LOTERÍA DE MEDELLÍN

MANUAL DE RIESGOS

FECHA DE APROBACION: _____

LA REPRODUCCIÓN PARCIAL O TOTAL DE ESTE MANUALSOLO PUEDE HACERSE CON AUTORIZACIÓN DEL COMITÉ DE GESTIÓN Y DESEMPEÑO DE LA LOTERÍA DE MEDELLÍN.

CONTENIDO

	Pág.
PRESENTACIÓN	2
CONCEPTOS BÁSICOS RELACIONADOS CON LA GESTIÓN DEL RIESGO	7
MARCO DE REFERENCIA CON EL MIPG	12
Beneficios	14
COMPROMISO DE LA DIRECCIÓN	16
CONOCIMIENTO Y ANÁLISIS DE LA ENTIDAD	18
CONTEXTO ESTRATÉGICO	20
LINEAMIENTOS RIESGOS DE GESTIÓN	23
Metodología	23
Pasos para la Administración del Riesgos	23
PASO 1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	25
Objetivo	26
Alcance	26
Nivel de aceptación al riesgo	26
a) Capacidad del riesgo	27
b) Tolerancia del riesgo	27
c) Apetito del riesgo	27
Niveles para calificar el impacto	29
Niveles para calificar la probabilidad	30
Tratamiento del riesgo	30
Monitoreo	31
PASO 2. IDENTIFICACIÓN DEL RIESGO	32
Análisis de los Objetivos estratégicos y de los procesos	32
Identificación de los puntos de riesgo	34
Identificación de áreas de impacto	35
Identificación de áreas de factores de riesgo	36
Descripción del riesgo	37
Premisas para una adecuada redacción del riesgo	38

Clasificación del riesgo	38
Matriz de calor	39
PASO 3: VALORACIÓN DEL RIESGO	41
Análisis de riesgos	42
Determinar la probabilidad	42
Determinar el impacto	43
Evaluación de riesgos	44
Valoración de controles	44
Estructura para la descripción del control	44
Tipología de controles	45
Análisis y evaluación de los controles – Atributos	46
Efectividad del Control	49
Riesgo residual	50
Formato mapa de riesgos:	51
a) identificación del riesgo	51
b) Valoración del riesgo	51
c) Planes de acción	52
Estrategias para combatir el riesgo	52
Herramientas para la gestión del riesgo	53
Monitoreo y revisión	54
Responsabilidades	55
LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN	59
Definición de riesgo de corrupción	59
Generalidades acerca de los riesgos de corrupción	60
Valoración de riesgos	62
a) Análisis de la probabilidad	62
b) Análisis del impacto	62
c) Análisis del impacto en riesgos de corrupción	63
Valoración de los controles – diseño de controles	64

Tratamiento del riesgo	65
Monitoreo de riesgos de corrupción	66
Reporte de la gestión del riesgo de corrupción	66
Seguimiento de riesgos de corrupción	67
Acciones a seguir en caso de materialización de riesgos de corrupción	67
LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	68
Identificación de los activos de seguridad de la información	69
Pasos para la identificación de activos	70
Identificación del riesgo	71
Valoración del riesgo	71
Controles asociados a la seguridad de la información	72

PRESENTACIÓN

En cumplimiento a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, versión 5 definido por el Departamento Administrativo de la Función Pública, donde recomienda la metodología para la Administración del Riesgo y en concordancia con lo establecido en la Ley 1474 de 2011 y en el Decreto 2641 de 2012 como estrategia de lucha contra la corrupción y atención al ciudadano y enmarcado en los lineamientos del Modelo Estándar de Control Interno MECI 1000, emanado por el Departamento Administrativo de la Función Pública, La Junta Directiva de la Lotería de Medellín, aprueba el Manual de Riesgos con el fin de identificar y documentar el modelo metodológico del riesgo que se basa en un conjunto de actitudes compartidas, valores y prácticas que caracterizan cómo la entidad enfrenta el riesgo en el "día a día", como un valor en sí mismo, sin que sea necesario que emerja de una norma.

Esta propuesta metodológica se constituye en un soporte para el fortalecimiento de la política de la Administración del Riesgo y contribuye al fortalecimiento e interiorización de la cultura de Autocontrol y Autoevaluación. Es por esto que la política de la entidad se enmarca en la planeación, procesos y controles para garantizar el logro de los objetivos estratégicos institucionales.

Para la implementación de la gestión del riesgo, es necesario que la entidad haga un análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a las necesidades de cada organización, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a nuestros usuarios aspectos fundamentales frente a la generación de valor público, eje fundamental en el quehacer de la Lotería de Medellín.

De acuerdo con lo anterior y para iniciar la estructura metodológica, lo determina en tres pasos:

I. Política de administración del riesgo, se definen los lineamientos, teniendo en cuanta que se trata de un paso esencial en cabeza de la alta dirección de la Lotería de Medellín, en tanto se constituye en la base para la gestión del riesgo en todos los niveles de la Entidad.

II. Identificación del riesgo, se propone una estructura para la redacción adecuada del riesgo, lo que facilita el análisis de la causa y se proponen una serie de premisas básicas para evitar errores o generalizaciones del riesgo

que dificultan la aplicación de los pasos siguientes definidos en la metodología. En este mismo apartado se precisan los factores de riesgo y su relación con las tipologías de riesgo.

III. Valoración del riesgo, se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad.

En este sentido, este manual facilita la concreción de la administración del riesgo para que sea incorporada en la práctica gerencial de la Lotería de Medellín como una política de gestión y de control por parte de la alta dirección y cuente con la participación y respaldo de todos los funcionarios; tarea que se facilitará con la implementación de la metodología aquí presentada lo cual permite establecer mecanismos para la administrar los riesgos de Gestión, de Corrupción, de TICS y de SARLAFT, igualmente se realiza análisis de la contratación, del contexto interno y externo de la entidad, la planeación estratégica, los planes, programas y proyectos a los que constantemente están expuestos al quehacer diario de la Entidad y poder de esta manera fortalecer los Sistemas Integrados para lograr el más alto grado de eficacia y eficiencia institucional.

CONCEPTOS BÁSICOS RELACIONADOS CON LA GESTIÓN DEL RIESGO

Administración de riesgos: Una rama de administración que aborda las consecuencias del riesgo. Consta de dos etapas:

- El diagnóstico o valoración, mediante Identificación, análisis y determinación del Nivel y,
- El manejo o la administración propiamente dicha, en que se elabora, ejecuta y hace seguimiento al Plan de manejo que contiene las Técnicas de Administración del Riesgo propuestas por el grupo de trabajo, evaluadas y aceptadas por la alta dirección.

Administrador: Entidad encargada del recaudo, fiscalización, liquidación, cobro, sanción y todos los demás aspectos relacionados con el cumplimiento de las obligaciones derivadas de la operación de suerte y azar.

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

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

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

Análisis de riesgos: Determinar el Impacto y la Probabilidad del riesgo. Dependiendo de la información disponible pueden emplearse desde modelos de simulación, hasta técnicas colaborativas.

Apetito del 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 del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Apostador o jugador: Persona natural que arriesga cierta cantidad de dinero en un juego de suerte y azar, del que espera obtener un premio en dinero o en especie.

Apuestas en eventos hípicos: Modalidad de juego de suerte y azar, en el que se apuesta sobre los resultados de carreras de caballos efectuadas en hipódromos nacionales e internacionales. Las apuestas son de tipo paramutual lo que implica que se otorga como premio un porcentaje del monto de las apuestas, a los apostadores que acierten los resultados de las carreras.

Apuestas permanentes o chance: Es una modalidad de juego de suerte y azar en la cual el jugador, en formulario oficial, en forma manual o sistematizada, indica el valor de su apuesta y escoge un número de no más de cuatro (4) cifras, de manera que si su número coincide, según las reglas predeterminadas, con el resultado del premio mayor de la lotería o juego autorizado para el efecto, gana un premio en dinero, de acuerdo con un plan de premios predefinido y autorizado por el Gobierno Nacional mediante decreto reglamentario.

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

Canal de distribución: Medios físicos o electrónicos a través de los cuales el sujeto obligado interactúa con sus clientes, usuarios o proveedores, para el suministro de productos o servicios propios del desarrollo de su objeto social o actividad económica.

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.

Cliente externo: Proveedores, distribuidores, contratistas, outsourcing, contrapartes no vigiladas, etc.

Cliente Interno: Funcionarios de nómina, temporales y contratistas permanentes.

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.

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

Control: Medida que permite reducir o mitigar un riesgo, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.

Concesionario: Persona jurídica que celebra un contrato de concesión con las entidades contempladas en el artículo 22 de la Ley 643 de 2001, con el objeto de operar el juego de apuestas permanentes o chance.

Conflicto de Interés: Situación que se le presenta a una persona, en razón de su actividad, con distintas alternativas de conducta y con relación a intereses incompatibles, ninguna de las cuales puede recomendar en razón a sus obligaciones legales y contractuales.

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

CGDI: Comité de Gestión y Desempeño Institucional.
CICCI: Comité Institucional de Coordinación de Control Interno.
Control: Es toda acción que tiende a minimizar los riesgos, significa analizar el desempeño de las operaciones, evidenciando posibles desviaciones frente al resultado esperado para la adopción de medidas preventivas. Los controles proporcionan un modelo operacional de seguridad razonable en el logro de los objetivos.
Contingencia: posible evento futuro, condición o eventualidad.
Continuidad del negocio: capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
CNJSA: Consejo Nacional de Juegos de Suerte y Azar.
Crisis: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
Costo: Se entiende por costo las erogaciones, directas e indirectas en que incurre la entidad en la producción, prestación de un servicio o manejo de un riesgo.
Dependencia: Hace referencia a un área, dirección, subdirección, jefatura, unidad administrativa, entre otras, vigente en la organización o entidad.
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
Enfoque Basado en Riesgos: Es la aplicación de metodologías para la administración de sus riesgos en función del conocimiento que tengan sobre ellos, considerando entre otros, su sector y objeto social o actividad económica en el que desarrolla sus actividades o funciones; tamaño, estructura organizacional y funcional, relaciones contractuales o legales de cualquier índole o los mercados en que actúa, con el fin de aplicarle medidas proporcionales a la magnitud de estos y proveerle los recursos humanos, técnicos y tecnológicos ajustados.
Entidad de supervisión: Entidad del Estado encargada de ejercer la inspección, vigilancia o control sobre los sujetos obligados.
Entidad Concedente: Departamentos, Empresas Industriales y Comerciales del Estado, Sociedades de Capital Público Departamental, el Distrito Capital y Distritos Especiales, encargadas de conceder la operación de juegos de suerte y azar de índole territorial, a través de licitación pública, de acuerdo con la ley del régimen propio.
Evento de riesgo: Situación, incidente, suceso, acontecimiento o eventualidad, que puede ocurrir en un lugar o en la ejecución de cualquier actividad, durante un período de tiempo.
Factores de riesgo: Son las fuentes generadoras de riesgos, como las manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Identificación del Riesgo: Establecer la estructura del riesgo; fuentes o factores, internos o externos, generadores de riesgos; puede hacerse a cualquier nivel: total entidad, por áreas, por procesos, incluso, bajo el viejo paradigma, por funciones; desde el nivel estratégico hasta el más humilde operativo.
Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.
Indicador: es la valoración de una o más variables que informa sobre una situación y soporta la toma de decisiones, es un criterio de medición y de evaluación cuantitativa o cualitativa.
Integridad: Propiedad de exactitud y completitud.
Juegos de suerte y azar. Juegos en los cuales, según reglas predeterminadas por la ley y el reglamento, una persona que actúa en calidad de jugador realiza una apuesta o paga por el derecho a participar, a otra que actúa en calidad de operador, que le ofrece a cambio un premio, en dinero o en especie, el cual ganará si acierta, dados los resultados del juego, no siendo este previsible con certeza, por estar determinado por la suerte, el azar o la casualidad.
Juegos de suerte y azar territoriales: Tienen cobertura a nivel departamental, son explotados y administrados por los Departamentos y el Distrito Capital, operados por empresas industriales y comerciales o por terceros, son los siguientes: lotería tradicional o de billetes, apuestas permanentes o chance, apuestas en eventos hípicos, lotería instantánea, así como rifas y promocionales que operen en más de un municipio de un mismo departamento o en un municipio y el Distrito Capital.
Juegos de suerte y azar Nacionales: Tienen cobertura en todo el territorio colombiano, son administrados y autorizados por Coljuegos.
Lotería Tradicional: Es una modalidad de juego de suerte y azar realizada en forma periódica por un ente legal autorizado, el cual emite y pone en circulación billetes indivisos o fraccionados de precios fijos singularizados con una combinación numérica y de otros caracteres a la vista obligándose a otorgar un premio en dinero, fijado previamente en el correspondiente plan al tenedor del billete o fracción cuya combinación o aproximaciones preestablecidas coincidan en su orden con aquella obtenida al azar en sorteo público efectuado por la entidad gestora.
Mapas de riesgos: herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias.
MIPG: Modelo Integrado de Planeación y Gestión.
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.
Tratamientos: Parte del manejo de riesgos que contiene las acciones a ejecutar, con el fin de dar continuidad con la implementación los controles.
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.
Plan de manejo del Riesgo: Plan de acción propuesto por el grupo de trabajo, cuya evaluación de beneficio costo resulta positiva y es aprobado por la gerencia.
Plan de mejoramiento: Parte del plan de manejo que contiene las técnicas de la administración del riesgo orientadas a prevenir, evitar, reducir, dispersar, transferir o asumir riesgos.
Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, una medida que puede ser expresada como porcentaje o actividad o razón para estimar la posibilidad de que ocurra un incidente o evento, contando con registros, puede estimarse a partir de su frecuencia histórica mediante modelos estadísticos de mayor o menor complejidad
Responsables: Son las dependencias o áreas encargadas de adelantar las acciones propuestas.
Retroalimentación: Información sistemática sobre los resultados alcanzados en la ejecución de un plan, que sirven para actualizar y mejorar la planeación futura.
Riesgo: posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.
Riesgo absoluto: el máximo riesgo sin los efectos mitigantes de la administración del riesgo.
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).
Riesgo Operativo: la posibilidad de que un sujeto obligado incurra en pérdidas o eventual incumplimiento de sus obligaciones por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura, los sistemas internos o por la ocurrencia de acontecimientos externos.
Riesgo Reputacional: Es la posibilidad de pérdida en que incurre un sujeto obligado por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de su entidad u organización y sus prácticas de negocios y derive en dificultades en el logro o no consecución de sus objetivos misionales, funcionales u

