérdida grave de la disponibilidad, integridad o confidencialidad de la información.	80%
MODERADO	Impacto que afecte la ejecución presupuestal entre 50 y 100 SMLMV: • Pérdida de recursos por la no captación de recursos en los servicios de trámites entre 50 y 100 SMLMV. • Pago de indemnizaciones y/o acciones legales que afecten el presupuesto de la entidad entre 50 y 100 SMLMV. • Pago sanciones económicas por incumplimiento fiscal y normativo entre 50 y 100 SMLMV.	Imagen institucional afectada con algunos usuarios de relevancia frente al logro de los objetivos: • Interrupción en los servicios de la entidad por de 1 día • Reclamaciones o quejas de usuarios por la no prestación oportuna del servicio y denuncias ante entes de control. • Inoportunidad en la información que pueda generar retrasos en la prestación de los servicios y trámites institucionales • Reprocesos de actividades generando ineficiencia en la prestación de los servicios a los ciudadanos. • Investigaciones penales, fiscales	60%

		y disciplinarias • Pérdida moderada de la disponibilidad, integridad o confidencialidad de la información.	
MENOR	Impacto que afecte la ejecución presupuestal entre 10 y 50 SMLMV. • Pérdida de recursos por la no captación de recursos en los servicios de trámites entre 10 y 50 SMLMV. • Pago de indemnizaciones y/o acciones legales que afecten el presupuesto de la entidad entre 10 y 50 SMLMV. • Pago sanciones económicas por incumplimiento fiscal y normativo entre 10 y 50 SMLMV.	Imagen institucional afectada internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. • Interrupción en los servicios de la entidad por algunas horas • Reclamaciones o quejas de usuarios que generan investigaciones administrativas y disciplinarias. • Pérdida leve de la disponibilidad, integridad o confidencialidad de la información.	40%
LEVE	• Impacto que afecte la ejecución presupuestal menor a 10 SMLMV. • Pérdida de recursos por la no captación de recursos en los servicios de trámites menor a 10 SMLMV. • Pago de indemnizaciones y/o acciones legales que afecten el presupuesto de la entidad menor a 10 SMLMV. • Pago sanciones económicas por incumplimiento fiscal y normativo menor a 10 SMLMV.	Imagen institucional afectada en algún área de la organización. • No hay sanciones económicas o administrativas • No hay interrupción en la prestación de servicios de trámite en la entidad. • Sin afectación de la disponibilidad, integridad o confidencialidad de la información.	20%

Tabla 7. Tabla criterios de impacto de riesgos de gestión y seguridad de la información

Impacto Riesgos de Corrupción

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la Entidad. Para facilitar la asignación del puntaje se diligenciará el siguiente formato:

¿Si el riesgo se materializa podría?	**SI**	**NO**
¿Afectar al grupo de funcionarios del proceso?		
¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
¿Afectar el cumplimiento de misión de la entidad?		
¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
¿Generar pérdida de confianza de la entidad, afectando su reputación?		
¿Generar pérdida de recursos económicos?		
¿Afectar la generación de los productos o la prestación de servicios?		
¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
¿Generar pérdida de información de la entidad?		
¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
¿Dar lugar a procesos sancionatorios?		
¿Dar lugar a procesos disciplinarios?		
¿Dar lugar a procesos fiscales?		
¿Dar lugar a procesos penales?		
¿Generar pérdida de credibilidad del sector?		
¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
¿Afectar la imagen regional?		
¿Afectar la imagen nacional?		
¿Generar daño ambiental?		
Total respuestas afirmativas		

De acuerdo al número de respuestas respondidas afirmativas se escogerá el nivel de impacto del riesgo de corrupción:

Medición de Impacto del Riesgo de Corrupción			
Descriptor	Descripción	Nivel	Respuestas afirmativas
Moderado	Afectación parcial al proceso y a la dependencia. Genera medianas consecuencias para la entidad.	60%	1 – 5

Mayor	Impacto negativo para la Entidad. Genera altas consecuencias para la entidad.	80%	6 – 11
Catastrófico	Consecuencias desastrosas sobre la entidad. Genera consecuencias desastrosas para la entidad.	100%	12 - 19

Tabla 8. Tabla criterios de impacto riesgos de corrupción

IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

La probabilidad e impacto inherente deben llenarse en las siguientes columnas del instrumento matriz de riesgos:

	Análisis del riesgo inherente					
Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente
2400	Alta	80%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo

Ilustración 8. Instrumento matriz de riesgos de gestión y seguridad de la información sección análisis del Riesgo inherente SIG-M06A

Análisis del riesgo inherente					
Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente
Posible	60%	Entre 12 y 19 criterios para calificar el impacto son afirmativos. Genera un impacto catastrófico	Catastrófico	100%	Extremo

Ilustración 9. Instrumento matriz de riesgos de corrupción sección análisis del Riesgo inherente formato SIG-M06A

4.4.2. EVALUACIÓN DEL RIESGO

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

4.4.2.1. ***Análisis preliminar (riesgo inherente):*** se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

