

CONTENIDO

[PRESENTACIÓN 3](#_TOC_250019)

[OBJETIVOS DE LA ADMINISTRACIÓN DEL RIESGO 4](#_TOC_250018)

[GENERAL 4](#_TOC_250017)

[ESPECÍFICOS 4](#_TOC_250016)

[MARCO CONCEPTUAL 5](#_TOC_250015)

[MARCO LEGAL 7](#_TOC_250014)

[CONCEPTOS Y DEFINICIONES 9](#_TOC_250013)

[COMPONENTES DE LA ADMINISTRACIÓN DEL RIESGO 11](#_TOC_250012)

[IDENTIFICACIÓN DEL RIESGO 11](#_TOC_250011)

* Establecimiento del contexto 11
* [Identificación del Riesgo 12](#_TOC_250010)

[VALORACIÓN DEL RIESGO 14](#_TOC_250009)

* [Análisis del Riesgo 14](#_TOC_250008)
* [Evaluación del riesgo 17](#_TOC_250007)
* [Monitoreo y Revisión 22](#_TOC_250006)
* [Seguimiento 23](#_TOC_250005)

[COMUNICACIÓN Y CONSULTA 24](#_TOC_250004)

* [Forma de Divulgación 24](#_TOC_250003)
* [Sitio de consulta 25](#_TOC_250002)

[REFERENCIAS 25](#_TOC_250001)

[CONTROL DE CAMBIOS 25](#_TOC_250000)

INDICE DE TABLAS

Tabla 1. Categorías de Probabilidad de ocurrencias 14

Tabla 2. Niveles de impacto del riesgo 15

Tabla 3. Criterios 16

Tabla 4. Valoración 17

Tabla 5. Zonas de riesgo 17

Tabla 6. Criterios para aplicar controles 20

**INDICE DE ILUSTRACIONES**

Ilustración 1. Matriz de calificación y evaluación del riesgo 18

PRESENTACIÓN

Es necesario para las entidades poder administrar todo tipo de riesgo que pueda afectar el normal desarrollo de las actividades y logro de los objetivos planificados. Es por eso por lo que la Honorable Cámara de Representantes (HCR), en cumplimiento de la Ley 87 de 1993 y en virtud a lo consagrado en el Decreto No. 1599 del 20 de mayo de 2005, la Resolución M.D. No. 0332 del 1 de febrero de 2008 por la cual se adopta el Modelo Estándar de Control Interno MECI 1000:2005, Resolución MD 3064 del 25 de noviembre de 2008, debido a lo cual se implementa el Sistema de Gestión de la Calidad establecido en la norma técnica de calidad para la gestión pública NTCGP 1000:2004 y se establecen responsabilidades para la implementación y mantenimiento de este, se adopta el presente Manual de Riesgos.

De acuerdo con la segunda dimensión del Modelo integrado de Planeación y Gestión (MIPG) y como se demuestra en la gráfica que se relaciona a continuación, las organizaciones deben implementar una cultura organizacional sólida basada en la información, la evaluación, el control, para la toma de decisiones y la mejora continua y definir de esta manera la ruta estratégica que servirá de base para su gestión institucional. Por lo anterior la HCR actualiza su manual de Riesgos tomando como base los lineamientos dados por el Departamento Administrativo de la Función Pública (DAFP).



OBJETIVOS DE LA ADMINISTRACIÓN DEL RIESGO

**GENERAL**

Fortalecer en la Honorable Cámara de Representantes-HCR la implementación y desarrollo de la política de la administración del riesgo a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de las metas y objetivos de la institución, a la vez que facilite la toma de decisiones organizacional y logre prevenir las posibles amenazas que puedan afectar la operación de los procesos y reducir el nivel de los daños.

**ESPECÍFICOS**

* Establecer un manual para gestionar las diferentes etapas del sistema de gestión de riesgos.
* Generar en la estructura organizacional de la HCR una visión sistémica acerca de la administración y evaluación de riesgos, consolidado en un Ambiente de Control adecuado a la Corporación y un Direccionamiento Estratégico que fije la orientación clara y planeada de la gestión dando las bases para el adecuado desarrollo de las Actividades de Control y asegurar su sostenibilidad.
* Proteger los recursos de la organización y asegurar el cumplimiento de normas, leyes y regulaciones, resguardándolos contra la materialización de los riesgos.
* Introducir dentro de los procesos y procedimientos las acciones de mitigación resultado de la administración del riesgo.
* Involucrar y comprometer a todas las dependencias de la HCR en la búsqueda de acciones orientadas a prevenir y administrar los riesgos permitiéndole fortalecer su gestión y desarrollo misional.
* Fomentar en la institución una actitud preventiva, encaminada a la administración de los riesgos.