organizacionales.
Riesgo residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riesgo Inherente: Nivel de riesgo propio de la actividad o proceso. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
Riesgo residual: es el riesgo que queda cuando las técnicas de la administración del riesgo han sido aplicadas.
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.
Rifas: Es una modalidad de juego de suerte y azar en la cual se sortean en una fecha predeterminada premios en especie entre quienes adquirieron o son poseedores de unas varias boletas, emitidas en serie continua y puestas en venta en el mercado a precio fijo por un tercero debidamente autorizado. Son del orden territorial las rifas se operen: en un municipio o el Distrito Capital, en más de un municipio de un mismo departamento o en un municipio y el Distrito Capital.
Promocionales: Son modalidades de juegos de suerte y azar organizados y operados con fines de publicidad o promoción de bienes o servicios, por establecimientos, empresas, o entidades, en los cuales se ofrece un premio al público, sin que para acceder al juego se pague directamente. Son del orden territorial los promocionales que se operen: en un municipio o el Distrito Capital, en más de un municipio de un mismo departamento o en un municipio y el Distrito Capital.
Seguimiento: Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la planeación futura.
Sistema: Conjunto de cosas o partes coordinadas, ordenadamente relacionadas entre sí, que contribuyen a un determinado objetivo.
SNS: Superintendencia Nacional de Salud.
Técnicas para manejar el Riesgo: Inaceptables, Moderados, Tolerables y Aceptables.
Tipologías: Descripción de los modos y características de las acciones desarrolladas por la delincuencia para la comisión de delitos.
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.
Tratamiento del riesgo: Conjunto de medidas administrativas tendientes a mitigar o reducir la probabilidad o impacto de los eventos de riesgo.
Valoración del riesgo: Es el resultado de confrontar la evaluación del riesgo con los controles existentes

MARCO DE REFERENCIA CON EL MIPG

El modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades en la Lotería de Medellín, este modelo tiene el fin de generar resultados que atiendan los planes, programas y proyectos y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio Manual Operativo MIPG 2019 el cual opera a través de 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán que el modelo funcione y opere adecuadamente, en la siguiente figura podemos visualizar las 7 dimensiones del modelo:

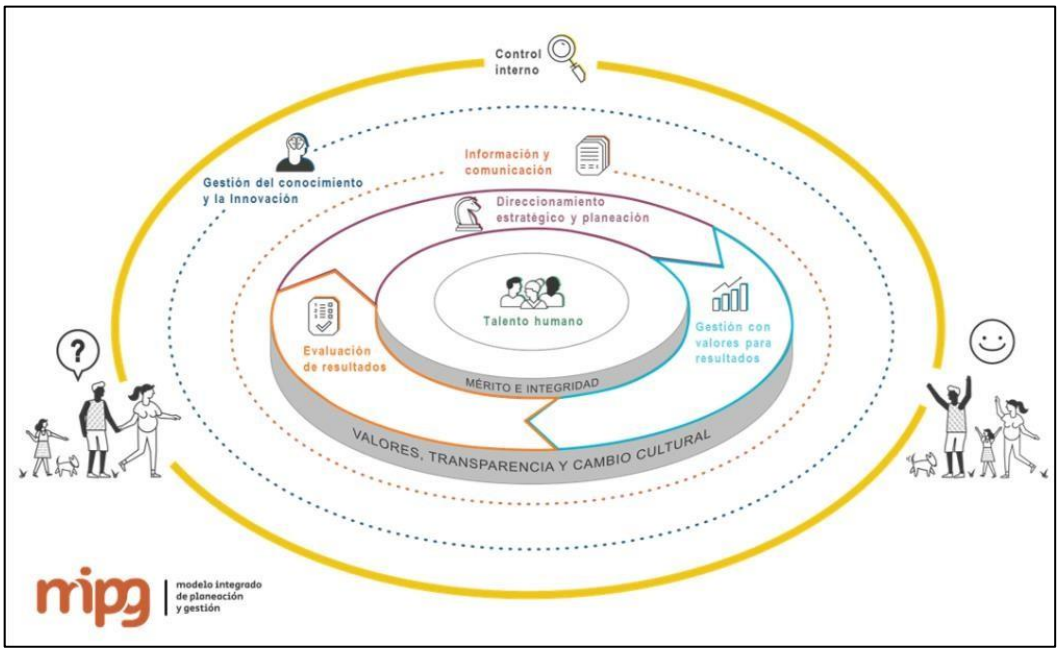


Figura 1 Esquema general del modelo integrado de planeación y gestión (MIPG)

De acuerdo con el numeral 2.2.1 “política de planeación institucional” de la dimensión “Direccionamiento estratégico y planeación” del MIPG, para responder a la pregunta ¿cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su

cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

En este sentido, es claro que la identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos.

El Modelo Integrado de Planeación y Gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

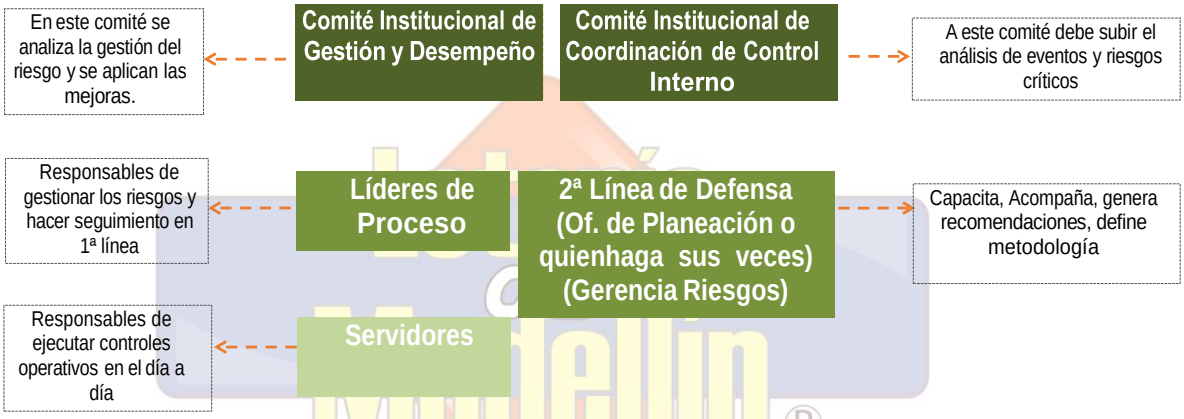


Figura 2. Dirección de Gestión y Desempeño Institucional de Función Pública

Nota: En entidades de alta complejidad se puede considerar la figura de gestores de riesgos. Se trata de personas clave en las áreas o procesos que ayudan al líder de proceso y a la 2ª línea de defensa en la gestión del riesgo, esta figura es opcional no obligatoria en su implementación.

Beneficios

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la

administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones
- Garantizar la operación normal de la organización
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
- Fortalecimiento de la cultura de control de la organización
- Incrementa la capacidad de la entidad para alcanzar sus objetivos
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente
- Fomentar la gestión proactiva
- Ser conscientes de la necesidad de identificar y tratar el riesgo en toda la Entidad
- Cumplir con las exigencias legales y reglamentarias pertinentes, así como las normas internacionales
- Mejorar la información financiera
- Mejorar la gobernabilidad
- Mejorar la confianza de los grupos de interés (*stakeholder*)
- Establecer una base confiable para la toma de decisiones y la planificación
- Asignar y utilizar con eficacia los recursos para el tratamiento del riesgo
- Mejorar la eficacia y eficiencia operacional
- Mejorar la salud y seguridad, así como la protección del medio ambiente
- Mejorar la prevención de pérdidas, así como la gestión de incidentes
- Mejorar el aprendizaje organizacional

COMPROMISO DE LA DIRECCIÓN

El compromiso adquirido por la Alta Dirección de la Lotería de Medellín para el año 2017 en la actualización del Modelo de Operación por Procesos -MOP- determinó la estructura organizacional con la colaboración, apoyo y asesoramiento en materia de riesgos de la Entidad de la Oficina de Planeación, e igualmente se identifica los interesados de gestionar la gestión de riesgos de la Entidad y cada uno de sus procesos, tal como se puede apreciar en el MOP (Modelo de Operación por Procesos) de la Lotería de Medellín.

