POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU

Contenido

INTRODUCCIÓN 2

1. DECLARACIÓN DE POLÍTICA DE ADMINISTRACIÓN DE RIESGOS 3

1.1 Lineamiento 1: Pensamiento basado en riesgos 3

1.2 Lineamiento 2: Nivel de aceptación del riesgo 4

2. OBJETIVOS 5

2.1 Objetivo General 5

2.2 Objetivos Específicos 5

3. ALCANCE 6

4. TERMINOS Y DEFINICIONES 6

5. METODOLOGÍA 7

6. RESPONSABILIDADES Y ROLES 8

7. PRIORIZACIÓN DE RIESGOS A CONTROLAR 11

7.1 Clases de Riesgos 11

7.1.1 De Corrupción 12

7.1.2 De Seguridad Digital 12

7.2 Identificación del Riesgo 13

7.3 Análisis del riesgo 14

8. NIVELES DE CALIFICACIÓN, PROBABILIDAD E IMPACTO 14

8.1 Probabilidad riesgos de gestión, corrupción, seguridad digital 15

8.2 Impacto riesgos de gestión 15

8.3 Impacto riesgos de corrupción 17

9. NIVEL DE ACEPTACIÓN DEL RIESGO 19

10. EVALUACIÓN DEL RIESGO 20

10.1 Diseño redacción de un control 21

10.2 Análisis y evaluación del diseño del control 22

11. MONITOREO Y REVISIÓN – Rol de las Líneas de Defensa 26

12. COMUNICACIÓN Y CONSULTA. 26

INTRODUCCIÓN

La Política de Administración del riesgo es la expresión del compromiso de la Alta Dirección de la Empresa para la Seguridad y Soluciones Urbanas – ESU, frente a la identificación, tratamiento y control de los riesgos y oportunidades, que influencian los resultados de la gestión y permiten el cumplimiento de su misión institucional, de las metas establecidas en el Plan de Acción Institucional y en los procesos de la Entidad.

La cual involucra mediante un ámbito estratégico y tres líneas de defensa, a todos los servidores públicos y los trabajadores oficiales de la entidad, soportándose en los mecanismos de comunicación disponibles y cubriendo todas las responsabilidades institucionales, las de cada proceso y las propias de cada funcionario. Los niveles de aceptación de riesgo, los ciclos de establecimiento y seguimiento, los niveles de calificación, la identificación de riesgos estratégicos, operacionales, de corrupción y los de contratación, entre otros, hacen parte fundamental del lenguaje y herramientas disponibles para la administración de riesgos.

Esta política pretende direccionar e influenciar la cultura organizacional, en función del pensamiento basado en riesgos. Esta forma de gestionar representa una herramienta de gran utilidad para anticiparse y contribuir a “Hacer que las cosas pasen, y que pasen bien”; teniendo en cuenta que los riesgos son posibilidades de ocurrencia de situaciones que pueda afectar el normal desarrollo de las actividades de los procesos e impidan el logro de los objetivos estratégicos para el cumplimiento de la misión institucional.

Para dar continuidad a las políticas de administración de riesgos, se hace necesario definir criterios orientadores respecto al tratamiento de los riesgos identificados a fin de mitigar sus efectos en la Entidad, siendo éste el objetivo de la presente política, con la cual se pretende en primera instancia establecer desde la alta dirección la forma de abordar la gestión de los riesgos institucionales, unificando con los servidores públicos y los trabajadores oficiales de la Entidad un lenguaje común sobre el tema, así como el establecimiento de criterios que permitan la sostenibilidad de la administración del riesgo.

