CÁMARA DE REPRESENTANTES

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023.

OFICINA DE PLANEACIÓN Y SISTEMAS
BOGOTÁ, DICIEMBRE DE 2022.

CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

LA CÁMARA Se Transforma

CONTENIDO

1. INTRODUCCIÓN

El entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las mismas organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan las medidas suficientes, tanto en el fortalecimiento de la seguridad, como en la generación de la confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

2. OBJETIVOS

2.1 GENERAL

Describir la metodología para determinar las acciones de tratamiento de *Riesgos de Seguridad y Privacidad de la Información*, identificar, valorar y monitorear los riesgos digitales, de gestión y corrupción, así como las oportunidades de los procesos de la Cámara de Representantes, con el objetivo de prevenir y reducir efectos no deseados, aumentar los efectos deseables y lograr la mejora continua.

2.2 ESPECÍFICOS

- Definir y apropiar la metodología para la *Gestión de los Riesgos de Seguridad Digital* de la Entidad.
- Trabajar el marco metodológico alineado de *Gestión de Riesgos de Seguridad Digital* de acuerdo con el marco estratégico definido por el *Gobierno Nacional en el Modelo de Gestión de Riesgos de Seguridad Digital* y a la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas* y a las mejores prácticas internacionales.
- Apropiar un modelo para identificar, analizar, valorar y tratar los riesgos sobre los activos de información de la Cámara de Representantes.
- Estandarizar el proceso de *Gestión de Riesgos de Seguridad Digital* para los diferentes procesos que soportan la misión de la Entidad.
- Proponer estrategias para la generación de planes de tratamiento de los riesgos que han sido identificados, con el fin de controlarlos a un nivel aceptable por la Entidad.

3. ALCANCE

El presente plan aplica a todos los procesos que conforman el Sistema Integrado de Gestión de la Cámara, inicia con la necesidad de identificar posibles riesgos digitales y oportunidades, sus causas potenciales, continua con el establecimiento de controles y actividades a implementar para evitar la materialización en el caso del riesgo y aumentar los efectos deseables en el caso de las oportunidades y finaliza con el seguimiento y evaluación de la eficacia de las acciones efectuado por la Oficina de Control Interno.

4. MARCO LEGAL

NORMA	AÑO	DESCRIPCIÓN
Decreto 1008	2016	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la Protección de Datos Personales.
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
MSPI	2016	Modelo de Seguridad y Privacidad de la Información establecida en la Guía de Gestión de Activos.
Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, artículo 73.
MGRSD	2018	Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
Guía para la administración del riesgo y el diseño de controles en entidades públicas	2020	Riesgos de Gestión, Corrupción y Seguridad Digital - Versión 5 emitida por el DAFP
ISO 27005	2018	Gestión de Riesgos de la Seguridad la Información
ISO 31000 para la Gestión de Riesgos	2018	La ISO 31000 es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones. ... Esta norma provee de una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.
CONPES 3854	2016	Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.
ISO 27001	2013	Sistema de Gestión de Seguridad de la Información

5. DEFINICIONES

ACEPTAR EL RIESGO: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).

ACTIVIDADES DE CONTROL: Son las acciones establecidas a través de políticas (establecen las líneas generales del control interno.) y procedimientos (son los que llevan dichas políticas a la práctica.) que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

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

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

COMPARTIR EL RIESGO: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad.

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.

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

CONTROL PREVENTIVO: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

CONTROL DETECTIVO: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

EVITAR EL RIESGO: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

GESTIÓN DE RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de sus objetivos.

IMPACTO: Son las consecuencias o efectos que puede ocasionar a la organización la materialización del riesgo.

MAPA DE RIESGO: Documento con la información resultante de la gestión del riesgo.

MONITOREAR: comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.

OPORTUNIDAD: Efecto Potencial Beneficioso.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del Riesgo NTC ISO 31000, La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

PROBABILIDAD: Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia (Número de eventos en un periodo determinado) o Factibilidad (Se analiza la presencia de factores internos y externos que pueden propiciar el riesgo).

REDUCIR EL RIESGO: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

RIESGO DE GESTIÓN: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
RIESGO DE CORRUPCIÓN: Posibilidad de que por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado.