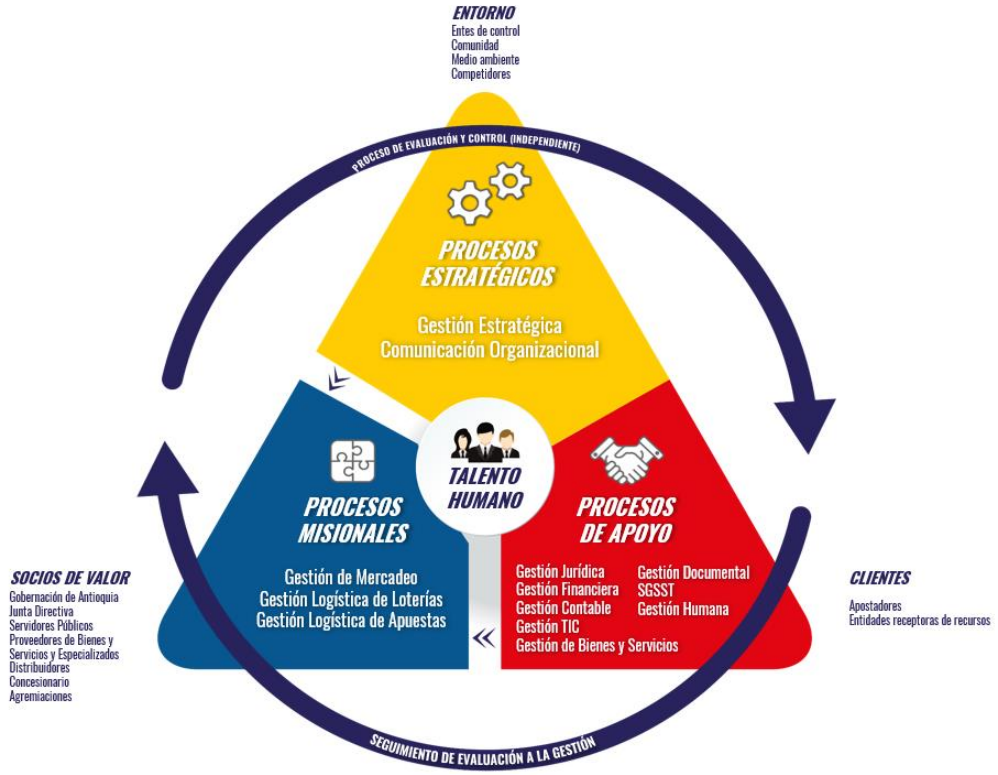


Figura 3. Mapa de procesos de la Lotería de Medellín

Siendo la Lotería de Medellín una Entidad de la administración pública debe darle cumplimiento a su misión constitucional y legal, a través de los objetivos institucionales los cuales desarrollan a partir del diseño y ejecución de los diferentes planes, programas y proyectos. El cumplimiento de dichos objetivos se puede ver afectado por la presencia de riesgos, ocasionados por factores tanto internos como

externos, razón por la cual se hace necesario contar con acciones tendientes a administrarlos dentro de la Entidad.
Para el éxito en la Implementación de una adecuada Gestión del Riesgo, es indispensable el compromiso de la Alta Dirección como encargada, en primera instancia, de estimular la cultura de la identificación y prevención del riesgo y en segunda instancia de definir las políticas. Para lograrlo es importante la definición de canales directos de comunicación y el apoyo a todas las acciones emprendidas en este sentido, propiciando los espacios y asignando los recursos necesarios. Así mismo, debe designar a un directivo de primer nivel que asesore y apoye todo el proceso de diseño e implementación del Componente de la Gestión del Riesgo.

Es importante definir los líderes de los procesos para trabajar el tema en las diferentes dependencias y conozcan muy bien la entidad y el funcionamiento de los diferentes procesos para que se facilite la administración del riesgo y la construcción de los mapas de riesgos institucionales.

Es significativo que se implementen los mecanismos que permitan visualizar y estar atento a la aparición de nuevos riesgos que se generen por los desarrollos socioeconómicos y tecnológicos, y que cada funcionario de la Entidad sea:

- Responsable de desarrollar la política de gestión del riesgo dentro de su organización;
- Encargado de asegurar que el riesgo se gestiona de manera eficaz dentro de la organización, considerada en su totalidad o en un área, un proyecto o una actividad específicos;
- Responsables de evaluar la eficacia de una organización en materia de gestión del riesgo; y
- Los que desarrollan normas, guías, procedimientos y códigos de buenas prácticas que, en su totalidad o en parte, establecen cómo se debe tratar el riesgo dentro del contexto de la Misión de la Entidad.

Es así que los jefes o líderes de los procesos deben de tener en cuenta estos tres compromisos:

1. ***Saber:*** Debe conocer en profundidad el proceso que lidera, sus objetivos y riesgos.
2. ***Poder:*** Debe tener capacidad para la toma de decisiones y mejorar el proceso, en función del grado de responsabilidad delegada a cada uno.

3. ***Querer:*** Debe entender el valor de gestionar los riesgos y asumir voluntariamente su responsabilidad contribuyendo así al logro de los objetivos estratégicos de la Entidad.

CONOCIMIENTO Y ANÁLISIS DE LA ENTIDAD

Este desarrollo se da en los diferentes niveles de la organización, por lo que cada entidad, de acuerdo con su esquema de direccionamiento estratégico, procesos, procedimientos, políticas de operación, sistemas de información, tendrá insumos esenciales para iniciar con la aplicación de la metodología propuesta para la administración del riesgo. En la Figura 4 se puede observar esta interrelación.

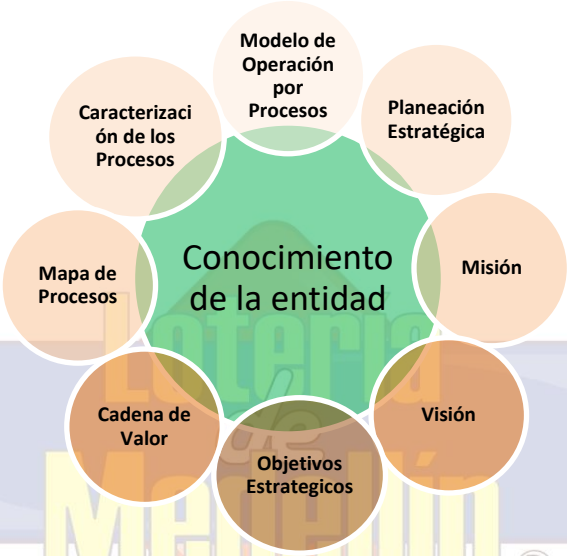


Figura 4 Conocimiento y análisis de la entidad

Modelo de operación por Procesos (MOP): el modelo de operación por procesos es el estándar organizacional que soporta la operación de la entidad, integrando las competencias constitucionales y legales que rigen con el conjunto de planes y programas necesarios para el cumplimiento de su misión, visión y objetivos estratégicos, con lo que se pretende determinar la mejor y más eficiente forma de ejecutar las operaciones de la entidad.

Planeación Estratégica: las estrategias de la Entidad, generalmente se definen por parte de la Alta Dirección con el apoyo del personal de la organización, y obedecen a la razón de ser que desarrolla la misma, a los planes que se traza en el medio de juegos de suerte y azar, a políticas específicas que define sus entes rectores, en

este contexto la entidad define su planeación y hace uso de sus procesos estratégicos, misionales, de apoyo y de evaluación para materializarla o ejecutarla, por lo tanto la administración del riesgo no puede verse de forma aislada.
Misión: constituye la razón de ser de la Lotería de Medellín; sintetiza los principales propósitos estratégicos y los valores esenciales que deben ser conocidos, comprendidos y compartidos por todas las personas que hacen parte de la Lotería de Medellín.

Visión: es la proyección de la Lotería de Medellín a largo, que permite establecer su direccionamiento el rumbo, las metas y lograr su desarrollo. Debe ser construida y desarrollada por la Alta Dirección de manera participativa, en forma clara, amplia, positiva, coherente, convincente, comunicada y compartida por todos los empleados de la entidad.

Objetivos Estratégicos: identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable de la entidad. El cumplimiento de estos objetivos institucionales se materializa a través de la ejecución de la planeación anual de la Lotería de Medellín.

Cadena de valor: es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios o grupos de interés.

Mapa de procesos: es la representación gráfica de los procesos estratégicos, misionales, de apoyo y de evaluación y sus interacciones.

Caracterización de procesos: estructura que permite identificar los rasgos distintivos de los procesos. Establece su objetivo, la relación de los demás procesos, los insumos, los activos, su transformación a través de las actividades que desarrolla y las salidas del proceso, se identifican los proveedores y clientes o usuarios, que pueden ser internos o externos.

Nota: para los objetivos de los procesos como punto de partida fundamental para la identificación del riesgo debemos de tener en cuenta que estos objetivos son los resultados que se espera lograr para cumplir la misión y visión. Debemos de determinar el cómo logro la política trazada y el aporte que se hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: establecer, identificar, recopilar, investigar, registrar, buscar.

La Lotería de Medellín como entidad pública que maneja recursos públicos debe necesariamente, contar con unos procesos que regulen su gestión garantizando que genere resultados visibles y medibles para la ciudadanía. Bajo este principio, el Gobierno Nacional de Colombia ha establecido que todas las entidades de carácter público deben desarrollar un Plan Estratégico Institucional que garantice planeación, calidad, ejecución, desempeño y seguimiento a su gestión.

Es por esto que la Lotería de Medellín, como Empresa Industrial y Comercial del Estado del orden departamental, mediante la formulación del Plan Estratégico define la ruta de su gestión institucional para el próximo cuatrienio, esta ruta está alineada con el Plan de Desarrollo Departamental.

El Plan Estratégico Institucional está contemplado dentro del Modelo Integrado de Planeación y Gestión en la dimensión de direccionamiento estratégico y planeación, como una herramienta que define la ruta estratégica que guiará la gestión institucional de la entidad, con miras a satisfacer las necesidades de nuestros grupos de interés, así como fortalecer su confianza y legitimidad; todo esto, a través de la articulación de sus procesos y de una adecuada administración de los recursos.

En este sentido, el Plan Estratégico Institucional recoge todas las acciones que permiten dar cumplimiento a la Plataforma Estratégica de la Lotería de Medellín, además establece la manera en que esas decisiones se transformarán en acciones, garantizando el desempeño y el seguimiento de la gestión para alcanzar los resultados y estos sean visibles para los ciudadanos y grupos de interés.

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

CONTEXTO ESTRATÉGICO

El Contexto Estratégico se inicia desde la contextualización, formulación y operación de la política de administración del riesgo es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión de manera que no se perciba esta herramienta gerencial como algo aislado del mismo accionar administrativo. Por ende, el diseño se establece a partir de los insumos, la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos y por ende la salida de los productos, tal como se puede apreciar en la siguiente figura:

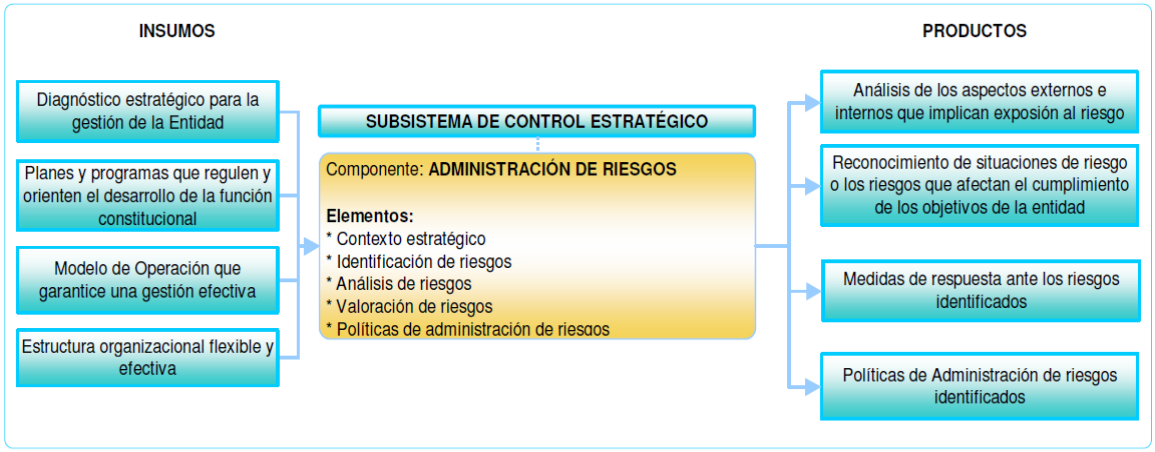


Figura 5 contexto estratégico

La detección de las situaciones de riesgo, que puedan afectar el normal desarrollo de una actividad, es una labor permanente en cada uno de los procesos de la Entidad, por lo cual involucra el compromiso y la participación de todos los funcionarios, dado que es cada uno de ellos quien mejor puede detectar oportunamente a través de su autocontrol las posibles desviaciones que pueden suceder en sus procesos.

Se recomienda la aplicación de varias herramientas y técnicas como, por ejemplo:

Entrevistas estructuradas con expertos en el área de interés, reuniones con directivos o jefes de oficina (Comités de Gerencia) y con personas de todos los niveles en la entidad, evaluaciones individuales usando cuestionarios, lluvias de ideas con los servidores de la entidad, entrevistas e indagaciones con personas ajenas a la entidad, usar diagramas de flujo, análisis de escenarios y hacer

revisiones periódicas de factores económicos y tecnológicos que puedan afectar la organización, entre otros.