MARCO CONCEPTUAL

La Administración Pública al ocuparse de los fenómenos de organización y gestión, no puede ser ajena a las herramientas disponibles y a las nuevas tendencias en administración, para lo cual requiere estar en constante actualización y estar abierta al cambio y a la aplicación de diferentes instrumentos que le permitan a las entidades ser cada vez más eficientes, por lo que se hace necesario tener en cuenta todos aquellos hechos o factores que puedan afectar en un momento determinado el cumplimiento de los objetivos institucionales.

Por lo anterior, se hace necesario introducir el concepto de la Administración del Riesgo en las entidades, teniendo en cuenta que todas las organizaciones independientemente de su naturaleza, tamaño y razón de ser están permanentemente expuestas a diferentes riesgos o eventos que pueden poner en peligro su existencia. Desde la perspectiva del control, se toma como referencia el modelo internacional de Control Interno: COSO; el cual, interpreta que la eficiencia del control es la reducción de los riesgos, es decir: el propósito principal del control es la eliminación o reducción de estos propendiendo porque el proceso y sus controles garanticen, de manera razonable que los riesgos están minimizados o se están reduciendo y, por lo tanto, los objetivos de la organización serán alcanzados.

La gestión de riesgos es esencial para anticiparnos a los desafíos, aprovechar oportunidades y garantizar la sostenibilidad de la HCR. Nos permite tomar decisiones informadas y promover una cultura de mejora continua. Así mismo, la gestión de riesgos nos ayuda a proteger y potenciar el cumplimiento de estos objetivos.

MARCO LEGAL

* Ley 87 de 1993: Se describen los aspectos esenciales de la Ley 87 de 1993 que establece la obligación de implementar sistemas de control interno y gestión de riesgos en las entidades públicas.
* Decreto No. 1599 de 2005: Se explica cómo este decreto establece los lineamientos para la implementación de la Ley 87 de 1993 en las entidades estatales.
* Resolución M.D. No. 0332 de 2008: Se detallan los requisitos de la Resolución M.D. No. 0332 de 2008 en relación con la implementación del Sistema de Gestión de la Calidad y la gestión de riesgos
* Resolución MD 3064 de 2008: Se abordan los requisitos y lineamientos establecidos en la Resolución MD 3064 de 2008 relacionados con el Sistema de Gestión de la Calidad y la gestión de riesgos.
* Norma Técnica de Calidad NTCGP 1000:2004: Se destaca cómo esta norma establece los criterios para la implementación de sistemas de gestión de calidad en las entidades públicas, incluyendo la gestión de riesgos.
* Modelo Integrado de Planeación y Gestión (MIPG): Se explica la importancia de la segunda dimensión del MIPG en la gestión de riesgos y su alineación con las normativas mencionadas.

CONCEPTOS Y DEFINICIONES

El mapa de riesgos es una herramienta de gestión que permite a la corporación visualizar en forma de matriz los posibles riesgos que se puedan presentar en el desarrollo misional y administrativo es decir en los diferentes procesos.

En cada proceso de la corporación se aplicarán las matrices de riesgos (gestión, digital y de Corrupción) según sea el caso con el fin de evaluar el desarrollo de la gestión de esta y siempre en búsqueda de realizar un mejoramiento continuo eficaz y productivo.

El mapa de calor es una herramienta que le permite visualizar de una manera gráfica la probabilidad y el impacto generado por los riesgos implementados en cada proceso.

**DEFINICIONES**

**RIESGO:** Se define el riesgo como la posibilidad de que eventos inciertos afecten negativamente los objetivos institucionales.

**RELACIÓN ENTRE RIESGO Y CONTROL INTERNO:** Se explica cómo la gestión de riesgos es una parte integral del control interno, contribuyendo a la eficiencia, efectividad y cumplimiento de los objetivos.

**COMPONENTES DEL SISTEMA DE GESTIÓN DE RIESGOS:** Se presentan los elementos clave de la gestión de riesgos, incluyendo la identificación, evaluación, tratamiento y monitoreo.

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

**DESCRIPCION:** Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

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

**POSIBLES CONSECUENCIAS:** Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros.

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

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

**RIESGO RESIDUAL:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

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

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

**CONFIDENCIALIDAD:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

**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.

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

**CONTROLES EXISTENTES:** Referido a las actividades o sistemas de control establecidos por la dependencia previendo la ocurrencia del riesgo.