RIESGO DE SEGURIDAD DIGITAL: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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

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

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

RESPONSABLES:

Línea Estratégica: Alta Dirección, Coordinación de Control Interno

Primera Línea Defensa: Jefes de Planeación, Líderes de procesos, programas y proyectos

Segunda Línea Defensa: Supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión

Tercera Línea Defensa: Oficina de Control Interno

RESPONSABILIDADES

Las responsabilidades se encuentran determinadas de acuerdo al Modelo de Líneas de Defensa descritas estas según la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública, las cuales se hacen parte del establecimiento de la Política de Administración de Riesgos aprobada por el Comité Institucional de Coordinación de Control Interno de la Entidad.

La Oficina de Planeación y Sistemas asesorará a la primera línea de defensa (líderes de procesos) y acompañará a la Segunda Línea de Defensa en la identificación, construcción del Mapa de Riesgos, y monitoreo de los riesgos de seguridad digital y en las recomendaciones de establecimiento de controles para mitigar estos riesgos.

Los líderes de procesos (Primera Línea de Defensa) es el responsable de identificar y documentar el contexto estratégico, los Riesgos, sus indicadores, establecer los controles, actividades de control, nivel y tratamiento del Riesgo de acuerdo al objetivo del proceso y de los objetivos de sus planes y proyectos que derivan de la gestión del proceso y reporta oportunamente a la Segunda Línea de Defensa de la gestión de riesgos realizada, la materialización de riesgos, o los cambios que generen nuevos riesgos o controles a los existentes finalmente atiende el seguimiento y evaluación de la tercera línea de defensa, propendiendo por la mejora continua del proceso.

La Oficina Asesora de Planeación realizará la consolidación del Mapa de Riesgos y liderará la Gestión de los Riesgos de la Entidad hasta su monitoreo, reportando a la tercera línea de Defensa (Oficina de Control Interno).

La Oficina de Control Interno es la encargada del seguimiento y evaluación independiente de la Gestión de los Riesgos de la Entidad y realizará Auditorías a partir de los Riesgos.

6. GENERALIDADES

La administración de riesgos busca que la Corporación a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos asociados a los procesos minimice perdidas y maximice oportunidades, es por esto, que la administración de los riesgos, se convierte en una herramienta fundamental para la Cámara de Representantes, debido a que su correcta aplicación tiene como resultado evitar la ocurrencia de hechos o situaciones que afecten la gestión de la entidad y el cumplimiento de sus objetivos institucionales.

Es responsabilidad de los líderes de los procesos identificar y documentar los riesgos, sin importar la fuente de información (contexto estratégico, indicadores, resultados de auditoría, quejas, observación directa, entre otros), para ello contará con la asesoría de la Oficina de Planeación y Sistemas de la Entidad.

6.1 IDENTIFICACIÓN DE RIESGOS

6.1.1 ESTABLECIMIENTO DEL CONTEXTO

Al establecer el **Contexto Interno** se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos, se pueden considerar factores como la estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y conocimientos con que se cuenta (económicos, personas, procesos, sistemas, tecnología, información), relaciones con las partes involucradas, cultura organizacional.

Debe considerarse la gestión del cambio y realizar las actualizaciones que requiera el contexto revisándolo por lo menos una vez al año.
El contexto Interno se establece a partir del establecimiento del contexto externo y del contexto del proceso los cuales determinan los siguientes factores:

Establecimiento del: CONTEXTO EXTERNO	**Establecimiento del: CONTEXTO DEL PROCESO**
Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar los Factores PESTAL:	Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar Factores como: - Objetivo del proceso

- **P**olíticos - **E**conómicos y financieros - **S**ociales y culturales - **T**ecnológicos - **A**mbientales - **L**egales y reglamentarios	- Alcance del proceso - Interrelación con otros procesos - Procedimientos asociados al proceso - Responsables del proceso - Activos de seguridad digital del proceso - Quejas o denuncias de corrupción asociadas a la ejecución del proceso.