Igualmente pueden utilizarse diferentes fuentes de información de la entidad, tales como registros históricos, experiencias significativas registradas, opiniones de especialistas y expertos, informes de años anteriores, los cuales pueden proporcionar información importante, la técnica utilizada dependerá de las necesidades y naturaleza de la entidad.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la entidad.
- Identificar los factores internos que pueden ocasionar la presencia de riesgos con base en el análisis de los componentes Ambiente de Control, Direccionamiento Estratégico y demás estudios que sobre la cultura organizacional y el clima laboral se hayan adelantado en la Entidad.
- Aportar información que facilite y enriquezca las demás etapas de la Administración del Riesgo.

También son fuentes valiosas para la identificación de riesgos, los resultados de las auditorías internas y externas. La Empresa cuenta con este manual de riesgos, en el cual se identifican y clasifican todos los riesgos a los cuales está expuesta la Entidad de acuerdo con su fuente u origen, a través de mapas de riesgos con su respectivo plan de acción.

El manual del riesgo establece las responsabilidades respecto a la aplicación objetiva, sistemática y homologada del procedimiento para el manejo óptimo de los riesgos, en el contexto de viabilizar la continuidad de las operaciones e incrementar la ventaja competitiva, preservando la integridad de los recursos de la Entidad.

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno de la Entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos.

LINEAMIENTOS RIESGOS DE GESTIÓN

Metodología

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

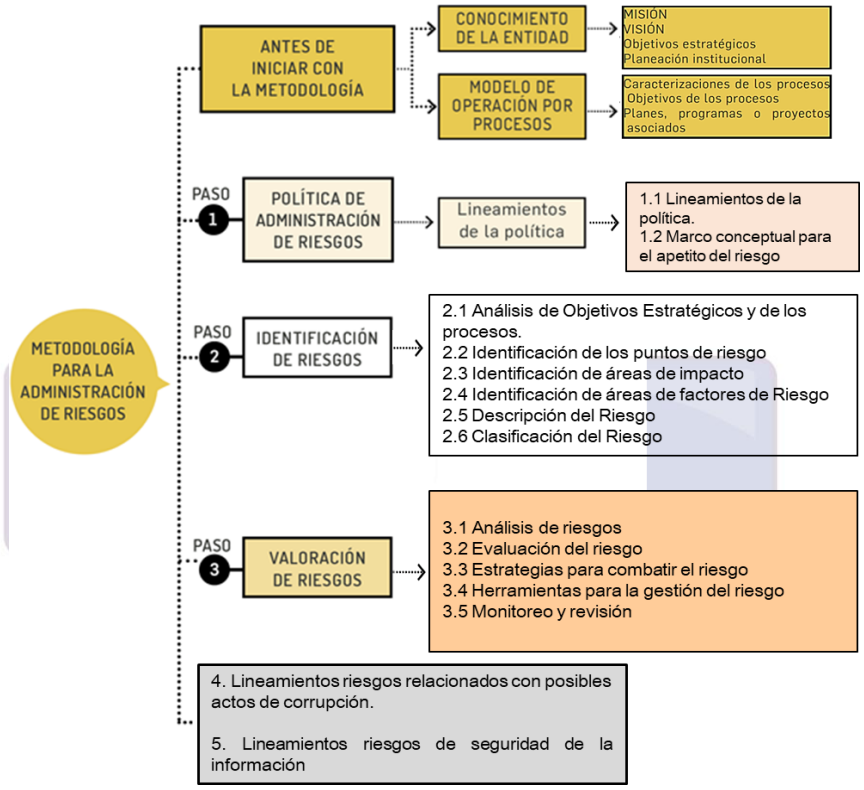


Figura 6 Metodología para la administración del riesgo, elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Pasos para la Administración del Riesgos

Para la implementación de la Gestión de Riegos en la Entidad, se conduce a un método lógico que se inicia con la identificación de riesgos en los procesos, para

luego efectuar su clasificación basados en el análisis y evaluación y finalmente adoptar decisiones que conducen a la reducción de las probabilidades de que ocurra el riesgo o de la minimización de la consecuencia en caso de que se materialice.

Para la implementación de la Gestión del Riesgo se toman como base los Planes, Programas y Proyectos, el Modelo de Operación y sus diferentes niveles de despliegue, a fin de establecer los posibles riesgos de los procesos y las actividades.

Este componente toma como base la identificación de los factores internos o externos y de operación que puedan afectar el desarrollo de la función administrativa de la entidad; una vez identificados se asocian a los procesos, analizándolos, valorándolos y calificándolos en términos de su impacto en la gestión. Finalmente, este resultado permitirá definir las directrices para la Administración del Riesgo, en base a eso insumos se debe definir la Gestión del Riesgo y generar uno productos tal como lo indica en los siguientes tres pasos:

PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos la Lotería de Medellín, es la declaración de la dirección y las intenciones generales de la Entidad con respecto a la gestión del riesgo y es donde se establece los lineamientos precisos acerca del tratamiento, manejo y seguimiento de los riesgos, y tiene un carácter estratégico, donde se acoge al modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas y las normas internacionales como buenas prácticas acogidas por la Entidad e incorporadas en el Manual de Administración de Riesgos de la Lotería de Medellín, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Esta política es establecida por la Alta Dirección, con el liderazgo del representante legal y con la participación activa del Comité Institucional de Coordinación de Control Interno, en la que se deben de tener en cuenta los objetivos estratégicos, los niveles de responsabilidad frente al manejo de los riesgos, los mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad, a las áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de procesos que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de contratación los podemos identificar desde el inicio del estudio de conveniencia y oportunidad de todos los procesos para la contratación d ele entidad.
- Los riesgos de LA/FT/FPADM puedan afectar la confidencialidad e integridad de nuestros grupos de valor en relación con la entidad.
- Los riesgos de Seguridad Digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad y los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

La Lotería de Medellín determina que la administración de riesgos aplicado dentro el Modelo de Operación por Procesos a toda la organización y acogida por la Entidad, es la herramienta para identificar, valorar, evaluar y administrar los riesgos

de Gestión, Contratación, de Corrupción, LA/FT/FPADM y de Seguridad Digital, para lo cual la oficina de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, cargue de información y dispone un manual de uso para el servicio de todos los procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual de la Oficina de Planeación, asegurando la articulación de éstos con los compromisos de cada proceso.

Objetivo

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.

Alcance

Aplica a todo el Modelo de Operación por Procesos de la Entidad hasta la identificación de los posibles riegos que puedan afectar su grupo de interés, las contrataciones y conocimiento del cliente. La tipificación de los riesgos previsibles podrá consistir en la identificación de los distintos riesgos que pueden ocurrir durante su relación con la entidad, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

Niveles de aceptación de riesgo

El 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.

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis de la entidad, iniciando con las siguientes definiciones:

a) Capacidad de riesgo:

Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual la Alta Dirección considera que no sería posible el logro de los objetivos de la entidad.

La entidad debe aplicar los valores de probabilidad e impacto contenidos en este Manual y con base en esto debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

i. Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
ii. Valor máximo que, según el buen criterio de la Alta Dirección y bajo los requisitos del marco legal aplicable a la Lotería de Medellín, puede ser resistido por la Entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección que no sería posible el logro de los objetivos de la entidad.

b) Tolerancia del riesgo

La tolerancia de 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.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la Alta Dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

c) 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.

Luego de definida la capacidad de riesgo por parte de la Alta Dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del Modelo Integrado de Planeación y Gestión en la Entidad.

Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la Entidad puede aceptar, relacionado 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.

Nota: para la decisión informada de tomar un riesgo particular, para los riesgos de corrupción es inaceptable la aceptación.

Gráficamente los anteriores conceptos se relacionan así:

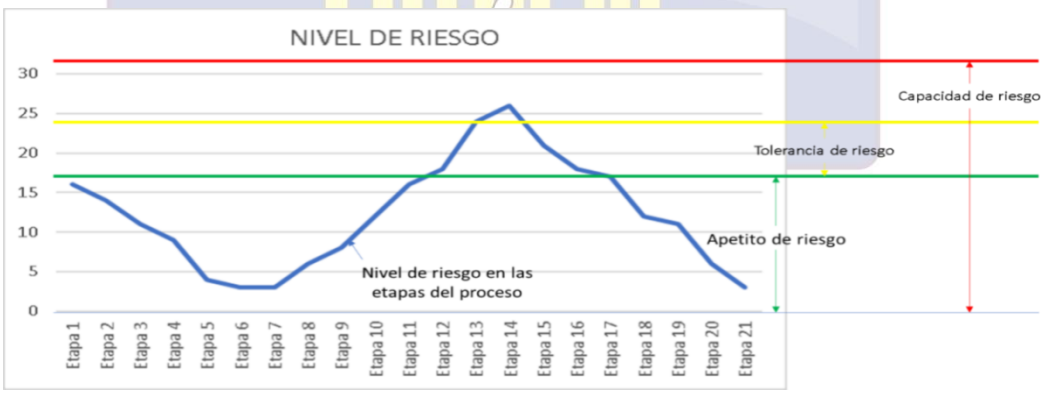


Figura 7. Definiciones de apetito, tolerancia y capacidad de riesgo

Usando un ejemplo sencillo como la velocidad a la que circula un vehículo, podría decirse que el vehículo admite una velocidad máxima de 200 km/h, o que su **capacidad** es de 200 km/h. pero su conductor, teniendo en cuenta su habilidad para conducir, el tipo de vía, la climatología y las condiciones del vehículo **toleraría** ir a un máximo de 160 km/h. aun así, considerando que su objetivo es llegar a su destino lo antes posible pero de forma segura, decide conducir el vehículo a 110

km/h, ya que es la velocidad que le permite hacer el recorrido respetando los límites establecidos, en un tiempo adecuado y sintiéndose confortable en la conducción. Este seria, por tanto, su nivel de **apetito**.

Niveles para calificar el impacto

Para determinar los niveles de impacto, se construye la tabla de criterios que definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional.

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

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.

NIVEL	RANGOS	DESCRIPCIÓN GENERAL	DESCRIPCIÓN	
			AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
1	Leve			
2	Menor			
3	Moderado			
4	Mayor			
5	Catastrófico			

Niveles para calificar la probabilidad

Para determinar los niveles de probabilidad de ocurrencia, se construye la tabla de criterios que definen las opciones de conocimiento de la actividad o de ejecuciones de actividades como las variables principales. Cabe señalar que la administración del riesgo contempla la exposición de los procesos de acuerdo con su conocimiento

o actividad del proceso, dependiendo de su nivel de madurez que se tiene de la gestión de los riesgos en la Lotería de Medellín.

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

Bajo el esquema de la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad las ocurrencias presentadas o la frecuencia con la que se lleva a cabo una actividad, ya que bajo esta óptica de mantener las dos opciones histórica y repetición de actividades.

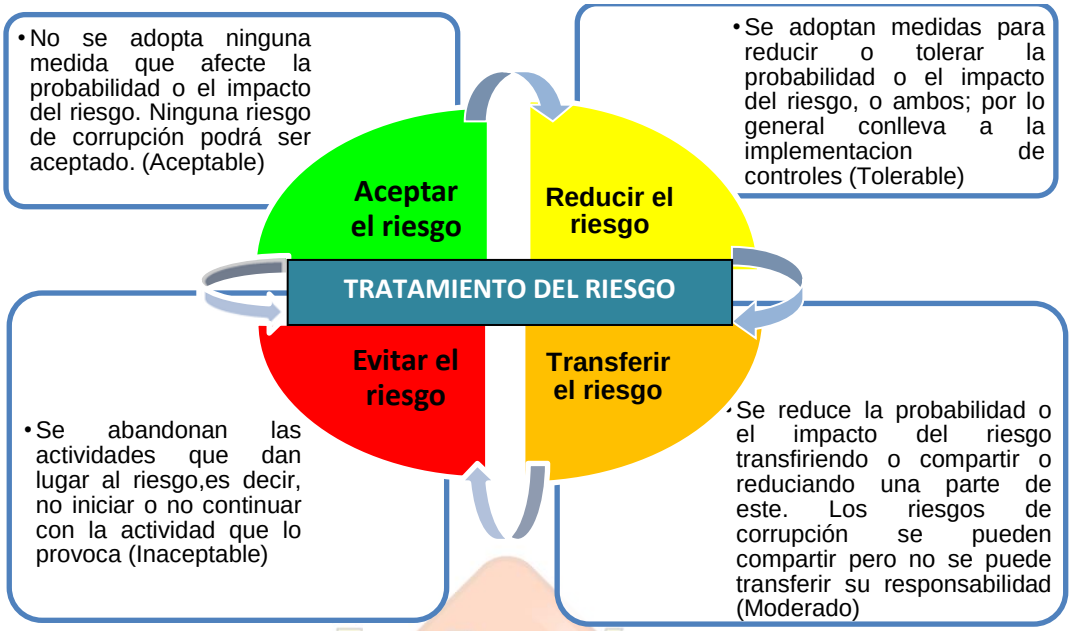
NIVEL	RANGO	Frecuencia	
		Opción 1 (Histórica)	Opción 2 (Actividades)
1	Muy baja		
2	Baja		
3	Media		
4	Alta		
5	Muy Alta		

Tratamiento del riesgo

El tratamiento de los riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos de gestión, contratación, LA/FT/FPADM e 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:



Monitoreo

Una vez diseñado y analizado la matriz de riesgos institucional de la Lotería de Medellín, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de los responsables de los procesos, el profesional de riesgos y en consecuencia con la Dirección de Auditoría Interna, su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. La Oficina de Auditoría Interna dentro de su función asesora comunicará y presentará luego del seguimiento y evaluación sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

PASO 2: IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la Lotería de Medellín, 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.