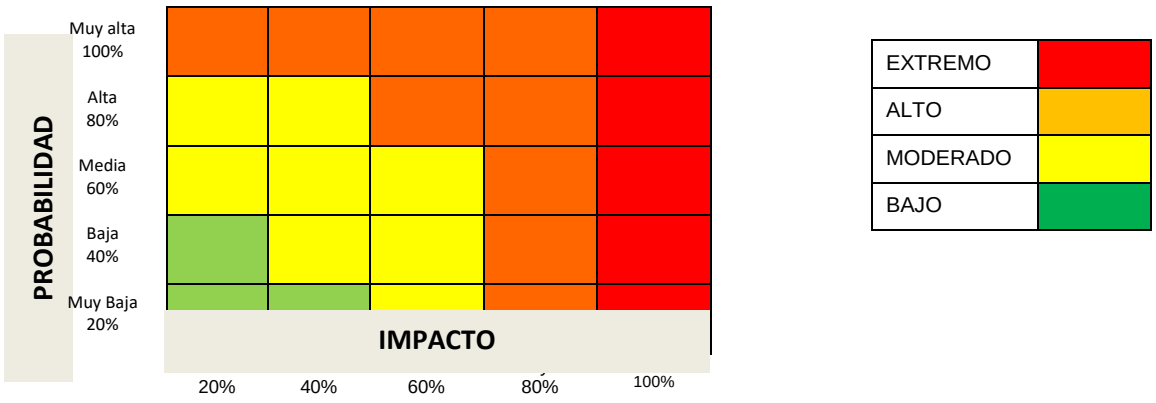
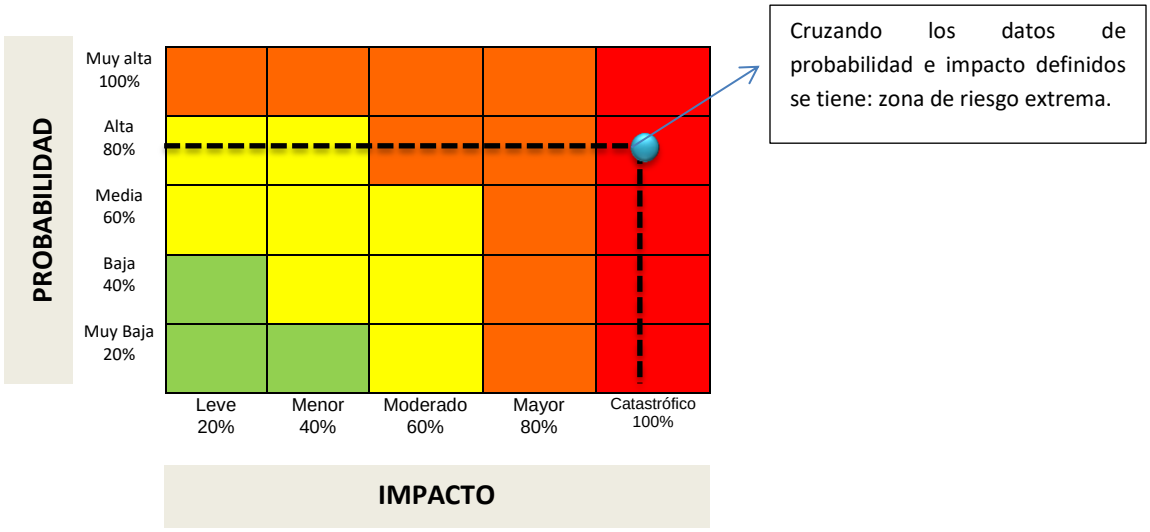


Ilustración 10. Figura 14 Matriz de calor (niveles de severidad del riesgo)

Ejemplo (continuación): Siguiendo con el ejemplo del proceso de reeducación al ciudadano en la matriz de riesgos de gestión.

Proceso:	Reeducación al conductor
Objetivo:	Actualizar la formación de los conductores en el conocimiento de normas y comportamientos al momento de conducir un vehículo.
Alcance:	Inicia con la identificación de los requisitos que debe contener la capacitación continua con la liquidación de cursos, capacitar, evaluar cursos y termina con la evaluación de capacitaciones
Riesgo	Posibilidad de afectación económica y reputacional por pérdida de confianza por parte de la ciudadanía al igual de posibles investigaciones por entes de control debido a fallas en el cargue de la información en el software contravencional y de trámites relacionada con los comparendos electrónicos y de otros organismos de tránsito que afectan la liquidación de los cursos de reeducación al conductor
	Probabilidad inherente 80% Impacto inherente: 100%



4.4.2.2. ***Valoración de controles:*** en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

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

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

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

El profesional de Contratación

Verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación,

A través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Ilustración 11. Estructura propuesta aplicación control

4.4.2.2.2. *Tipología de controles y los procesos:* a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, a continuación se consideran 3 fases globales del ciclo de un proceso así:

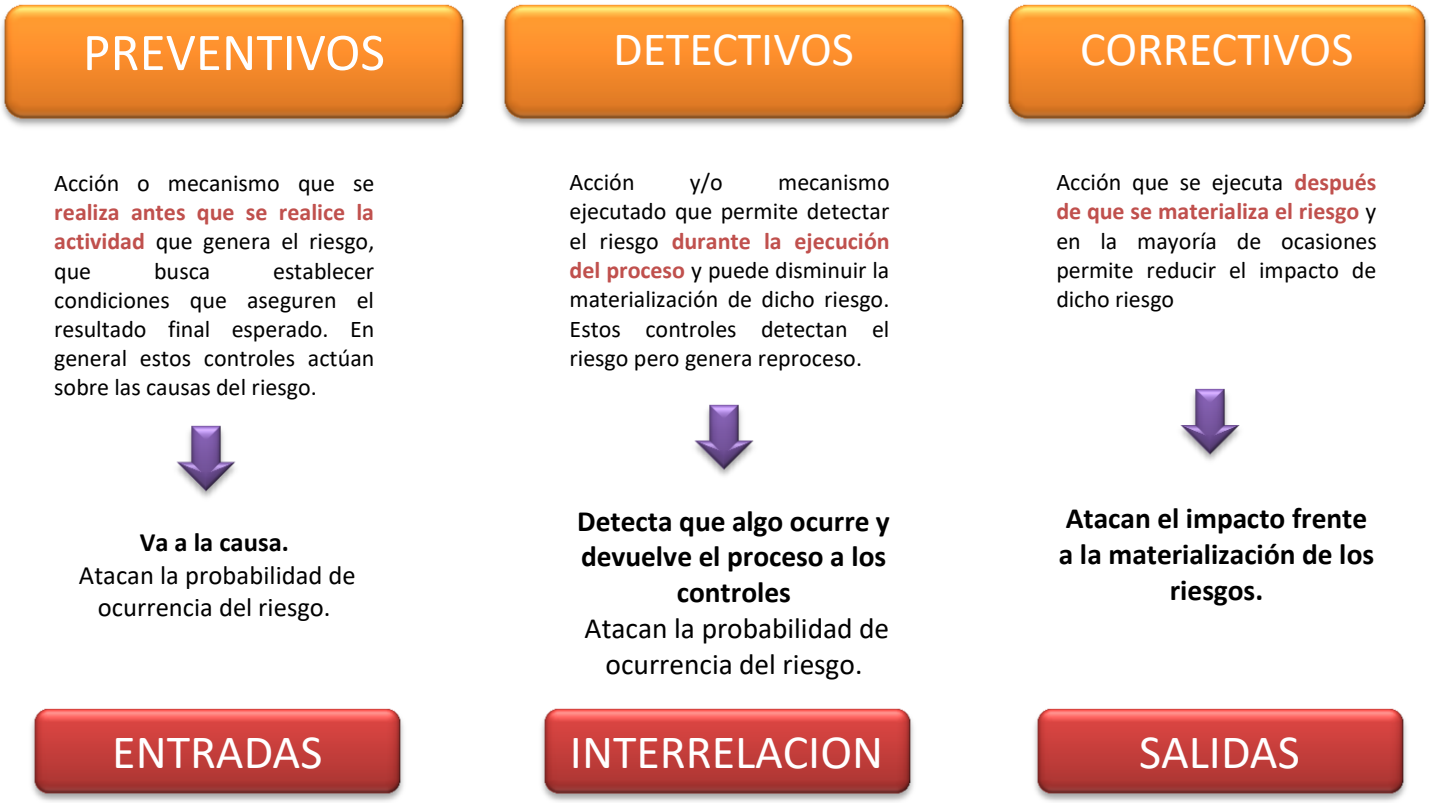


Ilustración 12. Ciclo del proceso y tipologia de controles

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

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

4.4.2.2.3. Análisis y evaluación de los controles

Valoración controles en los riesgos de gestión y seguridad de la información. A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 9 se puede observar la descripción y peso asociados a cada uno así:

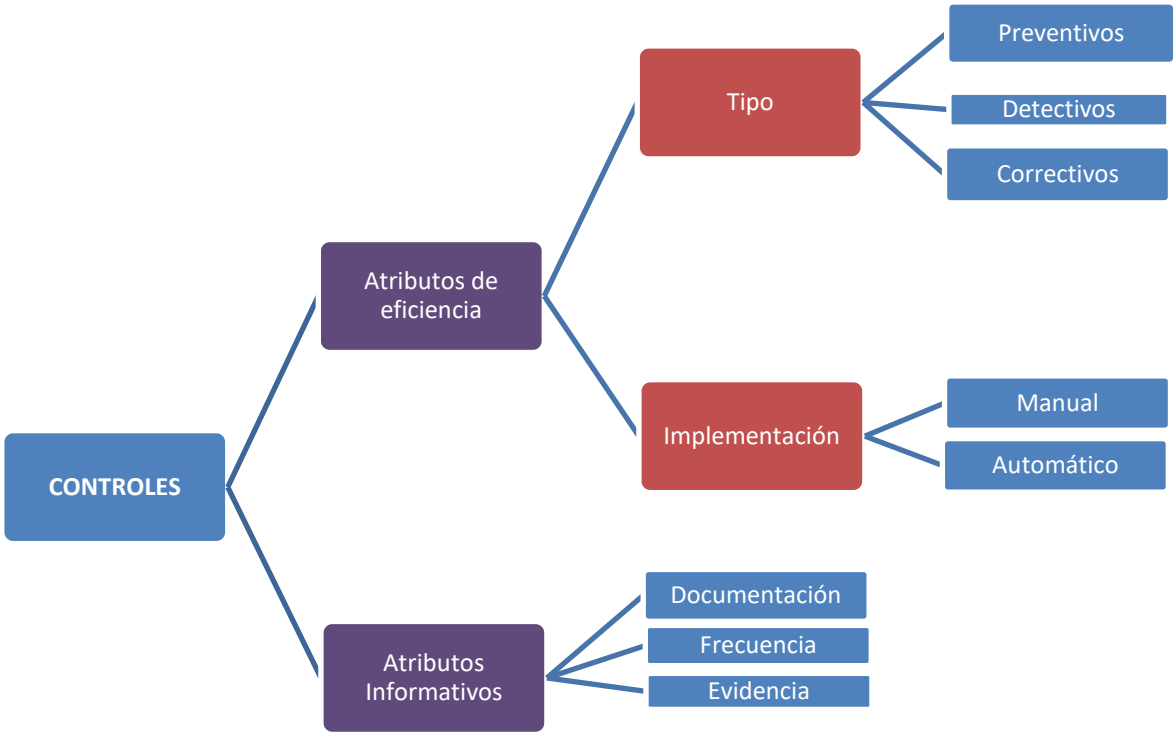


Ilustración 13. Definición controles riesgos de gestión y seguridad de la información

CARACTERÍSTICAS DE EFICIENCIA			PESO
TIPO	PREVENTIVO	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
	DETECTIVO	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
	CORRECTIVO	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo e	10%

		n su implementación.	
IMPLEMENTACIÓN	AUTOMÁTICO	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
	MANUAL	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
CARACTERÍSTICAS DE FORMALIZACIÓN			
DOCUMENTACIÓN	DOCUMENTADO	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	NO TIENEN PESO SOLO PERMITEN DARLE FORMALIDAD AL CONTROL CON EL FIN DE CONOCER EL ENTORNO DE CONTROL
	SIN DOCUMENTAR	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso .	
FRECUENCIA	CONTINUA	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	
	ALEATORIA	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	
EVIDENCIA	CON REGISTRO	El control deja un registro permite evidencia la ejecución del control.	
	SIN REGISTRO	El control no deja registro de la ejecución del control.	
	CARACTERÍSTICAS DE EFICACIA		

	DESEMPEÑO DEL CONTROL # eventos / frecuencia del riesgo (# veces que se hace la actividad)

Tabla 9. Atributos de para el diseño del control riesgos de gestión y seguridad de la información