CONTEXTO	FACTORES DE CONTEXTO
EXTERNO	- **Políticos**: Cambios de gobierno, legislación y políticas públicas. - **Económicos y financieros**: Disponibilidad de recursos. - **Sociales y Culturales:** Demografía, responsabilidad social, orden público. - **Tecnológicos**: Avances en tecnología, acceso a sistemas de información externos, gobierno digital. - **Ambientales:** Emisiones y residuos, energía, catástrofes naturales. - **Legales y reglamentarios:** Leyes, decretos, ordenanzas y acuerdos.
INTERNO	- **Financieros:** Presupuesto de funcionamiento y recursos de inversión. - **Personal:** Competencia y disponibilidad del personal, seguridad y salud ocupacional. - **Procesos:** Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. - **Tecnología:** Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. - **Estratégicos:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. - **Comunicación Interna:** Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
DEL PROCESO	- **Diseño del proceso:** Claridad en la descripción del alcance y objetivo del proceso. - **Interacciones con otros procesos:** Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. - **Transversalidad:** Procesos que determinan lineamientos

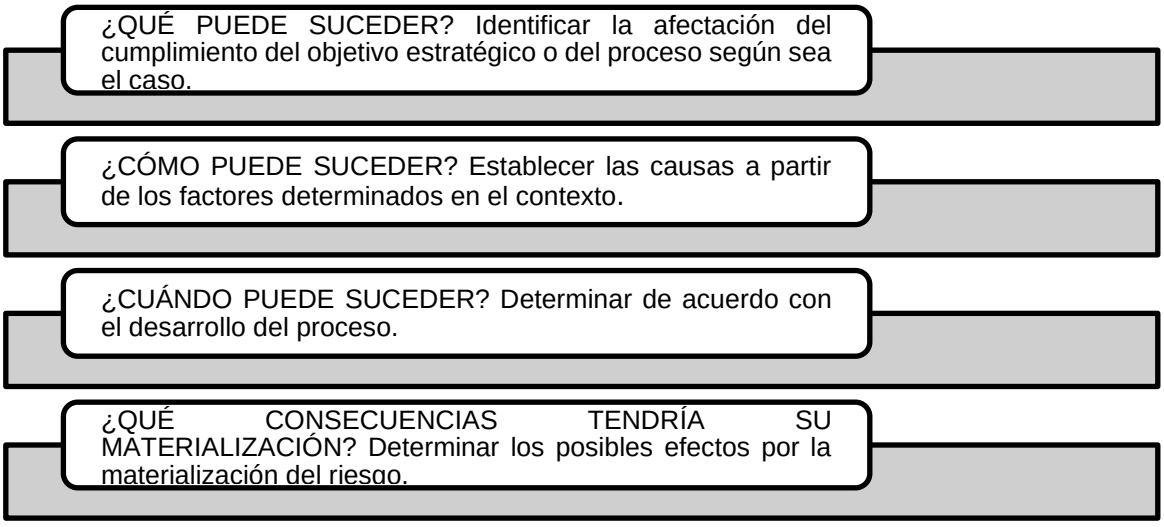
	necesarios para el desarrollo de todos los procesos de la entidad. - **Procedimientos asociados:** Pertinencia en los procedimientos que desarrollan los procesos**.** - **Responsables del proceso:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso. - Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos. - **Activos de seguridad digital del proceso:** Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

6.1.2 IDENTIFICACIÓN Y REDACCIÓN DE RIESGOS

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Las preguntas claves para la identificación del riesgo permiten determinar:



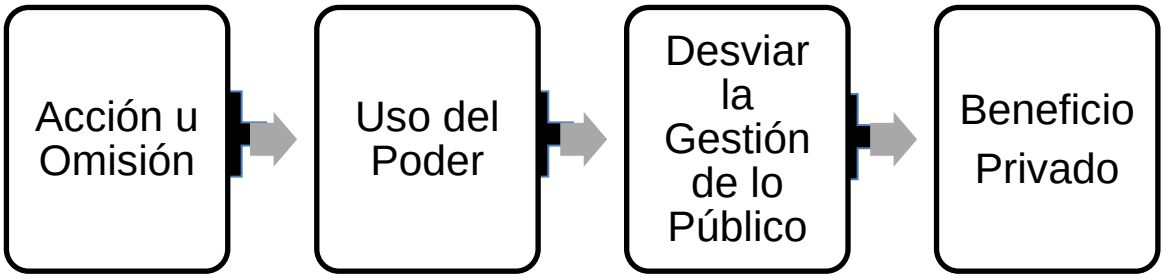
NOTA: Al redactar el Riesgo se debe evitar iniciar con palabras negativas como: **"NO"**, **"Que no"**, o con palabras que denoten un factor de riesgo evitando utilizar palabras como: "**Ausencia de", "falta de", "poco", escaso", "insuficiente", "deficiente", "debilidades en".**

El Riesgo debe generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo.