1. DECLARACIÓN DE POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

la Empresa para la Seguridad y Soluciones Urbanas – ESU, conforme a su misión, establece que la administración de riesgos asociados a los procesos de la Entidad, tendrá un carácter prioritario y estratégico, fundamentada en el modelo de operación por Procesos, teniendo en cuenta el contexto estratégico de la entidad, la normatividad vigente aplicable y el Modelo Integrado de Planeación y Gestión-MIPG, En virtud de lo anterior, la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos se circunscribirá a los objetivos de los planes institucionales, de los procesos, de los proyectos y a las acciones ejecutadas por los servidores públicos, los trabajadores oficiales y particulares que ejercen funciones públicas, durante el ejercicio de sus funciones y actividades, teniendo en cuenta los siguientes lineamientos:

1.1 Lineamiento 1: Pensamiento basado en riesgos

Para todo el Sistema Integrado de Gestión de la Empresa para la Seguridad y Soluciones Urbanas – ESU – SIG y su modelo de operación por procesos, el pensamiento basado en riesgos debe ser la herramienta funcional para el desarrollo de la planeación, el control, la evaluación y la mejora.

Directrices:

Primera línea de defensa, los directivos deben fortalecer la cultura de gestión de riesgos en el ámbito institucional, bajo un enfoque estratégico, revisando las necesidades de adaptación al cambio y definiendo o actualizando la política de Administración del Riesgo. Los responsables de procesos, programas y proyectos, deben gestionar los riesgos a partir del plan de tratamientos definido, y su respectivo seguimiento durante la ejecución de las actividades de control, así como la comunicación de los resultados obtenidos y generación de alertas tempranas. Los Directivos se comprometen a fomentar un clima y unos escenarios de trabajo, que favorezcan el análisis de los riesgos, la implementación de controles y la generación de acciones para realizar el tratamiento de riesgos y la gestión de oportunidades, que faciliten su mitigación u optimización.

Segunda línea de defensa, todos los servidores públicos y los trabajadores oficiales que tengan rol o funciones de supervisión, control, planeación, seguridad o calidad, debe fortalecer su conocimiento, la verificación y la evaluación de controles en las diferentes tipologías de riesgos y, la intensidad y frecuencia de los controles, según corresponda.

Los líderes del SIG deben requerir y compartir la información relacionada con la comunicación y consulta de los seguimientos, el monitoreo, y las estadísticas e indicadores. Toda materialización de riesgos debe ser tratada de forma inmediata y reportada al líder del proceso, a la coordinación de calidad y al responsable del Plan Anticorrupción y de Atención al Ciudadano - PAAC y del mapa de riesgos de corrupción, si se trata de un riesgo de este tipo (Oficina estratégica - Planeación o quien haga sus veces), incluyendo la información y soportes relacionados con el seguimiento a las acciones realizadas para mitigar el impacto.

Tercera línea de defensa, toda auditoría interna debe estar basada en riesgos y debe asegurar la eficacia de las metas de gobierno, mediante la evaluación de la gestión del riesgo y el control interno, incluyendo la operación de las dos primeras líneas de defensa.

1.2 Lineamiento 2: Nivel de aceptación del riesgo

Se establece que, el nivel de aceptación del riesgo, una vez se determine su valoración residual, llega hasta la valoración con nivel bajo, para todas las tipologías de riesgos identificadas. Por lo anterior, para los casos en que, al realizar seguimiento al riesgo, la valoración residual situé el riesgo en los niveles extremo, alto y moderado, se deben modificar los controles existentes o generar tratamientos adicionales.

Directrices:

En La primera línea de defensa, cada directivo debe reconocer los riesgos que están identificados en el Plan Anticorrupción y Atención al Ciudadano, donde tiene responsabilidad sobre el resultado. El Gerente y demás Directivos se comprometen a fomentar un clima que favorezca el análisis de los riesgos y la implementación de controles y acciones para tratar riesgos y oportunidades que permitan su mitigación y promoción.

Todos los responsables de procesos, programas y proyectos, deben gestionar los riesgos de corrupción: ejecutar los controles, comunicar sus resultados y generar las alertas tempranas que corresponda.