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

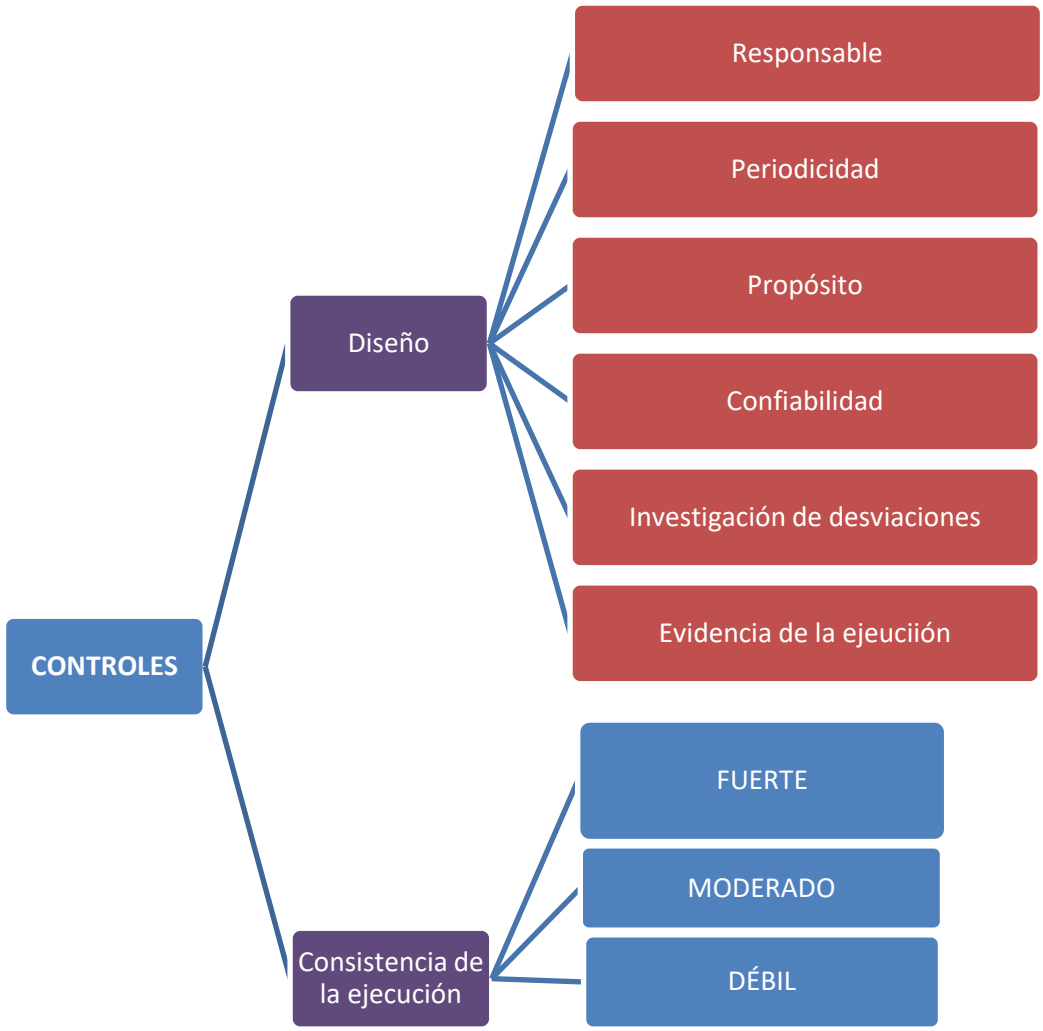


Ilustración 14. Definición controles riesgos de corrupción

El análisis y evaluación del diseño del control se realiza de acuerdo con las seis (6) variables establecidas y el peso o participación de cada variable en el diseño del control para la mitigación del riesgo:

Criterio de evaluación	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	PESO E N LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No asignado	0
1.2 Segregación y autoridad del responsable	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		No adecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	15
		No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	15
		Incompleta / no existe	0

Tabla 10. Variables y su ponderación en el diseño del control riesgos de corrupción

Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EVALUACIÓN DEL DISEÑO
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla 11. Criterios calificación diseño del control de riesgos de corrupción

Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute.

Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna o control interno.

RANGO DE CALIFICACIÓN DEL DISEÑO	RESULTADO – PESO EN LA EJECUCIÓN DEL DISEÑO
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla 12. . Criterios calificación ejecución del control de riesgos de corrupción

4.4.2.2.4. Análisis y evaluación de los controles para la mitigación de los riesgos:

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

En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

PESO EN EL DISEÑO DE CADA CONTROL	PESO EN LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL: 0	DEBEN ESTABLECERSE ACCIONES PARA FORTALECER EL CONTROL SI/NO
Fuerte Calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
Moderado Calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
Débil Calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Tabla 13. Solidez individual controles riesgos de corrupción

[La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.]

4.4.2.2.5. Solidez del conjunto de controles:

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

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Tabla 14. Solidez del conjunto de controles riesgos de corrupción

4.4.2.3. Disminución de probabilidad e impacto.

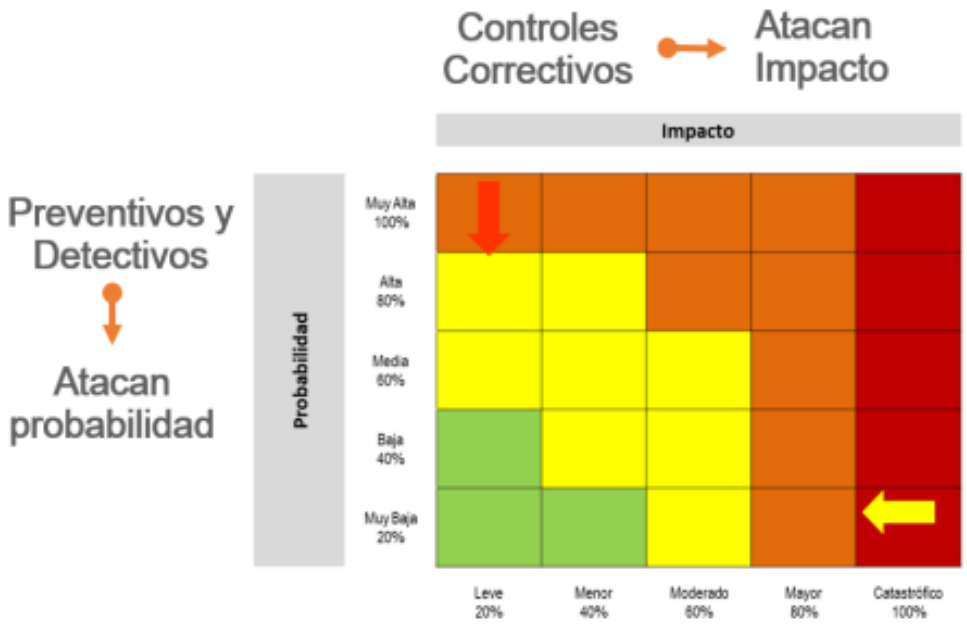


Ilustración 15. Movimiento en la matriz de calor

4.4.2.3.1. Disminución probabilidad e impacto Riesgos de gestión y seguridad de la información:

Ejemplo (continuación):