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

**APETITO AL RIESGO:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.1

1 Definiciones tomadas de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, v4

COMPONENTES DE LA ADMINISTRACIÓN DEL RIESGO

IDENTIFICACIÓN DEL RIESGO

Cada líder de proceso o persona delegada deberá identificar y comprender los posibles riesgos que podrían afectar a la organización (Gestión, digital y corrupción). Esto se logra a través de la evaluación de factores internos y externos que podrían generar situaciones de riesgo.

CONTEXTO INTERNO:

El contexto interno se refiere a los factores y elementos dentro de la organización que pueden influir en su capacidad para alcanzar sus objetivos y gestionar riesgos. Algunos aspectos para considerar en el contexto interno incluyen:

* Estructura organizativa: La forma en que la organización está organizada, sus departamentos, jerarquías y procesos internos pueden influir en cómo los riesgos se gestionan y comunican.
* Cultura organizacional: La cultura y los valores de la organización pueden influir en cómo se abordan los riesgos. Una cultura de apertura y responsabilidad tiende a facilitar la identificación y comunicación de riesgos.
* Recursos humanos: Las habilidades, competencias y actitudes de los empleados pueden influir en la capacidad de la organización para reconocer y gestionar riesgos.
* Políticas y procedimientos: Las políticas internas y los procedimientos operativos establecidos pueden afectar la identificación y manejo de riesgos, ya que definen cómo se toman decisiones y se ejecutan actividades.
* Tecnología y sistemas: Los sistemas de información y las tecnologías utilizadas en la organización pueden ser fuentes de riesgos y oportunidades, como ciberataques o avances tecnológicos.
* Infraestructura y activos: Los activos físicos de la organización, como edificios, equipos y vehículos, también pueden estar expuestos a riesgos que deben ser considerados.

CONTEXTO EXTERNO:

* El contexto externo se refiere a los factores y elementos fuera de la organización que pueden afectar sus objetivos y operaciones. A continuación, se detallan aspectos a considerar en el contexto externo:
* Economía: Las condiciones económicas, como recesiones o cambios en las tasas de interés, pueden influir en la demanda de productos o servicios de la organización.
* Competencia: La actividad de competidores en el mercado puede presentar riesgos en términos de pérdida de cuota de mercado, cambios en las preferencias de los clientes, etc.
* Marco legal y regulador: Cambios en leyes y regulaciones pueden introducir nuevos riesgos o requerimientos de cumplimiento que la organización debe abordar.
* Tendencias del mercado: Las tendencias en el mercado, como cambios en el comportamiento del consumidor o avances tecnológicos, pueden crear riesgos u oportunidades.
* Factores sociopolíticos: Eventos políticos, sociales o culturales pueden tener un impacto en la organización y generar riesgos.
* Entorno natural: Los desastres naturales, el cambio climático y otros eventos relacionados con el medio ambiente pueden representar riesgos para la organización.

Al considerar tanto el contexto interno como el externo, la organización puede obtener una comprensión completa de los riesgos potenciales a los que está expuesta y tomar medidas adecuadas para su identificación y gestión.

**CONTEXTO DEL PROCESO:**

Para desarrollar el contexto del proceso en la corporación se tendrá en cuenta como fuente principal las características esenciales evidenciadas en la caracterización del proceso debido a que encontraremos la interrelación de procedimientos, objetivos, alcance, responsables entre otros.

**CONTEXTO DE SEGURIDAD DIGITAL:**

El contexto de seguridad digital es fundamental para la identificación de riesgos en el ámbito de la seguridad cibernética y de la información. Al considerar el contexto en el que una organización opera en términos de tecnología, sistemas, amenazas y activos digitales, se pueden identificar mejor los riesgos potenciales que podrían afectar la seguridad digital. Aquí hay algunos aspectos clave del contexto de seguridad digital que influyen en la identificación de riesgos:

* Infraestructura tecnológica: Evaluar la infraestructura tecnológica de la organización, que incluye redes, servidores, dispositivos y sistemas, ayuda a identificar las posibles vulnerabilidades y puntos débiles que podrían ser explotados por ciberatacantes.
* Sistemas críticos: Identificar los sistemas y activos digitales que son críticos para las operaciones de la organización es esencial. Un ataque exitoso contra estos sistemas podría tener un impacto significativo en la continuidad del negocio.
* Datos sensibles: Reconocer qué tipos de datos sensibles maneja la organización y dónde se almacenan es clave para identificar riesgos relacionados con la protección y privacidad de esos datos.
* Amenazas y vulnerabilidades: Analizar las amenazas cibernéticas actuales y emergentes, así como las vulnerabilidades conocidas en la infraestructura y los sistemas, permite anticipar posibles escenarios de ataque y riesgos.
* Actividades de terceros: Considerar las interacciones con terceros y proveedores digitales es importante para identificar riesgos asociados con compartir datos o sistemas con entidades externas.
* Regulaciones y cumplimiento: Las leyes y regulaciones aplicables al contexto de seguridad digital también pueden identificar riesgos potenciales si la organización no cumple con los requisitos de seguridad y privacidad.
* Historial de incidentes: Revisar incidentes de seguridad anteriores que la organización haya enfrentado puede proporcionar información valiosa sobre los tipos de riesgos a los que está expuesta y cómo podrían manifestarse en el futuro.
* Cultura y conciencia: Evaluar la cultura de seguridad y la conciencia de los empleados sobre las mejores prácticas de seguridad digital ayuda a identificar riesgos relacionados con posibles negligencias o comportamientos inseguros.
* Evolución tecnológica: Considerar cómo las nuevas tecnologías y tendencias, como la adopción de la nube, el Internet de las cosas (IoT) y la inteligencia artificial, pueden introducir nuevos riesgos o amplificar los existentes.
* Escenario competitivo: Analizar el panorama competitivo puede ayudar a identificar riesgos relacionados con la posibilidad de ciberespionaje, robo de propiedad intelectual u otras amenazas dirigidas por competidores.
* En resumen, al evaluar estos aspectos del contexto de seguridad digital, una organización puede identificar los riesgos potenciales de manera más efectiva y tomar medidas proactivas para mitigarlos. Esto es esencial para mantener la integridad de la seguridad digital y proteger los activos digitales de la organización.
* Identificación del Riesgo

Para determinar las diferentes causas que puede ocasionar el riesgo identificado se tomara como base el desarrollo del contexto (interno, externo, del proceso y de seguridad digital) realizado en el ítem anterior. Debemos preguntarnos **¿QUÉ PUEDE SUCEDER?,**

¿CÓMO PUEDE SUCEDER?, ¿CUÁNDO PUEDE SUCEDER? Y ¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

* Clasificación de los Riesgos

Las entidades públicas enfrentan una variedad de riesgos en su funcionamiento. Estos riesgos pueden ser categorizados de diferentes maneras según su naturaleza y origen. A continuación, se clasifican los riesgos:

* RIESGO ESTRATEGICO: Se asocia con la forma en que se administra la HCR, relacionados con decisiones estratégicas, cambios en el mercado, competidores y factores macroeconómicos, afines con la misión y el cumplimiento de los objetivos estratégicos y las acciones concretas. También se asocia con las dificultades para llevar a cabo la estrategia planificada de la institución.
* RIESGO OPERATIVO: Son los relacionados con problemas en los procesos internos, tecnológicos, de recursos humanos y legales. Comprende los riegos relacionados tanto con la parte operativa como técnica de la dependencia, incluye riesgos provenientes de las deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
* RIESGOS DE CONTROL: Están directamente relacionados con inadecuados o inexistentes puntos de control y en otros casos, con puntos de control obsoleto, inoperante y poco efectivo. Pueden ser mitigados o eliminados mediante acciones y medidas específicas.
* RIESGOS FINANCIEROS: Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. Así mismo, también se relacionan con fluctuaciones en los mercados financieros, tasas de interés, tipos de cambio, entre otros. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas depende en gran parte del éxito o fracaso de la HCR.
* RIESGOS DE CUMPLIMIENTO: Se asocian con la capacidad de la entidad de cumplir con los requisitos de regulaciones, leyes, estándares, contractuales, de ética y en general con su compromiso con la comunidad.
* RIESGOS DE TECNOLOGIA: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporten el cumplimiento de la misión.
* RIESGOS GERENCIALES: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
* RIESGO DE IMAGEN O REPUTACIONAL: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
* RIESGOS DE CORRUPCIÓN: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
* RIESGOS DE SEGURIDAD DIGITAL: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

En la cámara de representantes se han identificado principalmente 3 tipos de riesgos los cuales son: Riesgos de Gestión, Riesgos de corrupción y Riesgos digitales sin embargo la corporación está en disposición de incluir otro tipo de riesgo si fuese el caso.

VALORACIÓN DEL RIESGO

El líder de cada proceso o persona delegada debe establecer la probabilidad de ocurrencia del riesgo determinado y las posibles consecuencias o impactos que pueden generar en la corporación la materialización de este.