Riesgos de Corrupción:

Los Riesgos de Corrupción se establecen sobre PROCESOS, su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

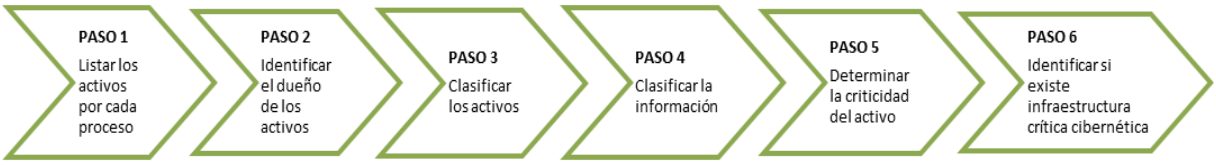
El Riesgo de Corrupción debe cumplir los siguientes componentes para que no se genere confusión con los Riesgos de Gestión, estos componentes son los aspectos diferenciadores que le dan sentido al Riesgo para que sea identificado por Corrupción:



Seguridad Digital- IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Todo lo que no está plenamente identificado no está debidamente asegurado, los líderes de procesos con el lineamiento de la Oficina de Planeación y Sistemas de la Cámara de Representantes, identifican los activos de información de su proceso, como contexto a partir del cual se identifican los riesgos de Seguridad Digital, así:

Análisis de los Objetivos Estratégicos:	Análisis de los Objetivos del Proceso:
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicativos de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.	De esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así 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.



6.1.3 TIPOLOGÍA DE RIESGOS

TIPO RIESGO	DESCRIPCIÓN
ESTRATÉGICOS	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
GERENCIALES	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
OPERATIVOS	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
FINANCIEROS	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
TECNOLÓGICOS	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
DE CUMPLIMIENTO	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
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.
DE CORRUPCIÓN	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
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.

6.2 VALORACIÓN DE RIESGOS

Valoración del Riesgo = Probabilidad X Impacto

6.2.1 ANÁLISIS DE RIESGOS

PROBABILIDAD

Probabilidad= Frecuencia X Factibilidad

Al buscar establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial o riesgo inherente, se debe empezar **analizando las causas**: Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por lo tanto **se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito**; estos factores se deben tener en cuenta al identificar las causas que originan la materialización de los riesgos.

Para analizar las causas, el líder del proceso y sus colaboradores cuentan con herramientas como: Análisis de Debilidades, Oportunidades, Fortalezas y Amenazas (DOFA), Diagrama de Pareto, 5 porqué o 3 porqué, Matriz de priorización, Análisis de causa raíz RCA, Espina de pescado, Tormenta de ideas, Análisis de árbol de fallos, Análisis de causa y efecto, Análisis de árbol de eventos, Análisis qué pasa si, Árboles de decisión, Análisis de modo y efecto de la falla, Delphi.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años.

IMPACTO

El impacto, son las consecuencias que ocasiona a la organización la materialización del riesgo, incluyendo sus potenciales consecuencias.

Para los Riesgos de Gestión y Seguridad Digital el impacto se mide en cinco (5) niveles a saber: Insignificante, Menor, Moderado, Mayor y Catastrófico.

Criterios para calificar el IMPACTO de los RIESGOS DE GESTIÓN

NIVEL	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO

CATASTRÓFICO 5	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR 4	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación.
MODERADO 3	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance

	terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR 2	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE 1	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

	- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	

Criterios para calificar el IMPACTO de los RIESGOS DE CORRUPCIÓN

Para los Riesgos de Corrupción los niveles de impacto son tan solo tres (3): Moderado, Mayor y Catastrófico, porque los Riesgos de Corrupción **SIEMPRE SON SIGNIFICATIVOS** en el impacto para la entidad, por eso NUNCA se pueden ASUMIR NI TOLERAR, y su impacto se califica a través de una Encuesta de Criterios.

Para calificar el **impacto** a los **riesgos de corrupción** **se debe partir del caso hipotético de la materialización del riesgo**, mediante el siguiente formato:

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA SI	RESPUESTA 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 misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		

9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de **UNA a CINCO** pregunta (s) genera un impacto **MODERADO** Responder afirmativamente de **SEIS a ONCE** pregunta (s) genera un impacto **MAYOR** Responder afirmativamente de **DOCE a DIECINUEVE** pregunta (s) genera un impacto **CATASTRÓFICO**			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Fuente: Secretaría de Transparencia de la Presidencia de la República

6.2.2 NIVEL DE RIESGO

Nivel de Riesgo Inherente:

Para definir el nivel del riesgo, se inicia ubicando la valoración de la probabilidad (Rara vez, Improbable, Posible, Probable ó Casi seguro). Posteriormente se determina el impacto en las columnas correspondientes (Insignificante, Menor, Moderado, Mayor ó Catastrófico).