Proceso:	Reeducación al conductor
Objetivo:	Actualizar la formación de los conductores en el conocimiento de normas y comportamientos al momento de conducir un vehículo.
Alcance:	Inicia con la identificación de los requisitos que debe contener la capacitación continua con la liquidación de cursos, capacitar, evaluar cursos y termina con la evaluación de capacitaciones
Riesgo	Posibilidad de afectación económica y reputacional por pérdida de confianza por parte de la ciudadanía al igual de posibles investigaciones por entes de control debido a fallas en el cargue de la información en el software contravencional y de trámites relacionada con los comparendos electrónicos y de otros organismos de tránsito que afectan la liquidación de los cursos de reeducación al conductor
	Probabilidad inherente 80% Impacto inherente: 100%

Valoración controles del riesgo:

CARACTERÍSTICAS DE EFICIENCIA		PESO	C1	C2
TIPO	PREVENTIVO	25%	X	
	DETECTIVO	15%		
	CORRECTIVO	10%		X
IMPLEMENTACIÓN	AUTOMÁTICO	25%	X	X
	MANUAL	15%		

CARACTERÍSTICAS DE FORMALIZACIÓN				
DOCUMENTACIÓN	DOCUMENTADO	0%	X	X
	SIN DOCUMENTAR	0%		
FRECUENCIA	CONTINUA	0%	X	X
	ALEATORIA	0%		
EVIDENCIA	CON REGISTRO	0%	X	X
	SIN REGISTRO	0%		
TOTAL			50%	35%

Tabla 15. Aplicación tabla atributos a ejemplo propuesto

Aplicándolo en el instrumento podremos diligenciarlo en las siguientes columnas:

Evaluación del riesgo - Valoración de los controles								
No. Control	Descripción del Control	Afectación	Atributos					
			Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia
1	El proveedor del software contravencional revisa la	Probabilidad	Preventivo	Automático	**50%**	Documentado	Contínua	Con registro
2	El proveedor del software contravencional regenera la información	Impacto	Correctivo	Automático	**35%**	Documentado	Contínua	Con registro

Ilustración 16. Instrumento matriz de riesgos de gestión y seguridad de la información sección evaluación del riesgo - valoración de los controles SIG-M06A

A continuación se presenta la sección anterior aplicada en los riesgos de corrupción

Valoración del diseño																		Valoración de la ejecución del control	SOLIDEZ INDIVIDUAL DEL CONTROL		CANTIDAD DE CONTROLES AL RIESGO	SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	
No.Control	Descripción del Control	RESPONSABLE ¿Existe un responsable asignado a la ejecución del control?		RESPONSABLE ¿El responsable tiene la autoridad y adecuada separación de funciones		PERIODICIDAD ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación		PROPOSITO ¿Las actividades que se desarrollan en el control realmente buscan por sí		COMO SE REALIZA ¿La fuente de información que se utiliza en el desarrollo del control es		QUE PASA CON LAS OBSERVACIONES O DESVIACIONES		EVIDENCIA ¿Se deja evidencia o rastro de la ejecución del control que permita a		Resultado de evaluación del diseño del control	Rango de calificación del diseño del control	*Fuerte: El control se ejecuta de manera consistente por parte del responsable. Moderado: El control se ejecuta algunas veces por parte del responsable. Débil: El control no se ejecuta por parte del responsable.	SOLIDEZ	PESO		PESO	SOLIDEZ
		Asignado / NO asignado	Peso en la evaluación	Adecuado / Inadecuado	Peso en la evaluación	Oportuna / Inoportuna	Peso en la evaluación	Prevenir / Detectar / No es control	Peso en la evaluación	Confiable / No confiable	Peso en la evaluación	Se investigan oportunamente / No se investigan	Peso en la evaluación	Completa / Incompleta / No existe	Peso en la evaluación								
1	el conductor verifica que la persona	Asignado	15	Adecuado	15	Oportuna	15	Prevenir	15	Confiable	15	Se investigan oportunamente	15	Completa	10	**100**	**Fuerte**	**Fuerte**	Fuerte	100	1	100	Fuerte
2			FALSO		FALSO		FALSO		FALSO		FALSO		FALSO		FALSO	**0**	**Débil**		Débil	0			
3			FALSO		FALSO		FALSO		FALSO		FALSO		FALSO		FALSO	**0**	**Débil**		Débil	0			
4			FALSO		FALSO		FALSO		FALSO		FALSO		FALSO		FALSO	**0**	**Débil**		Débil	0			
5			FALSO		FALSO		FALSO		FALSO		FALSO		FALSO		FALSO	**0**	**Débil**		Débil	0			

Ilustración 17. Instrumento matriz de riesgos de corrupción sección evaluación del riesgo - valoración de los controles SIG-M06B

La mayoría de los controles que se diseñan son para disminuir la probabilidad de que ocurra una causa o evento que pueda llevar a la materialización del riesgo y muy pocos son dirigidos al impacto:

EJEMPLO:

Para poder asignar un contrato se debe verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.