* Análisis del Riesgo

**PROBABILIDAD DE OCURRENCIA:**

La probabilidad de ocurrencia es uno de los componentes clave en la valoración de riesgos y se refiere a la posibilidad de que un riesgo identificado se materialice. Para determinar la probabilidad de ocurrencia del riesgo propuesto, se realizará mediante la asignación de 2 criterios, los cuales son la frecuencia y la factibilidad.

En el criterio de frecuencia se tendrá en cuenta el número de veces que este sucede en un periodo de tiempo determinado y en el criterio de factibilidad se analizará los factores tanto internos como externos que puede generar el riesgo, aunque este no se haya materializado.

Se han establecido las siguientes categorías:

|  |  |  |
| --- | --- | --- |
| **CATEGORIAS** | **VALOR**  **NUMERICO** | **DESCRIPCIÓN** |
| RARO | 1 | Nunca se presentaría. |
| IMPROBABLE | 2 | Sería casi que improbable que se presente |
| POSIBLE | 3 | Es muy poco factible que el hecho se presente |
| PROBABLE | 4 | Es factible que el hecho se presente |
| CASI SEGURO | 5 | Es muy factible que el hecho se presente |

Tabla 1. Categorías de Probabilidad de ocurrencias

**IMPACTO O CONSECUENCIAS DEL RIESGO**

Para conocer el impacto o consecuencia que puede ocasionar la materialización del riesgo propuesto, tendremos en cuenta los diferentes contextos (interno, externo, del proceso y de seguridad digital) desarrollados en el ítem de identificación del riesgo.

Se establecen los siguientes niveles de impacto del riesgo en la corporación:

|  |  |  |
| --- | --- | --- |
| **NIVELES DE**  **IMPACTO** | **VALOR**  **NUMERICO** | **DESCRIPCIÓN** |
| INSIGNIFICANTE | 1 | Sería un hecho que tendrá un manejo adecuado y sería fácil y de forma  pronta su corrección |
| MENOR O LEVE | 2 | Si el hecho llegara a presentarse tendría un bajo impacto con efectos  fácilmente corregibles. |
| MODERADO | 3 | Si el hecho llegare a presentarse tendría un mediano impacto con efectos remediables. |
| MAYOR | 4 | Si el hecho llegara a presentarse tendría impacto medio alto y sería considerado como gravísimo |
| CATASTROFICO | 5 | Si el hecho llegara a presentarse, tendría un alto impacto con efectos a la entidad gravísimos. |

Tabla 2. Niveles de impacto del riesgo

Cabe recordar que al momento de generar el impacto en el Riesgo de Corrupción solo aplicarán el nivel de: moderado, mayor y catastrófico debido a que esta clase de 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.

**NIVEL DE RIESGO**

El nivel del riesgo se determina hallando la probabilidad y el impacto del riesgo propuesto es decir la multiplicación (magnitud) entre el valor asignado a la probabilidad y el valor asignado a el impacto.

|  |  |  |  |
| --- | --- | --- | --- |
| **IMPACTO** |  | **PROBABILIDAD** |  |
| **INSIGNIFICANTE** | 1 | RARO | 1 |
| **MENOR** | 2 | IMPROBABLE | 2 |
| **MODERADO** | 3 | POSIBLE | 3 |
| **MAYOR** | 4 | PROBABLE | 4 |
| **CATASTRÓFICO** | 5 | CASI SEGURO | 5 |

Tabla 3. Criterios

En nivel del riesgo también lo podemos evidenciar en los diferentes mapas de calor asociados a cada uno de los procesos de la corporación como se muestra a continuación:

**REPRESENTACIÓN GRAFICA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **IMPACTO** | | | | |
| INSIGNIFICANTE  1 | MENOR  2 | MODERADO  3 | MAYOR  4 | CATASTRÓFICO  5 |
| **PROBABILIDAD** | RARO  1 |  |  |  |  |  |
| IMPROBABLE  2 |  |  |  |  |  |
| POSIBLE  3 |  |  | **R1** |  |  |
| PROBABLE  4 |  |  |  |  |  |
| CASI SEGURO  5 |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ABREVIATURA** | **ZONA DE RIESGO** | **MEDIDA** |
|  | B | BAJA | Asumir el Riesgo |
|  | M | MODERADA | Asumir el Riesgo, Reducir el Riesgos |
|  | A | ALTA | Reducir el Riesgo, Evitar, Compartir o Trasferir |
|  | E | EXTREMA | Reducir el Riesgo, Evitar, Compartir o Trasferir |

* valuación del riesgo

Para realizar una adecuada evaluación del riesgo lo debemos evaluar antes (riesgo inherente) y después (riesgo residual) de aplicar los controles definidos por cada líder de proceso para atacar las diferentes causas que han generado los riesgos propuestos.