Finalmente, se define el punto de intersección de las dos; que corresponderá al nivel de riesgo – INHERENTE (Antes de Controles).

Casi seguro 5							**Extremo**
Probable 4							**Alto**
Posible 3							**Moderado**
Improbable 2							**Bajo**
Rara vez 1							
	1	2	3	4	5		
	Insignificante	Menor	Moderado	Mayor	Catastrófico		
	IMPACTO						

Nivel de Riesgo Residual:

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

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

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2

fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

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

6.3 DISEÑO DE CONTROLES

Al momento de definir un control para que mitigue de manera adecuada el riesgo, se deben considerar obligatoriamente desde la redacción del mismo, que el control contenga las siguientes seis (6) variables:

VARIABLE	DESCRIPCIÓN
1. RESPONSABLE (QUIÈN)	- Persona asignada para ejecutar el control. - El control debe iniciar con un cargo responsable o un sistema o aplicación (nunca nombres de personas). - Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso (debe tener un remplazo o apoyo, para que así si este responsable quisiera hacer algo indebido, por sí solo, no lo podrá hacer).
2. PERIODICIDAD (CADA CUÀNTO)	- Definir una periodicidad específica para la ejecución del control. - De igual forma hay controles automáticos que son programados para que se ejecuten en un tiempo específico, estos controles también tienen una periodicidad (cada vez que se va a realizar...).

3. PROPÓSITO DEL CONTROL (QUÈ BUSCA)	- El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo. - El propósito debe indicar para qué se realiza y que ese propósito conlleve a prevenir las causas que generan el riesgo.
4. CÒMO SE REALIZA (CÒMO)	- Debemos preguntarnos si la fuente de información es confiable, el control debe indicar cómo se realiza de manera que se pueda evaluar la fuente (a través de.. se toma dicha información directamente de… comparando..) ejemplo listas de chequeo, portal web, base de datos entre otros.
5. QUÈ PASA CON LAS OBSERVACIONES O DESVIACIONES (QUÈ PASARÌA SI..)	- El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control (en caso de…). - Si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen la actividad NO debería continuarse hasta que se subsane la situación.
6. EVIDENCIA (DÓNDE QUEDA)	- Dejar evidencia de la ejecución del control, documento para poder evaluar que el control realmente fue ejecutado de acuerdo a las cinco variables anteriores.

6.4 VALORACIÓN DE LOS CONTROLES

El control si está bien diseñado mitiga el riesgo, al ejecutarlo como fue diseñado mitiga la probabilidad de que el riesgo se materialice o mitiga el impacto del riesgo una vez se materialice.

Para analizar y evaluar el diseño del control de acuerdo con las seis (6) variables establecidas en su diseño, así:

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

Al anterior análisis y evaluación se debe asignar un peso o participación por cada una de las variables de diseño del control para mitigar el riesgo, así:

CRITERIO DE EVALUACIÓN	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del	Adecuado	15

responsable	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

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

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

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

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

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

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

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

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

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE: 100 MODERADO: 50 DÉBIL: 0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
Fuerte: calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte+fuerte=fuerte	**NO**
	Moderado (algunas veces)	Fuerte+moderado=moderado	**SI**
	Débil (no se ejecuta)	Fuerte+débil=débil	**SI**
Moderado: calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado+fuerte=moderado	**SI**
	Moderado (algunas veces)	Moderado+moderado=moderado	**SI**
	Débil (no se ejecuta)	Moderado+débil=débil	**SI**
Débil: calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil+fuerte=débil	**SI**
	Moderado (algunas veces)	Débil+moderado=débil	**SI**
	Débil (no se ejecuta)	Débil+débil=débil	**SI**

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo, mediante el análisis de la Solidez del Conjunto de Controles.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, así:

Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

6.5 ACTIVIDADES DE CONTROL

Son las acciones establecidas a través de políticas (establecen las líneas generales del control interno) y procedimientos (llevan las políticas a la práctica) que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que indicen en el cumplimiento de los objetivos. La actividad de control debe por sí misma mitigar o tratar la causa del riesgo y ejecutarse como parte del día a día de las operaciones.