Para mitigar el impacto económico, en caso de que el contratista incumpla, se deben verificar las pólizas de seguros solicitadas al contratista seleccionado.

4.4.2.3.2. Disminución probabilidad e impacto Riesgos de corrupción

Generalmente se encuentran más controles que disminuyen directamente la probabilidad que el impacto.

Si no existieran controles para disminuir la probabilidad del riesgo, el impacto de un riesgo por el número de eventos que se llegarían a materializar sería mayor, en nuestro ejemplo, si no existiera el control "verificar que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación para poder asignar un contrato", el número de contratos que se incumplirían sería mayor, por tal razón, y para efectos de la elaboración de la matriz al momento de evaluar si los controles ayudan a disminuir el impacto o la probabilidad, estos controles se calificarán teniendo en cuenta que de manera indirecta disminuyen también el impacto.

4.4.2.4. Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente.

4.4.2.4.1. Nivel de riesgo residual (gestión y seguridad de la información)

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Para mayor claridad, en la siguiente tabla se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

[SE TOMA EL VALOR DE PROBABILIDAD 1 PARA APLICARLO AL CONTROL 2.
DENTRO DE LA POLÍTICA DE ADMINISTRACIÓN INTEGRAL DE RIESGOS SE ESTABLECIÓ LA REGLA DE REDUCCIÓN DE MÁXIMO 50%, ESTO CON EL FIN DE EVITAR QUE UN SOLO CONTROL BAJE MUCHO EL RIESGO.]

Tabla 16. Aplicación de controles para establecer el riesgo residual riesgos se gestión y seguridad de la información

4.4.2.4.2. Nivel de riesgo residual (corrupción):

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

SOLIDEZ DEL CONJUNTO DE CONTROLES	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL: 0	DEBEN ESTABLECERSE ACCIONES PARA FORTALECER EL CONTROL SI/NO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD
FUERTE	directamente	directamente	2
FUERTE	directamente	Indirectamente	2
FUERTE	directamente	No disminuye	2
FUERTE	No disminuye	Directamente	0
MODERADO	directamente	Directamente	1
MODERADO	directamente	Indirectamente	1
MODERADO	directamente	No disminuye	1
MODERADO	No disminuye	Directamente	0

Tabla 17. Solidez conjunto de controles riesgos de corrupción

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

Resultados del mapa de riesgo residual. Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la valoración del riesgo residual (después de los controles).

Ejemplo (continuación):

Proceso:	Reeducación al conductor
Objetivo:	Actualizar la formación de los conductores en el conocimiento de normas y comportamientos al momento de conducir un vehículo.
Alcance:	Inicia con la identificación de los requisitos que debe contener la capacitación continua con la liquidación de cursos, capacitar, evaluar cursos y termina con la evaluación de capacitaciones
Riesgo	Posibilidad de afectación económica y reputacional por pérdida de confianza por parte de la ciudadanía al igual de posibles investigaciones por entes de control debido a fallas en el cargue de la información en el software contravencional y de trámites relacionada con los comparendos electrónicos y de otros organismos de tránsito que afectan la liquidación de los cursos de reeducación al conductor
Evaluación inicial	Probabilidad inherente 80% Impacto inherente: 100%

Nueva evaluación:

Evaluación del riesgo - Nivel del riesgo residual								
Probabilidad Residual	Probabilidad Residual	%	Impacto Residual	%	Probabilidad Residual Final	Impacto Residual Final	Zona de Riesgo Final	Tratamiento
40,0%	Baja	40%	Catastrófico	100%	40,0%	65,0%	Alto	Reducir (Mitigar)
40,0%	Baja	40%	Mayor	65,0%				

Ilustración 18. Instrumento matriz de riesgos gestión y seguridad de la información sección evaluación del riesgos - Nivel del riesgo residual ejemplo aplicado SIG-M06A

CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	Ajuste en mapa de calor	% Probabilidad residual	PROBABILIDAD RESIDUAL	CONTROLES AYUDAN A DISMINUIR EL IMPACTO	Ajuste en mapa de calor	% impacto residual	IMPACTO RESIDUAL	RIESGO RESIDUAL
Directamente	40%	20%	Rara Vez	Indirectamente	20%	80%	Mayor	Alto

Ilustración 19. Instrumento matriz de riesgos de sección evaluación del riesgos - Nivel del riesgo residual riesgos de corrupción sección evaluación del riesgo – Nivel del riesgo residual SIG-M06B