Se establece la siguiente asignación numérica a cada criterio a tener en cuenta para la evaluación y posterior definición de la zona de riesgo en cada proceso.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IMPACTO | | | PROBABILIDAD | |
| INSIGNIFICANTE |  | 1 | RARO | 1 |
| MENOR | 2 | | IMPROBABLE | 2 |
| MODERADO | 3 | | POSIBLE | 3 |
| MAYOR | 4 | | PROBABLE | 4 |
| CATASTRÓFICO | 5 | | CASI SEGURO | 5 |

Tabla 4. Valoración

A continuación, se muestra la matriz definida por la corporación para realizar la respectiva calificación y evaluación de los riesgos a su vez se muestra el significado de cada una de las abreviaturas utilizadas y se definen las zonas de riesgo según su color.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **ABREVIATURA** | **ZONA DE RIESGO** | **MEDIDA** |
|  |  | B | BAJA | Asumir el Riesgo |
|  |  | M | MODERADA | Asumir el Riesgo, Reducir el Riesgos |
|  |  | A | ALTA | Reducir el Riesgo, Evitar, Compartir o Trasferir |
|  |  | E | EXTREMA | Reducir el Riesgo, Evitar, Compartir o Trasferir |

Tabla 5. Zonas de riesgo

**MATRIZ DE CALIFICACIÓN Y EVALUACIÓN**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **IMPACTO** | | | | |
| INSIGNIFICANTE  1 | MENOR  2 | MODERADO  3 | MAYOR  4 | CATASTRÓFICO  5 |
| **PROBABILIDAD** | RARO  1 | **B** | **B** | **M** | **A** | **A** |
| IMPROBABLE  2 | **B** | **B** | **M** | **A** | **E** |
| POSIBLE  3 | **B** | **M** | **A** | **E** | **E** |
| PROBABLE  4 | **M** | **A** | **A** | **E** | **E** |
| CASI SEGURO  5 | **A** | **A** | **E** | **E** | **E** |

Ilustración 1. Matriz de calificacion y evaluación del riesgo

Para realizar la Evaluación del Riesgo se debe tener en cuenta la posición del riesgo es la matriz, según la celda que ocupa, aplicando los siguientes criterios:

**Zona de Riesgo Aceptable:** Probabilidad raro, Impacto insignificante, lo cual permite a la Institución asumir el riesgo.

**Zona de Riesgo Inaceptable:** Probabilidad Alta, Impacto Catastrófico, por tanto, es aconsejable eliminar el factor de riesgo, en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo, controles de protección para disminuir el impacto a compartir o transferir el riesgo.

Cuando el riesgo se sitúe en las **Zonas de Riesgo menor, Moderado o mayor,** se deben tomar medidas para llevar los riesgos a la Zonas Aceptable o Tolerable en lo posible.

**MATRIZ DE CALIFICACIÓN Y EVALUACIÓN**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | **IMPACTO** | | | | |
| INSIGNIFICANTE  1 | MENOR  2 | MODERADO  3 | MAYOR  4 | CATASTRÓFICO  5 |
| **PROBABILIDAD** | RARO  1 | **B** | **B** | **M** | **A** | **A** |
| IMPROBABLE  2 | **B** | **B** | **M** | **A** | **E** |
| POSIBLE  3 | **B** | **M** | **A** | **E** | **E** |
| PROBABLE  4 | **M** | **A** | **A** | **E** | **E** |
| CASI SEGURO  5 | **A** | **A** | **E** | **E** | **E** |

Ilustración 1. Matriz de calificación y evaluación del riesgo

Para realizar la Evaluación del Riesgo se debe tener en cuenta la posición del riesgo es la matriz, según la celda que ocupa, aplicando los siguientes criterios:

**Zona de Riesgo Aceptable:** Probabilidad raro, Impacto insignificante, lo cual permite a la Institución asumir el riesgo.

**Zona de Riesgo Inaceptable:** Probabilidad Alta, Impacto Catastrófico, por tanto, es aconsejable eliminar el factor de riesgo, en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo, controles de protección para disminuir el impacto a compartir o transferir el riesgo.