Análisis de objetivos estratégicos y de los procesos:

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

Nota: los objetivos deben de incluir el “qué”, “cuánto”, “cómo”, “con qué” y “cuándo” y, si no están bien definidos los objetivos, no se puede continuar con la metodología de este manual de riesgos.

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, 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, para lo cual puede hacer uso de las características SMART, cuya estructura se explica a continuación:

Usando un ejemplo la caracterización del proceso de Gestión de Bienes y Servicios de la Subgerencia Financiera, realizamos la siguiente alineación a los Objetivos estratégicos de la entidad y la finalidad de la oficina de planeación:

Objetivo estratégico 2: *Fortalecer la gestión institucional*

Teniendo presente que la finalidad de la Subgerencia Financiera es *"proveer los recursos financieros, físicos, los servicios requeridos en todos los procesos de la empresa, en condiciones de eficiencia, eficacia y transparencia, de acuerdo la normatividad, principios y buenas prácticas, respecto a su consecución, administración y suministro, propiciando de una parte la sostenibilidad y desarrollo financiero de la empresa en el corto, mediano y largo plazo y de otra el manejo eficiente de los recursos, con el propósito de garantizar la gestión de los procesos de la empresa"*

Una vez identificado la finalidad de la Subgerencia Financiera y los Objetivos Estratégicos, construimos el objetivo de la Caracterización del proceso de Gestión Bienes y Servicios, mediante la metodología ***SMART***, dando como resultado la siguiente definición: "***Manejar y custodiar los bienes y servicios que adquiera la Lotería de Medellín para apoyar la gestión institucional, en cumplimiento a los planes de compra y servicios de manera permanente***".

Continuando con el ejemplo, bajamos la alineación a los procedimientos de la Gestión bienes y servicios del siguiente procedimiento e igualmente mediante la metodología SMART se construye:

Realizar los ingresos y salidas de elementos al almacén de los bienes adquiridos por la Entidad con el fin de ejercer y asegurar el control de las compras de elementos de consumo, artículos de inventarios, artículos devolutivos (Activos tangibles e intangibles) para las diferentes áreas. Y así poder tener los bienes devolutivos y de consumo inventariado y controlado oportunamente de forma eficiente y en cumplimiento a los planes de compra y servicios de manera permanente.

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.

Fuente: Dirección de Gestión y desempeño Institucional de función Pública, 2017

Usando como ejemplo el procedimiento codificado con el nombre *P-GBS-01 Entradas y salidas* del almacén del proceso de Gestión de Bienes y Servicios, el cual tiene como objetivo: "***Realizar los ingresos y salidas de elementos al almacén de los bienes adquiridos por la Entidad con el fin de ejercer y asegurar el control de las compras de elementos de consumo, artículos de inventarios, artículos devolutivos (Activos tangibles e intangibles) para las***

***diferentes áreas**. Y así poder tener los bienes devolutivos y de consumo inventariado y controlado oportunamente de forma eficiente y en cumplimiento a los planes de compra y servicios de manera permanente",* podemos identificar algunos puntos de riesgo que pueden afectar este objetivo, como son:

- No ejercer control al ingresar al sistema los bienes comprados.
- No ejercer control al identificar los bienes suministrados a los funcionarios, contratistas y practicantes.
- No ejercer control al identificar los bienes suministrados a los promocionales.
- No ejercer control sobre los bienes del inventario consumo.
- No ejercer control sobre los bienes muebles comprados por otras áreas.
- No ejercer control de la Conciliación mensual de los bienes entre contabilidad y almacén.
- No ejercer control para mantener actualizado los inventarios.
- No ejercer control por perdida, daño o hurto de los bienes.

Identificación de 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.

Continuando con el ejemplo anterior podemos identificar el impacto a lo que está expuesta la entidad por ***Perdida Económica***

Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos. En la siguiente tabla encontraremos un listado como ejemplo de factores de riesgo que puede tener una entidad.

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la Lotería de Medellín.		Falta de procedimientos, descripción de las actividades, falta de Transferencia del Conocimiento
			Errores de digitación, grabación, autorización, conciliación, consulta, suministro de información
			Errores en los pagos internos y externos

			Falta de capacitación y entrenamiento, temas relacionados con el personal, contratistas, dentro de sus funciones
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurtos activos de los bienes y de material POP
			Posibles comportamientos no éticos de los empleados y contratistas
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica dela entidad.		Daño de equipos internos o de los distribuidores o de la comercializadora para la venta de la Lotería de Medellín
			Caída de aplicaciones de venta, soporte, de los sistemas de información internos y de reporte de datos a las entidades vigilantes
			Caída de la WEB para el servicios y promoción en las redes sociales, sitio de la Lotería de Medellín, en la venta de la Lotería de Medellín, transmisión en la devolución de los distribuidores y envió de información
			Errores en programas, en las bases de datos, en las aplicaciones de venta
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Normatividad	Eventos relacionados con la regulación para la operación de los juegos de suerte y azar		Falta regulación para los mecanismos de explotación para los juegos de suerte y azar de los entes territoriales
			Falta apoyo en la normatividad para competir con los privados

Los factores de riesgo para la Lotería de Medellín son identificados de acuerdo a su complejidad propia y en el sector 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.

Continuando con el ejemplo anterior podemos identificar el factor de riesgo a lo que está expuesta la entidad por ***Procesos y Talento Humano.***

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 la siguiente 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 yDesempeño 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 Lotería de Medellín 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.

Continuando con el ejemplo anterior podemos describir los riesgos a lo que está expuesta la entidad para este procedimiento de *P-GBS-01 Entradas y Salidas* del almacén del proceso de Gestión de Bienes y Servicios, así:

- *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*
- *Posibilidad de pérdida económica por pérdida, daño o hurto de bienes de la entidad a los funcionarios o en la bodega del almacén por no ejercer el debido control sobre los bienes muebles e inmuebles de 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*.

Clasificación del riesgo

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

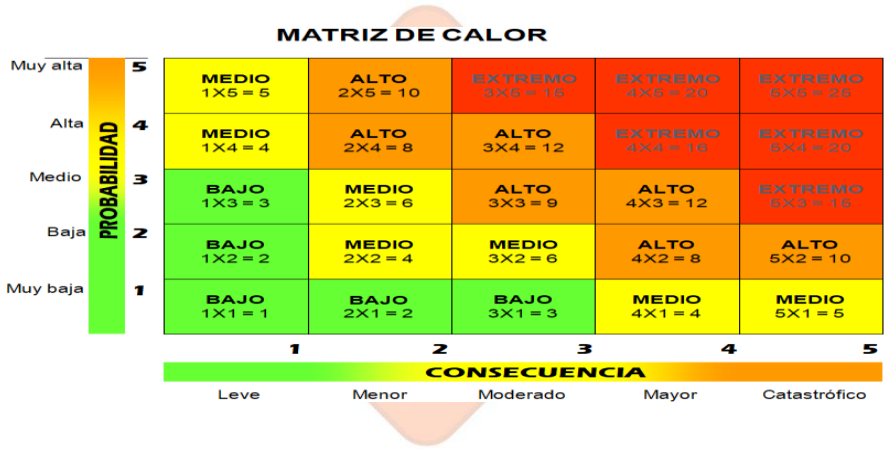
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones 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.

Continuando con el ejemplo anterior podemos identificar la clasificación del riesgo teniendo presente el área de factor a lo que está expuesta el procedimiento, es así que lo clasificamos en la siguiente categoría ***Ejecución y administración de procesos.***

Matriz de calor

El mapa de riesgos o también conocido como Mapa de Calor de riesgos, es una herramienta de visualización de datos para comunicar los riesgos específicos que enfrenta la Lotería de Medellín, este mapa de riesgos ayuda a la empresa a identificar y priorizar los riesgos asociados con su negocio, así:



Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, para el caso de la Lotería de Medellín se definen 4 zonas de severidad en la matriz de calor: Extremo, Alto, Medio y Bajo, en la siguiente tabla podemos ver la identificación donde está situado el riesgo después de realizar la valoración del impacto y la probabilidad, así:

EXTREMO **15 - 25**	**INACEPTABLE**: Tratar el riesgo. Un riesgo situado en esta zona de la matriz significa que en ninguna circunstancia se deberá mantener un riesgo con esa capacidad potencial de afectar la estabilidad de la empresa. Por ello estos riesgos requieren una atención inmediata o de alta Prioridad por parte de la Alta Gerencia para buscar disminuir o eliminarlos lo más pronto posible su afectación.
ALTO **8 - 12**	**MODERADO**: Tratar el riesgo. Un riesgo situado en esta zona de la matriz significa que se requiere desarrollar acciones prioritarias a corto plazo para su gestión, debido al alto impacto que tendrían sobre el sistema. Requiere atención de la alta gerencia.
MEDIO **4 - 6**	**TOLERABLE**: Retener el riesgo. Un riesgo situado en esta zona de la matriz significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, tienen una prioridad de segundo nivel, pudiendo ser a mediano plazo. Se deben mantener los controles existentes y la responsabilidad de la gerencia es específica.
BAJO **1 - 3**	**ACEPTABLE**: Retener el riesgo. Un riesgo situado en esta zona de la matriz significa que la combinación Probabilidad-Consecuencia no implica una gravedad significativa, por lo que no amerita la inversión de recursos y no requiere acciones adicionales para la gestión diferentes a las ya aplicadas en el riesgo. Se deben mantener los controles existentes y se administra con procedimientos rutinarios.

PASO 3: VALORACIÓN DEL RIESGO

Análisis del riesgo

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, tal como se indica a continuación:

Determinar la probabilidad

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo, identificado en la siguiente tabla:

PROBABILIDAD

NIVEL	RANGO	Frecuencia	
		Opción 1 (Conocimiento)	Opción 2 (Actividades)
1	Muy baja	Virtualmente imposible, se acerca a lo imposible. Puede ocurrir solamente en circunstancias excepcionales.	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.
2	Baja	Imaginable pero poco posible, ha ocurrido en otra parte. Podría ocurrir algunas veces.	La actividad que conlleva el riesgo se ejecuta de 3 a 79 veces por año.
3	Media	Poco usual. Ha ocurrido o puede ocurrir aquí. Es posible que ocurra algunas veces.	La actividad que conlleva el riesgo se ejecuta de 80 a 149 veces por año
4	Alta	Muy posible, con gran probabilidad de ocurrencia. Puede ocurrir en la mayoría de las circunstancias	La actividad que conlleva el riesgo se ejecuta mínimo 150 veces al año y máximo 299 veces por año
5	Muy Alta	Muy probable, de alta probabilidad de ocurrencia. Se espera que ocurra en la mayoría de las circunstancias	La actividad que conlleva el riesgo se ejecuta más de 300 veces por año

Continuando con el ejemplo anterior podemos describir la probabilidad de ocurrencia del riesgo a lo que está expuesta la entidad, para este procedimiento de *P-GBS-01 Entradas y Salidas* del almacén del proceso de Gestión de Bienes y Servicios, de los dos riesgos identificados:

- *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*
  Probabilidad: se identifica la frecuencia en la opción 2 de actividades *"La actividad que conlleva el riesgo se ejecuta de 3 a 79 veces por año"*, ubicada en el nivel 2.