6.5.1 Controles Preventivos

Están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos. Ejemplo: Revisión al cumplimiento de requisitos contractuales en el proceso de selección del contratista o proveedor.

6.5.2 Controles Detectivos

Controles que están diseñados para identificar un evento o resultado no previsto después que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes. Ejemplo: Realizar una conciliación bancaria para verificar que los saldos en libros correspondan a los saldos de bancos.

6.6 TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la primera línea de defensa (Líderes de Procesos) para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento.

En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo.
El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Gestión por Procesos y **Riesgos de Seguridad Digital**	Baja	Se **ACEPTARÁ** el riesgo, no se adoptará ninguna medida que afecte la probabilidad o el impacto del Riesgo. **NINGÚN RIESGO DE CORRUPCIÓN PODRÁ SER ACEPTADO. (**Esta Zona de Riesgo sólo aplica para Gestión y Seguridad Digital**).**
	Moderada	Se adoptan medidas para **REDUCIR** la probabilidad o el impacto del riesgo o ambos, generalmente conlleva a la implementación de controles.
	Alta y Extrema	*Se adoptan medidas para **REDUCIR** o, *Tomar decisión de **EVITAR** el riesgo mediante la cancelación-abandono de las actividades que dan lugar al riesgo, es decir no iniciar o no continuar con la actividad que lo provoca (No hay riesgos después de tomar medidas de tratamiento) *Si es muy difícil para la entidad reducir el riesgo a un nivel aceptable: **COMPARTIR** el riesgo, reduciendo la probabilidad o el impacto y se transfiere parte del riesgo Ejemplo: Seguros o Tercerización (mecanismos de transferencia del riesgo deben estar formalizados a través de un acuerdo contractual) No se transfiere la responsabilidad, si el riesgo
Riesgos de Corrupción	Moderado	**REDUCIR, EVITAR, COMPARTIR (**No se transfiere la responsabilidad)
	Alta Extrema	**REDUCIR, EVITAR, COMPARTIR (**No se transfiere la responsabilidad)

6.7 Seguimiento y Control

Conforme a lo establecido por el Departamento Administrativo de la Función Pública DAFP y de la Secretaria de Transparencia, y atendiendo a la normatividad vigente aplicable; la periodicidad establecida por la Cámara de Representantes será:

El monitoreo de la segunda línea de defensa y seguimiento y evaluación de la tercera línea de defensa seguimiento al mapa de riesgos de gestión y seguridad digital, será con una periodicidad de corte Semestral, generando las acciones de comunicación y consulta pertinentes.

En la Corporación se hace el tratamiento a los Riesgos de Seguridad Digital, de Gestión y Corrupción mediante tablas de seguimiento, donde se establece el control y el tratamiento al riego residual por procesos.

Para los Riesgos de Riesgos de Corrupción, el monitoreo por parte de la segunda línea de defensa se realizará bimestralmente, y el seguimiento y evaluación por parte de la tercera línea de defensa se realizará cuatrimestralmente, así:

- Primer seguimiento: Con corte al 30 de junio. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de julio.
- Segundo seguimiento: Con corte al 31 de septiembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de octubre.
- 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 o quien haga sus veces, deberá publicar los resultados de tales seguimientos en la página web de la Entidad en la sección: Transparencia y Acceso a la Información Pública, dentro del plazo establecido.

Los líderes de cada proceso en el ejercicio de monitoreo y revisión podrán realizar los ajustes o modificaciones requeridos orientados a la mejora del Mapa de Riesgos de su proceso, para lo cual deberá solicitar a la Oficina de Planeación y Sistemas la actualización del Mapa de Riesgos y esta a su vez debe informar a la Oficina de Control Interno los ajustes realizados, numerando y publicando en página web una nueva versión del mapa dejando la trazabilidad de control de cambios realizado.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

ÍTEM	DESCRIPCIÓN DE LA ACTIVIDAD	ÁREA RESPONSABLE	CARGO RESPONSABLE
1	Diligenciar el Mapa de Riesgos Institucional y los Criterios para calificar Impacto Riesgos de Corrupción teniendo en cuenta los siguientes ítems.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora) - Línea de Defensa.
	IDENTIFICACIÓN DEL RIESGO Y OPORTUNIDAD		
2	Identificar el contexto mediante los factores internos y externos que puedan afectar o favorecer el cumplimiento de los objetivos de los procesos y determinar las causas de los riesgos.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
3	Redactar los riesgos de gestión, seguridad digital y corrupción, así como las oportunidades y establecer los posibles efectos o consecuencias que podrían presentarse una vez se materialice el riesgo.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
	VALORACIÓN DEL RIESGO		
4	Calificar la probabilidad de ocurrencia de cada uno de los riesgos, de acuerdo a lo establecido en las generalidades del presente procedimiento.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
5	Calificar el impacto causado por la eventual ocurrencia de cada riesgo, de acuerdo a lo establecido en las generalidades del presente procedimiento.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
6	Determinar la zona de riesgo inherente de acuerdo lo establecido en las generalidades del presente procedimiento.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).