Cuando el riesgo se sitúe en las **Zonas de Riesgo menor, Moderado o mayor,** se deben tomar medidas para llevar los riesgos a la Zonas Aceptable o Tolerable en lo posible.

Controles

Los controles son medidas implementadas por una institución para mitigar o prevenir los riesgos asociados a sus procesos y procedimientos. Estos controles se pueden clasificar en dos categorías principales: preventivos y correctivos.

* + **Preventivos:** Aquellos que buscan evitar que los riesgos se materialicen y actúan para eliminar las causas que lo originan.
  + **Correctivos:** son los que se implementan en respuesta a un evento de riesgo que ya ha ocurrido; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Es importante que la selección y la implementación de controles sean específicas para la HCR y se adapten a su contexto y necesidades. Cada proceso o procedimiento puede requerir diferentes tipos de controles según la naturaleza de los riesgos asociados.

Para adelantar la evaluación de los controles existentes es necesario describirlos estableciendo si son preventivos o correctivos y responder las siguientes preguntas:

1. ¿Los controles están documentados?
2. ¿Se está aplicando en la actualidad?
3. ¿Es efectivo para minimizar el riesgo?

Una vez ha respondido todas las preguntas proceda a realizar la valoración, así:

* + Calificados y evaluados los riesgos analícelos frente a los controles existentes en cada riesgo.
  + Pondérelos según la tabla establecida, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas (los controles se encuentran documentados, se aplican y son efectivos).
  + Ubique en la Matriz de Calificación, Evaluación y Respuesta a los riesgos, el estado final de riesgo, de acuerdo a los resultados obtenidos en la valoración del mismo.

|  |  |
| --- | --- |
| **CRITERIOS** | **VALORACIÓN DEL RIESGO** |
| **No existen controles** | **Se mantiene el resultado de la evaluación antes**  **de controles** |
| **Los controles existentes no son efectivos** | **Se mantiene el resultado de la evaluación antes**  **de controles** |
| **Los controles existentes son efectivos, pero no están documentados** | **Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el**  **desplazamiento depende de sí el control afecta el impacto o la probabilidad)** |
| **Los controles son efectivos y están**  **documentados.** | **Pasa a escala inferior (el desplazamiento**  **depende de si el control afecta el impacto o la probabilidad)** |

Tabla 6. Criterios para aplicar controles

Estas opciones están basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del Riesgo, a su vez transmite la posición de la alta dirección y establecen las guías de acción necesarias a todos los servidores de la Honorable Cámara de Representantes.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto:

**Evitar el riesgo:** tomar las medidas encaminadas a prevenir la materialización. Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

**Reducir el riesgo:** Implica tomar las medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

**Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

**Asumir el riesgo:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la perdida residual probable y elabora planes de contingencia para su manejo.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. La selección de las acciones más convenientes debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes criterios:

1. La valoración del riesgo
2. EI balance entre la costa de la implementación de cada acción contra el beneficio de la misma.

Para la ejecución de las acciones, se den identificar las dependencias responsables de llevarlas a cabo, definir un cronograma y unos indicadores que permitan verificar el cumplimiento para tomar medidas correctivas cuando sea necesario.

Con la realización de esta etapa se busca encauzar el accionar de la HCR hacia el uso eficiente de los recursos, la continuidad en la prestación de los servicios, la protección de los bienes utilizados para servir la comunidad. Igualmente, se busca que la entidad tenga claridad sobre la política de Administración del Riesgo. Las acciones de manejo de riesgo, y el compromiso de la Dirección y de los servidores de la entidad.

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se procede nuevamente a elaborar el mapa de riesgo residual (después de los controles).

* + Monitoreo y Revisión

El modelo integrado de planeación y gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control permitiéndole a la entidad asegurar que sea capaz de identificar, evaluar y mitigar los riesgos de manera eficiente y efectiva.

Para adelantar este proceso se considera importante señalar los roles de los diferentes actores de acuerdo al Manual de Implementación del MECI 1000:2005.

RESPONSABILIDAD DEL REPRESENTANTE DE LA ALTA DIRECCION

1. Formular, orientar, dirigir y coordinar el proyecto de diseño e implementación del componente de la Administración del Riesgo.
2. Asegurar que se desarrollen a cabalidad cada una de las etapas previstas para el diseño e implementación del Componente de la Administración del Riesgo.
3. Informar a la alta dirección sobre la planificación y avances del proyecto de diseño e implementación del Componente de la Administración del Riesgo.
4. Los líderes y directivos tienen la responsabilidad de establecer la cultura de control interno y son los encargados de las actividades que requiere realizar el Equipo, en armonía y colaboración con los servidores de dichas áreas.
5. Hacer seguimiento a las actividades planeadas para el diseño e implementación del Componente de la Administración del Riesgo, aplicando correctivos donde se requiera.
6. Someter a consideración del Comité de Coordinación de Control Interno las propuestas de diseño e implementación del Componente de la Administración del Riesgo, para su aprobación.