- *Posibilidad de pérdida económica por pérdida, daño o hurto de bienes de la entidad a los funcionarios o en la bodega del almacén por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*
  Probabilidad: se identifica la frecuencia en la opción 1 de conocimiento, *"Poco usual, ha ocurrido o puede ocurrir aquí. Es posible que ocurra algunas veces"*, ubicada en el nivel 3

Determinar el impacto

Determinar el impacto: se entiende como los impactos económicos o reputacionales como variables principales de ocurrencia del riesgo, identificado en la siguiente tabla:

CONSECUENCIA

NIVEL	RANGOS	DESCRIPCIÓN GENERAL	DESCRIPCIÓN	
			AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
1	Leve	Perdidas financieras pequeñas	Menor a 1 SMLMV	De conocimiento **INTERNO** Sin consecuencias
2	Menor	Perdidas financieras medianas	Mayor que 1 SMLMV Menor que 5 SMLMV	De conocimiento **INTERNO** Con consecuencias
3	Moderado	Perdidas financieras altas	Mayor que 5 SMLMV Menor que 50 SMLMV	De conocimiento **EXTERNO** (CLIENTES-REGIONAL) Con consecuencias
4	Mayor	Perdidas financieras importantes	Mayor que 50 SMLMV Menor que 300 SMLMV	De conocimiento **EXTERNO** (SOCIOS DE VALOR-NACIONAL) Con Consecuencias
5	Catastrófico	Perdidas financieras enormes	Mayor que 300 SMLMV	De conocimiento **EXTERNO** (ENTORNO-INTERNACIONAL) Con Consecuencias

Continuando con el ejemplo anterior, podemos describir la probabilidad de ocurrencia del riesgo a lo que está expuesta la entidad, para este procedimiento de *P-GBS-01 Entradas y Salidas* del almacén del proceso de Gestión de Bienes y Servicios, de los dos riesgos identificados:

- *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*

Impacto: se identifica la afectación económica, *"Mayor que 5 SMLMV y Menor que 50 SMLMV"*, ubicada en el nivel 3.

- *Posibilidad de pérdida económica por pérdida, daño o hurto de bienes de la entidad a los funcionarios o en la bodega del almacén por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*
  Impacto: se identifica la afectación económica, *"Mayor que 1 SMLMV y Menor que 5 SMLMV"*, ubicada en el nivel 2.

Evaluación de riesgos

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

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.

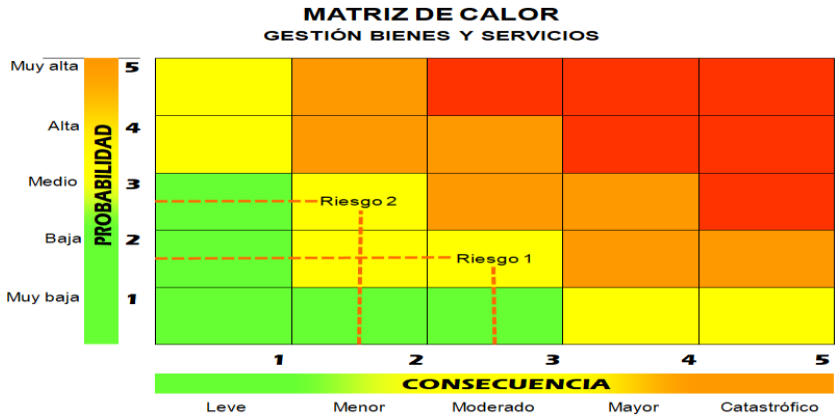
Una vez analizado se debe evaluar el riesgo:

- ***Nivel del riesgo***: Se define como el producto de la Probabilidad por la Consecuencia (NR = P X C) riesgo ***Inherente***.
- Inicialmente se evalúa el Nivel del riesgo ***Absoluto*** (considerando que NO existen controles o no están operando).
- Luego se evalúa el Nivel del riesgo ***Bruto*** (considerando que los controles existentes están operando).
- Posteriormente se recalifica el riesgo ***Residual*** (considerando que las medidas de tratamiento planteadas o implantadas funcionan de manera eficaz).

Continuando con el ejemplo realizamos la evaluación del nivel del riesgo:

#	Descripción del riesgo	Probabilidad	Consecuencia	Nivel de riesgo
1	*Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*	2	3	NR: 2x3=**6** **Medio**
2	*Posibilidad de pérdida económica por pérdida, daño o hurto de bienes de la entidad a los funcionarios o en la bodega del almacén por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*	3	2	NR: 3x2=**6** **Medio**

Aplicando la matriz de calor tenemos a la evaluación del riesgo en ejemplo lo podemos ubicar en la siguiente imagen:



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.

Estructura para la descripción del control:

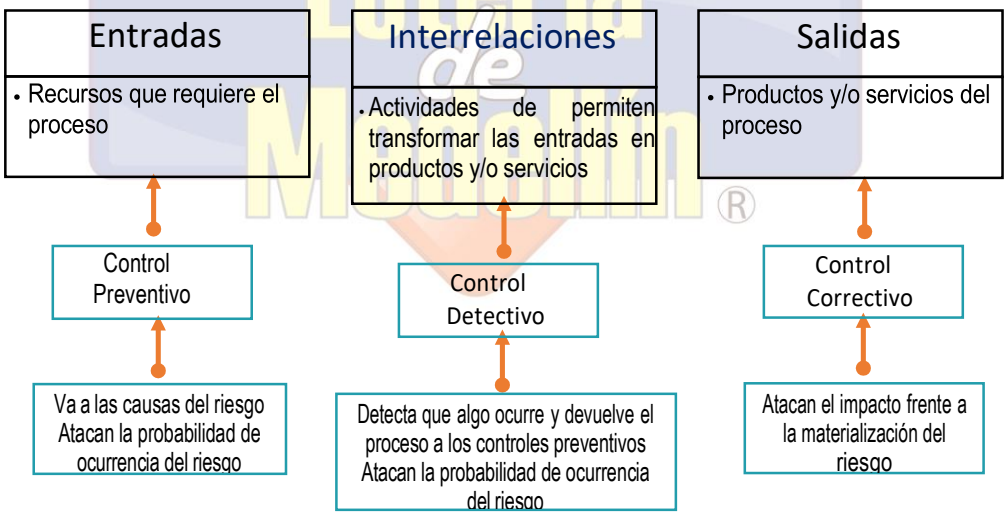
Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- **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.

Continuando con el ejemplo del procedimiento de *P-GBS-01 Entradas y Salidas* del almacén del proceso de Gestión de Bienes y Servicios, se describe el siguiente control:

Tipología de controles

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente imagen se consideran 3 fases globales del ciclo de un proceso así:



Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

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

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

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

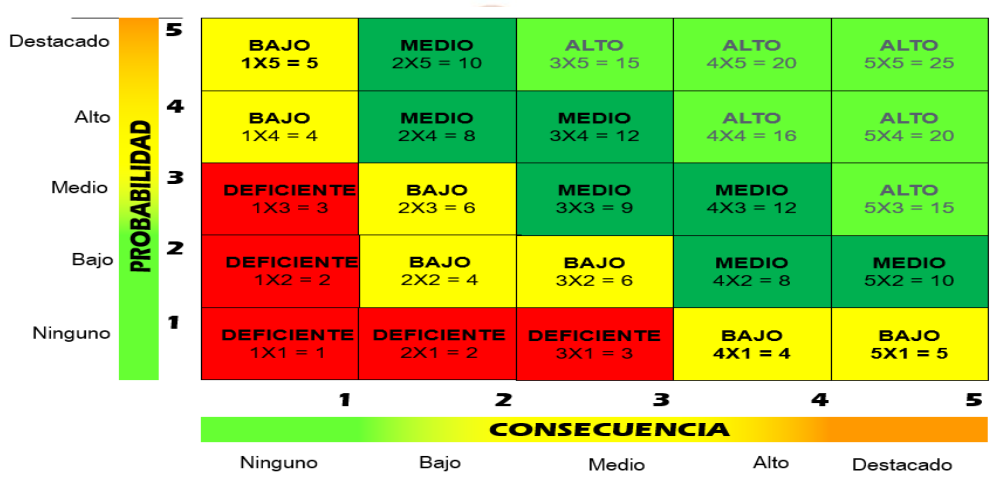
Análisis y evaluación de los controles – Tipología

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

Características				Descripción	Peso
PROBABILIDAD	Tipologías de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	2
			Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	1
		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	2
			Manual	Controles que son ejecutados por una persona, tiene implícito el error humano	1
		Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	1
			Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	1
				Suma	
CONSECUENCI	Tipologías de formalización	Tipo	Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	0

		Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	3
			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.	1
		Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	2
			Sin registro	El control no deja registro de la ejecución del control.	1
				Suma	

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura tal como se muestra el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Evaluación del control: se trata de determinar los niveles de control del riesgo a través de la combinación entre la probabilidad y la consecuencia (impacto). Se definen 4 zonas de control en la matriz de calor

Una vez analizado se debe evaluar el control:

- ***Nivel del control***: Se define como el producto de la Probabilidad (atributos de eficiencia) por la Consecuencia (atributos de formalización), Control = P X C.

Continuando con el ejemplo realizamos la evaluación del control del riesgo:

Proceso: *P-GBS-01 Entradas y salidas*

Objetivo: ***Realizar los ingresos y salidas de elementos al almacén de los bienes adquiridos por la Entidad con el fin de ejercer y asegurar el control de las compras de elementos de consumo, artículos de inventarios, artículos devolutivos (Activos tangibles e intangibles) para las diferentes áreas. Y así poder tener los bienes devolutivos y de consumo inventariado y controlado oportunamente de forma eficiente y en cumplimiento a los planes de compra y servicios de manera permanente***

Riesgo 1 identificado: *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*

Probabilidad Inherente= 2
Impacto Inherente= 3
Zona de riesgo= medio
Controles identificados:

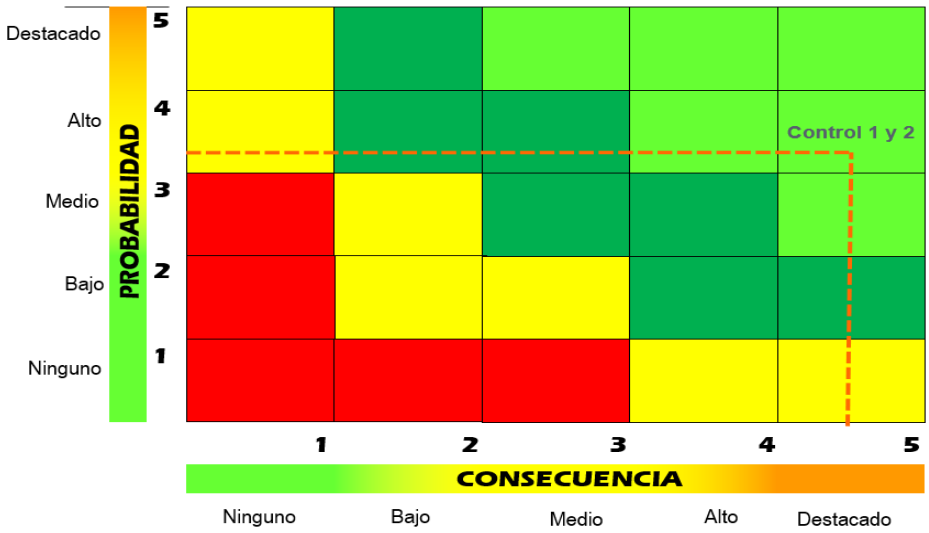
Control 1: *El almacenista general realiza entrada y salidas de bienes mediante las actas y se comprara el inventario físico con el aplicativo según la periodicidad establecida en el procedimiento*.