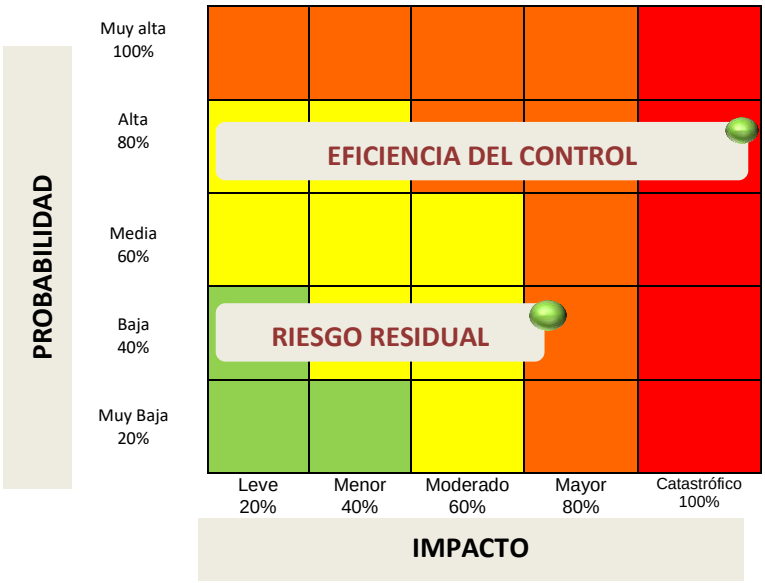


Ilustración 20. Movimiento en la matriz de calor con el ejemplo propuesto

4.3. ESTRATEGIAS PARA COMBATIR EL RIESGO

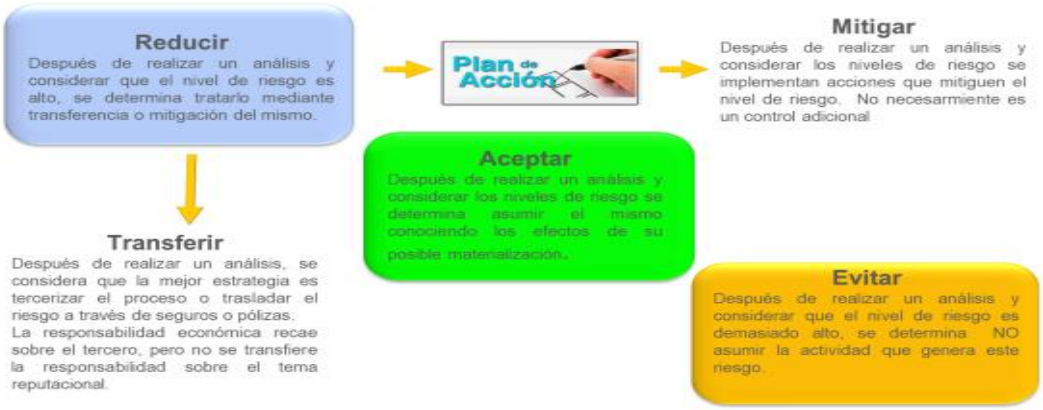
Es la decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

¿Qué es tratamiento del riesgo?

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías



Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

NOTA:

El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio y se consideraría un control correctivo.

Plan de Acción						Indicador clave de riesgo Nombre/Métrica	Desempeño del control= # eventos /frecuencia del riesgo
Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado		
Revisar la parametrizaci	Proveedor Software	1/06/2021	Mensual	Se están desarrollan	En curso	Cantidad de cursos liquidados sin los lineamientos de tránsito establecido	Según el seguimiento

Ilustración 21. Instrumento matriz de riesgos de sección plan de acción o tratamiento, continuación ejemplo aplicado

4.4. GESTIÓN DE EVENTOS

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad.

Se debe contar con una base histórica de eventos que permita:

- Revisar si el riesgo fue identificado y qué sucedió con los controles.
- En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.
- Algunas fuentes para establecer una base histórica de eventos pueden ser: Mesa de ayuda, Las PQRD (peticiones, quejas, reclamos, denuncias), Oficina jurídica, Líneas internas de denuncia.

Para identificar los eventos se debe implementar el siguiente indicador:

EFICACIA DEL CONTROL: Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad).

El seguimiento a la eficiencia del control se realizará durante las secciones de monitoreo y seguimiento desarrollados por las oficinas asesoras de planeación y control interno. Así como también por los líderes de los procesos en el seguimiento de sus controles y acciones proyectadas.

4.5. INDICADORES CLAVES DE RIESGO

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento.

De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

El comportamiento de los mismos puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la siguiente tabla se muestran algunos nos ejemplos de estos indicadores.

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

Plan de Acción						Indicador clave de riesgo Nombre/Métrica	Desempeño del control= # eventos /frecuencia del riesgo
Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado		
Revisar la parametrizaci	Proveedor Software	1/06/2021	Mensual	Se están desarrollan	En curso	Cantidad de cursos liquidados sin los lineamientos de tránsito establecido	Según el seguimiento

Ilustración 22. Continuación ejemplo aplicado sección indicadores clave de riesgo