EQUIPO

El Equipo cumplirá los siguientes roles y responsabilidades:

1. Implementación del Componente de la Administración del Riesgo bajo las orientaciones del representante de la dirección.
2. Capacitar ó socializar a los servidores de la entidad en el Modelo y el Componente de la Administración del Riesgo de forma periódica.
3. Prestar apoyo y acompañamiento a las áreas de la entidad en el diseño e implementación del Componente de la Administración del Riesgo.
4. Revisar, analizar y actualizar la información para presentar propuestas de diseño e implementación del Componente de la Administración del Riesgo al representante de la dirección, para su aplicación.
5. Trabajar en coordinación con los servidores designados por área en aquellas actividades requeridas para la promulgación, conocimiento y ejecución de la política de administración del riesgo.
   * Seguimiento

La oficina Coordinadora de Control Interno estará a cargo de realizar periódicamente la verificación sobre el cumplimiento de los controles, acciones implementadas en los diferentes riesgos propuestos en cada uno de los procesos que componen la corporación.

Rol directo: Asesorar y controlar el proceso de actualización de forma periódica en las diferentes áreas de los riesgos institucionales evidenciados y con base en ellos, realizar recomendaciones preventivas y/o correctivas con los responsables de los procesos. Igualmente, la Oficina de Control Interno debe hacer seguimiento a la evolución de los riesgos y al cumplimiento de las acciones propuestas, con el fin de verificar el cumplimiento de las mismas y proponer mejoras.

Rol indirecto: Verificar que en la entidad se lleve a cabo la implementación de la política de la Administración del Riesgo y los mecanismos reales para la Administración del Riesgo.

Así mismo, dentro del rol de asesor asignado a la Oficina de Control Interno, el Decreto 1537 de 2001 en su artículo 4º: “Administración de riesgos”, especifica que la identificación y el análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y dichas oficinas.

Por último, es importante resaltar, que esta herramienta gerencial con lleva al igual que los roles anteriores al ejercicio analítico de la gerencia pública en los asuntos misionales específicos de cada sector, a través de la implementación de mecanismos que permitan visualizar y estar atento a la aparición de nuevos riesgos que se generen por los desarrollos socioeconómicos y tecnológicos.

La gestión de los Riesgos implementados por la corporación será reportada a través de las matrices de riesgos (gestión, digital y de corrupción) desarrolladas con su respectivo avance sobre el tema.

COMUNICACIÓN Y CONSULTA

* + Forma de Divulgación

El levantamiento de información como el desarrollo de las matrices de riesgos (gestión, digital y de corrupción) como el respectivo análisis del mapa de riesgo es un elemento transversal debido a que todos los funcionarios y contratista debe conocer su razón ser y la manera como esta herramienta de gestión se debe usar.

La divulgación del mapa de riesgos empecerá con el compromiso de la alta dirección seguirá a través de cada uno de los líderes de los diferentes procesos y a su vez será

replicada por los jefes de las divisiones hacia todos los funcionarios y contratistas de la Honorable Cámara de Representantes.

* + Sitio de consulta

El presente manual podrá ser consultado en el sitio de web de la HCR, en el Botón de La Cámara / Manuales / Manuales para las partes interesadas externas, así como a nivel interno a través de la intranet u otro medio tecnológico que aplique.

REFERENCIAS

* Manual para la administración del riesgo agosto 2022 –Versión 7

CONTROL DE CAMBIOS

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **FECHA DE**  **APROBACIÓN** | **CAMBIOS** | **REVISÓ** |
| 1 | 18/12/2020 | * Se replantean los objetivos específicos del Manual. * Se reformula el ítem de definiciones y clasificación a conceptos y definiciones. * Se reformula el ítem de Componentes de la administración del riesgo. * Se elimina el ítem de la política de administración del riesgo debido a que los lineamientos se incluirá   en un único documento. | Jefe oficina de Planeación y Sistemas |
| 2 | 31/01/2024 | * Se actualizan conceptos y definiciones * Se reformula el marco conceptual y marco legal * Se reformula el ítem de Componentes de la administración del riesgo. | Jefe oficina de Planeación y Sistemas |