Control 2: *El almacenista general realiza la entrega de los bienes muebles, mediante actas de salida y se realiza invitarlo físico anual y/o cuando se requiera según la periodicidad establecida en el procedimiento.*

Si observamos la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos:

Características				Descripción	Control 1	Control 2
PROBABILIDAD	Tipologías de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	2	2
			Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.		
		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		
			Manual	Controles que son ejecutados por una persona, tiene implícito el error humano	1	1
		Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	1	1
			Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo		
				Suma	**4**	**4**
CONSECUENCIA	Tipologías de formalización	Tipo	Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.		
		Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	3	3
			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		
		Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	2	2
			Sin registro	El control no deja registro de la ejecución del control		
				Suma	**5**	**5**

Aplicando la matriz de calor tenemos a la evaluación del control en ejemplo lo podemos ubicar en la siguiente imagen:



Efectividad del control

De acuerdo con lo anterior se evalúa la Efectividad de los controles e identificación del Riesgo Residual tal como se puede apreciar a continuación:

Continuando con el ejemplo del procedimiento de Gestión de Bienes y Servicios, del procedimiento *P-GBS-01 Entradas y salidas*, del riesgo 1: *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad.*

El promedio de los controles: Control 1: 20 y Control 2: 20 = **Promedio: 20**

La efectividad del control lo ubicamos en la siguiente imagen, el resultado dado del promedio 20, está ubicado entre 13 a 25 la efectividad es **Alto,** tal como se puede visualizar en la siguiente imagen:

EFECTIVIDAD	RESULTADO	EVALUACIÓN DEL CONTROL
ALTO	DE 13 A 25	Se da por el promedio de la Evaluación de los controles del riesgo
MEDIO	DE 7 A 12	
BAJO	DE 4 A 6	
DEFICIENTE	DE 1 A 3	

Riesgo residual

El riesgo residual, es el resultado de aplicar la efectividad de los controles al riesgo inherente, esta se da de la siguiente forma, se divide el Nivel del Riesgo sobre el promedio del control.

Continuando con el ejemplo del riego 1: *Posibilidad de pérdida económica debido a que no se cuenta con los inventarios actualizados por no ejercer el debido control sobre los bienes muebles e inmuebles de la entidad,* podemos valorar el riesgo residual así:

Riesgo residual = Nivel del riesgo 6 dividido el promedio de los Controles 20, dando como resultado: 0.3 el cual es **Tolerable**, esta valoración la podemos visualizar en la siguiente imagen:

NIVEL DEL RIESGO RESIDUAL	VALORACION
INACEPTABLE	> 5
IMPORTANTE	DE 3 A 5
MODERADO	DE 1.5 A 2.99
TOLERABLE	< 1.49

Los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

Formato mapa de riesgos

Es una herramienta de Excel que de forma metodológica nos permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y donde podemos encontrar las siguientes particularidades:

a) **Identificación del riesgo:** acá establecemos la estructura del riesgo; fuentes o factores, internos o externos, generadores de riesgos; puede hacerse a cualquier nivel: total entidad, por áreas, por procesos, incluso, bajo el viejo paradigma, por funciones; desde el nivel estratégico hasta el más humilde operativo y lo vamos a identifica así:

- Proceso
- Número de riesgo
- Nombre del riesgo
- Causa inmediata
- Clasificación del riesgo
- Responsable
- Causas o por qué (probabilidad)
- Consecuencias (impacto)
- Nivel del riesgo: evaluación de la consecuencia e impacto, riesgo bruto y apetito del riesgo

b) Valoración del riesgo

- Numero de control
- Tipo de riesgo
- Descripción del control
- Afectación
- Tipología de eficiencia (consecuencia): tipo, implementación y frecuencia
- Tipología de formalización (impacto): tipo, documentación y evidencia
- % de avance de implementación del control y tratamientos
- Efectividad del control: riesgo bruto, evaluación del control, riesgo residual, interpretación
- Opciones de tratamiento
- Documentación del riesgo: plan, procedimiento y/o formato de actividad
- Plan de contingencia

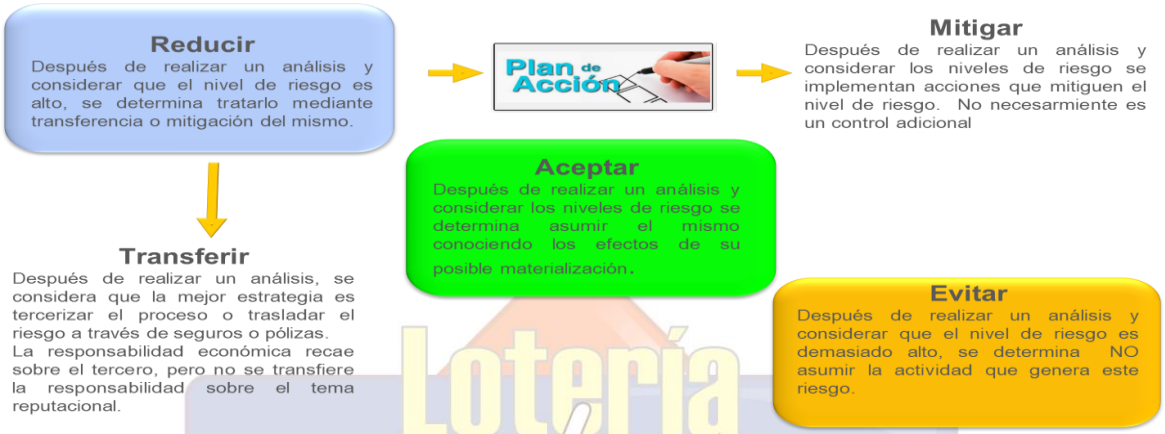
c) Planes de acción

- Plan de acción del riesgo
- Responsable
- Fecha implementación
- Fecha de seguimiento
- periodicidad
- Seguimiento
- Estado

Estrategias para combatir el riesgo

Las estrategias son las decisiones 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.

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.



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.

Herramientas para la gestión del riesgo

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

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)
- Secretaria General
- Líneas internas de denuncia y atención al cliente
- Buzones del primer piso de la Lotería de Medellín

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

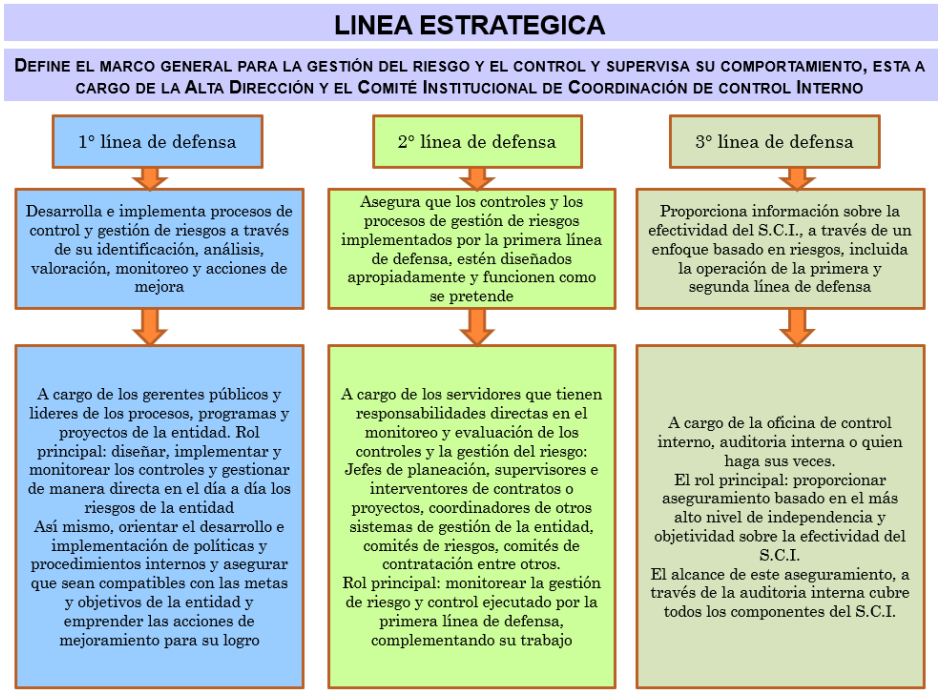
Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la salida de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia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

PROCESO ASOCIADO	INDICADOR	MÉTRICA	
		Histórica	Actividades
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Cantidad de horas de interrupción de los últimos 5 años	Número de horas de interrupción de aplicativos críticos al mes
Financiera	Tiempo de interrupción de aplicativos críticos en el mes	Cantidad de reportes fuera de términos en los últimos 5 años	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	Cantidad de solicitudes reiterativas o reiteraciones de conceptos no adecuados en los últimos 5 años	% solicitudes mensuales fuera de términos% solicitudes reiteradas por tema
Financiera	Errores en transacciones y su impacto en la gestión presupuestal	Cantidad de transacciones sobre la capacidad disponible en los últimos 5 años	Volumen de transacciones al mes sobre la capacidad disponible

Talento Humano	Rotación de personal	Cantidad de empleados que abandonan el puesto de trabajo o son retiraos por la administración en los últimos 5 años	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

Monitoreo y revisión

El Modelo Integrado de Plantación y Gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:



Responsabilidades

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:
Tabla 1. Responsabilidades de las Líneas de Defensa

Línea de defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité de Gerencia y CGDI	• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, LA/FT/FPADM y de Corrupción. • Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control de los riesgos de Gestión, Corrupción y LA/FT/FPADM. • Recomendaciones de mejoras a la política de operación para la administración del riesgo. • Garantizar el cumplimiento de los planes de la entidad. • Someter a aprobación del Gerente la política de administración del riesgo previamente estructurada por parte de la Oficina de Planeación, como segunda línea de defensa en la entidad. • Hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.
	CICCI	• Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Revisar la política de administración del riesgo por lo menos una vez al año y recomendar mejoras a la política de operación para la administración del riesgo actualización y validar su eficacia a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.
Primera Línea de defensa	Líderes de los Procesos Responsable del proyecto Servidores en General	• Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "Administración de riesgo" la política, metodología y el Manual de Administración de Riesgos aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos. • Informar a la Oficina de Planeación los cambios de responsables de reporte en caso de ausentismo laboral. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. • Revisar de acuerdo con su competencia y alcance la documentación de continuidad del negocio. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • Reportar a la Oficina de Planeación los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • 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 de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. • En caso de la materialización de un riesgo no identificado, este debe ser gestionado con el líder del proceso y el acompañamiento de la Oficina de Planeación y ser incluido en el mapa de riesgo institucional.
		El líder del proceso debe:

Primera Línea de defensa	Líderes de los Procesos Responsable del proyecto Servidores en General	• Verificar las acciones preventivas y registrar el avance junto con la evidencia en el SGI de acuerdo con la periodicidad definida. • Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. • Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento de la Oficina de Planeación.
		Los servidores en general deben: • Participar en el diseño de los controles que tienen a cargo. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes. El responsable del proyecto debe: • Realizar la identificación de los riesgos del proyecto. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Segunda Línea de defensa	Oficina de Planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Identificar cambios en el apetito del riesgo en la entidad y presentarlos para su aprobación del CICCI. • Capacitar al grupo de trabajo de cada dependencia para la gestión del riesgo. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología establecida por la entidad. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. • Revisar que el cargue de información en el SIGC esté acorde con lo aprobado por el líder del proceso. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CGDI. • Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SIGC. • Participar en los ejercicios de autoevaluación de eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Identificar cambios en el apetito del riesgo de la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos en el CICCI.

Segunda Línea de defensa	Oficina de Planeación	• Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Coordinar con los líderes de proceso el responsable del reporte de seguimiento a los riesgos, controles y planes de acción, el cual deberá ser enviado a la Oficina de Planeación en los tiempos acordados en la Matriz de Riesgos Institucional de la Lotería de Medellín. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso). • Socializar y publicar el mapa de riesgos institucional. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado y ser incluido en el mapa de riesgo institucional. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa
Segunda Línea de defensa	Secretaria General Subgerencia Comercial Subgerencia Financiera Dirección de Talento Humano Jefe de la TICS Oficina de Planeación Comunicación Organizacional Comité de Contratación Supervisores e Interventores de contratos	• Actualizar la documentación que soporta la estrategia del negocio, • Identificar, valorar, evaluar y gestionar los riesgos de pérdida de continuidad del negocio. • Mantener actualizado y gestionado el Comité de Contratación de la entidad, con el fin de gestionar los riesgos asociados a los contratos. • Los Supervisores e Interventores de los contratos deben de Identificar, valorar, evaluar y gestionar los riesgos de los contratos. • Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando. • Liderar mesas de trabajo para la determinación del análisis de impacto del negocio, documentación de los escenarios de riesgos institucional. • Actualizar, según se requiera, los escenarios de riesgos del negocio y la documentación asociada a la continuidad de negocio bajo su responsabilidad. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad • tener el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo
		• Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.