7	Identificar los controles para prevenir o reducir el impacto de los eventos que ponen en riesgo la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
8	Realizar la evaluación de los controles para posterior calificación del riesgo residual de acuerdo a lo establecido en las generalidades del presente procedimiento.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
9	Determinar la zona de riesgo residual de los Riesgos.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
10	Dependiendo del resultado obtenido en la zona de riesgo residual, determinar la opción del manejo del riesgo (evitar, reducir, compartir y/o trasferir y asumir) en la Matriz de Riesgos de Institucional.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
11	Establecer las acciones para el tratamiento de los riesgos para lograr los efectos deseables de acuerdo al tratamiento de los riesgos por dependencias	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
	MONITOREO Y REVISIÓN		
12	P.C Revisar periódicamente el mapa de riesgos aprobado, revisar las causas que originan los riesgos, revisar que los controles de estos riesgos no se hayan modificado en el tiempo, verificar que no se materialicen los riesgos o los cambios en los factores del contexto permitan la materialización.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
13	Proponer nuevos controles para los que son obsoletos y proponer las modificaciones al mapa de riesgos de	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del

	gestión y corrupción con base al análisis efectuado en el monitoreo y revisión del ítem anterior.		proceso (Grupo de mejora).
14	Remitir a la oficina Asesora de Planeación los ajustes o modificaciones necesarios orientados a mejorar los mapas de riesgos ya sea de gestión o corrupción.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
15	PC: Cumplir con las fechas estipuladas para el tratamiento de los riesgos por cada dependencia	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso (Grupo de mejora).
16	Solicitar a todos los procesos de la Corporación mediante memorando el reporte del mapa de riesgos Institucional de acuerdo a la periodicidad de seguimiento establecida en las generalidades del presente procedimiento.	Oficina de Planeación y Sistemas	Profesionales a cargo
17	Enviar los Reportes a la Oficina de Planeación y Sistemas con la descripción de las acciones ejecutadas, el porcentaje de cumplimiento y la descripción de las evidencias y la valoración del riesgo residual.	Oficina de Planeación y Sistemas	Líder de Proceso (Directivos, Jefes de Oficina), Profesionales del proceso
18	P.C Consolidar, y reportar a la Oficina de Control Interno el mapa de riesgos institucional con el avance de las acciones y controles reportados por cada uno de los procesos para su seguimiento y evaluación.	Oficina de Planeación y Sistemas	Profesionales a cargo
	SEGUIMIENTO		
19	Evaluar la información del Mapa de Riesgos Institucional para verificar el avance, la eficacia de las acciones y controles estableciendo las	Oficina de Control Interno	Profesionales de Control Interno

	observaciones y recomendaciones a que haya lugar.		
20	Publicar el seguimiento y evaluación a los riesgos de corrupción en la página web de la entidad dentro de los diez (10) primeros días hábiles de los meses de mayo, septiembre y enero.	Oficina de Control Interno	Profesionales de Control Interno
21	Asesorar, comunicar y presentar a los procesos de la Corporación luego del seguimiento y evaluación del mapa de riesgos institucional sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.	Oficina de Control Interno	Profesionales de Control Interno

8. CONTROL DE CAMBIOS

REVISIONES DEL DOCUMENTO				
Versión	Fecha	Proyectado por	Descripción	Aprobado por
1.0	08/10/2021	Ing. Carlos Manuel Gómez Damián	Creación del Documento	**Oficina de Planeación y Sistemas** Dr. Juan José Gómez Vélez – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 3 del 16 de Diciembre de 2021.
2.0	15/12/2022	Oficina de Planeación y Sistemas	Ajustes al documento	**Oficina de Planeación y Sistemas** Dr. Andrés Francisco Lozano Campos – Jefe OPS Revisión y ajustes: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2023.