Tercera Línea de defensa	Oficina Asesora de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. • Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. • Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. • Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. • Recomendar mejoras a la política de operación para la administración del riesgo

LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, a continuación, se transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, que reiterando sigue vigente.

Por otra parte, es de resaltar que la Secretaría de Transparencia, en la actualidad está analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción.

Definición de riesgo de corrupción:

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

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

Los riesgos de corrupción se establecen sobre procesos.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.
Con el fin de facilitar la identificación de 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 siguiente matriz, 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 RIEGO 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

Generalidades acerca de los riesgos de corrupción

- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades del orden nacional, departamental y municipal

- Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo

- **Consolidación:** la oficina de planeación, quien haga sus veces, o a la de dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción

- **Publicación del mapa de riesgos de corrupción:** se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año

  La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción

  Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados

- **Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas

- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción

- **Seguimiento:** el jefe de control interno o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción

Ejemplo: Información anonimizada

N°	Riesgo	Clasificación	Causa	Probabilidad	impacto	Riesgo residual	Opción de manejo	Actividad de control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	

Información anonimizada

Importante:
Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.
Una resolución no puede clasificar la información como clasificada o reservada

En la descripción de los riesgos deben concurrir TODOS los componentes de su definición:
Acción u omisión + uso de poder + desviación de la gestión de lo público + el beneficio privado

Valoración de riesgos

a) Análisis de la probabilidad

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

Criterios para calificar la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	**Posible**	El evento podrá ocurrir en cualquier 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

b) Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Criterios para calificar el impacto en riesgos de corrupción

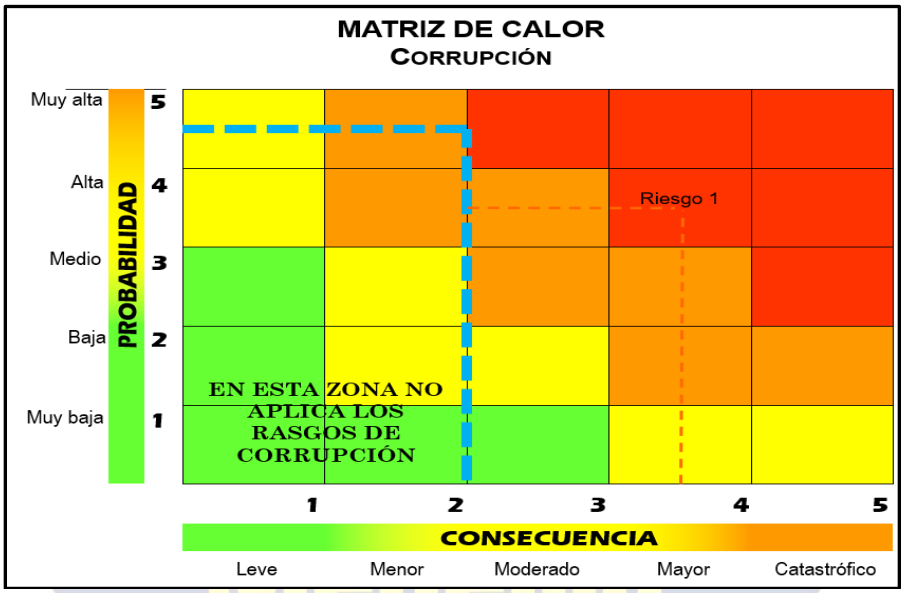
N°	PREGUNTA SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de la misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdidas de recursos económicos?		
7	¿Afectar la generación de los productos o de la prestación de servicios?		
8	¿Dar lugar a detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		
11	¿Dar lugar a los 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 pérdidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿generar daño ambiental?		
	• Responder afirmativamente de UNA a CINCO preguntas genera un impacto **moderado** • Responder afirmativamente de SEIS a ONCE preguntas genera un impacto **mayor** • Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto **catastrófico**		
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTROFICO	Genera consecuencias desastrosas sobre la entidad		

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.

c) Análisis del impacto en riesgos de corrupción

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.

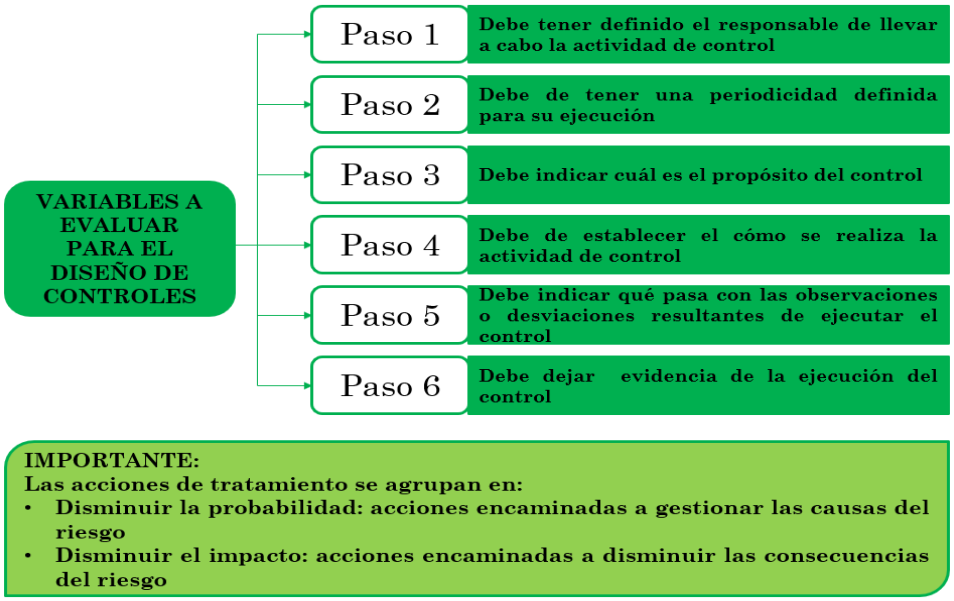
Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente



IMPORTANTE:
Aunque se utiliza el mismo mapa de calor, para los riesgos de gestión y de corrupción, a estos últimos solo les aplican las columnas de impacto Moderado, Mayor y Catastrófico.

Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, tal como se puede apreciar en la siguiente imagen:



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 categorías

Evitar el riesgo: Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y costosa, pero es un obstáculo para el

desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción

Compartir el riesgo: Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

Reducir el riesgo: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Monitoreo de riesgos de corrupción

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento

Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

Seguimiento de riesgos de corrupción

Gestión riesgos de corrupción

- Seguimiento: El jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

- Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

  El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver anexo 6. matriz de seguimiento a los riesgos de corrupción)

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.

- Seguimiento a la gestión del riesgo.

- Revisión de los riesgos y su evolución

Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Acciones para seguir en caso de materialización de riesgos de corrupción

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

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

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

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

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)3, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Identificación de los activos de seguridad de la información

como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Conceptualización activos de información:

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización -Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

Pasos para la identificación de activos

Nota: para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas”.

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión del Talento Humano	Base de datos nomina	Base de datos nomina con información de nómina de la entidad	Directora del Talento Humano	Información	Información reservada	No contiene datos personales	Alta	Alta	Alta	Alta
Gestión Financiera	Aplicativo de nomina	Servidor que contiene el SIGNUS	Subgerente financiero	Software	N/A	N/A	Baja	Medio	Baja	Media
Gestión Financiera	Cuentas de cobro	Formatos de cobro diligenciados	Subgerente financiero	Información	Información pública	No contiene datos personales	Baja	Baja	Baja	Baja

Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

Pérdida de la confidencialidad
Pérdida de la integridad
Pérdida de la disponibilidad

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

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

Ejemplo de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos vulnerables	Ejemplo de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Hurto de medios o documentos	Hurto de medios o documentos
Red	Hurto de medios o documentos	Hurto de medios o documentos
Información	Hurto de medios o documentos	Hurto de medios o documentos
Software	Software	Software
Red	Red	Red

Valoración del riesgo

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, tal como se indica a continuación:

Determinar la probabilidad

Determinar la probabilidad: se entiende como la posibilidad de ocurrencia del riesgo, identificado en la siguiente tabla:

Probabilidad: se identifica la frecuencia en la opción 1 de conocimiento, *"Poco usual, ha ocurrido o puede ocurrir aquí. Es posible que ocurra algunas veces"*, ubicada en el nivel 3

PROBABILIDAD

NIVEL	RANGO	Frecuencia	
		Opción 1 (Conocimiento)	Opción 2 (Actividades)
1	Muy baja	Virtualmente imposible, se acerca a lo imposible. Puede ocurrir solamente en circunstancias excepcionales.	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.
2	Baja	Imaginable pero poco posible, ha ocurrido en otra parte. Podría ocurrir algunas veces.	La actividad que conlleva el riesgo se ejecuta de 3 a 79 veces por año.
3	Media	Poco usual. Ha ocurrido o puede ocurrir aquí. Es posible que ocurra algunas veces.	La actividad que conlleva el riesgo se ejecuta de 80 a 149 veces por año
4	Alta	Muy posible, con gran probabilidad de ocurrencia. Puede ocurrir en la mayoría de las circunstancias	La actividad que conlleva el riesgo se ejecuta mínimo 150 veces al año y máximo 299 veces por año
5	Muy Alta	Muy probable, de alta probabilidad de ocurrencia. Se espera que ocurra en la mayoría de las circunstancias	La actividad que conlleva el riesgo se ejecuta más de 300 veces por año

Determinar el impacto

Determinar el impacto: se entiende como los impactos económicos o reputacionales como variables principales de ocurrencia del riesgo, identificado en la siguiente tabla:

CONSECUENCIA

NIVEL	RANGOS	DESCRIPCIÓN GENERAL	DESCRIPCIÓN	
			AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
1	Leve	Perdidas financieras pequeñas	Menor a 1 SMLMV	De conocimiento **INTERNO** Sin consecuencias
2	Menor	Perdidas financieras medianas	Mayor que 1 SMLMV Menor que 5 SMLMV	De conocimiento **INTERNO** Con consecuencias
3	Moderado	Perdidas financieras altas	Mayor que 5 SMLMV Menor que 50 SMLMV	De conocimiento **EXTERNO** (CLIENTES-REGIONAL) Con consecuencias
4	Mayor	Perdidas financieras importantes	Mayor que 50 SMLMV Menor que 300 SMLMV	De conocimiento **EXTERNO** (SOCIOS DE VALOR-NACIONAL) Con Consecuencias
5	Catastrófico	Perdidas financieras enormes	Mayor que 300 SMLMV	De conocimiento **EXTERNO** (ENTORNO-INTERNACIONAL) Con Consecuencias

Controles asociados a la seguridad de la información

La Lotería de Median podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013 “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Procedimientos operacionales y Responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

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

Junta Directiva

Aníbal Gaviria Correa
Gobernador de Antioquia

Nidia Catalina Naranjo Aguirre
Secretaria de Hacienda Departamental

Daniela Trejo Rojas
Secretaria de Productividad y Competitividad

Ligia Amparo Torres Acevedo
Secretaria de Salud y Protección Social de Antioquia

Pedro Juan González Carvajal
Miembro independiente

Uriel Hernando Sánchez Zuluaga
Miembro independiente

REVISIÓN
Comité Directivo

Viviana Marcela Ríos	Secretaria General (E)
Sergio Andrés Maestre	Sugerente Comercial y de Operaciones (E)
Beatriz Helena Ramírez Gallón	Subgerente Financiera
Esteban Jiménez Acevedo	Jefe de Oficina de Planeación
Camilo Antonio Aristizábal	Jefe Oficina de las TIC (E)
Gloria María Múnera Congote	Directora Talento Humano
Víctor Raúl Jaramillo Pereira	Director de Loterías
Álvaro Martín Villegas Díaz	Director de Operaciones
María Nancy Valencia Correa	Directora de Contabilidad
Diego Alonso Botero Álvarez	Director Auditoría Interna

ELABORACIÓN

Rafael Mariano Maldonado Cuartas