En la segunda línea de defensa, todo funcionario que tenga rol o funciones de supervisión, control, planeación, seguridad o calidad, es responsable de establecer y verificar los controles, en las diferentes acciones comprometidas en el PAAC.

En la tercera línea de defensa, toda auditoría interna debe estar basada en riesgos y debe asegurar la eficacia, mediante la evaluación de los controles establecidos para los riesgos de corrupción, incluyendo las maneras en que funcionan las líneas de defensa primera y segunda.

Toda materialización de riesgos debe ser reportada de inmediato al líder del proceso, a la coordinación de calidad y al responsable del Plan Anticorrupción y de Atención al Ciudadano – PAAC y del mapa de riesgos de corrupción si se trata de un riesgo de este tipo (Oficina estratégica - Planeación o quien haga sus veces), incluyendo el seguimiento a las acciones realizadas. "

2. OBJETIVOS

2.1 Objetivo General

Establecer el marco general para la Gestión de los riesgos en la Empresa para la Seguridad y Soluciones Urbanas – ESU, Direccionando la cultura organizacional, en función del desarrollo de un pensamiento basado en riesgos, orientando la toma de decisiones oportunas y minimizando la posibilidad de ocurrencia de eventos adversos que impidan el logro de los objetivos estratégicos y de los procesos.

2.2 Objetivos Específicos

- Analizar desde el contexto interno y externo a la Entidad y de los procesos, factores generadores de riesgo, que permitan la identificación de los factores que representan amenazas u oportunidades para el cumplimiento de los objetivos institucionales y la mejora continua en la gestión.
- Formalizar al interior de la Empresa para la Seguridad y Soluciones Urbanas – ESU, la metodología para administrar los riesgos de Gestión y de corrupción.
- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los servidores públicos y los trabajadores oficiales de la entidad (esquema de las líneas de defensa) en los riesgos de gestión.
- Fijar los parámetros para el establecimiento de acciones y controles que reduzcan la probabilidad de ocurrencia e impacto de los riesgos.
- Establecer lineamientos específicos para la Gestión de los riesgos de corrupción, de gestión de los procesos y de seguridad digital.
- Caracterizar el instrumento para la administración del riesgo (Mapa de riesgos).

3. ALCANCE

La Política de Administración de Riesgos de la Empresa para la Seguridad y Soluciones Urbanas – ESU, es aplicable al direccionamiento estratégico de la Entidad, a los procesos, a los planes institucionales, a los proyectos y a las acciones ejecutadas por los servidores públicos y los trabajadores oficiales durante el ejercicio de sus funciones; dándoles el tratamiento necesario, con base en la metodología definida, para cada tipología de riesgos.

4. TERMINOS Y DEFINICIONES

- **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 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 de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo 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.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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.
- **Gestión del riesgo:** proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.

- **Plan Anticorrupción y de Atención al Ciudadano:** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Integridad:** propiedad de exactitud y completitud.
- **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.
- **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).
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

5. METODOLOGÍA

La Empresa para la Seguridad y Soluciones Urbanas – ESU, establece su política para la gestión del riesgo bajo los parámetros establecidos en el documento Guía para la Administración del Riesgo de Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" expedido por el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones y en concordancia con la Norma Técnica Colombiana NTC-ISO 31000 en su última versión. Como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo de gestión, corrupción y los riesgos en seguridad digital, así como el control en todos los niveles de la organización, brindando seguridad razonable frente al logro de sus objetivos.

6. RESPONSABILIDADES Y ROLES

Primera Línea de Defensa Estratégica	Responsables: Alta Dirección y Comité Institucional de Coordinación de Control Interno CICCI.	ROLES: ✓ Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico. ✓ Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). ✓ Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. ✓ Realizar seguimiento y análisis periódico a los riesgos institucionales ✓ Realimentar al Comité de Gestión y Desempeño Institucional CGDI sobre los ajustes que se deban hacer frente a la gestión del riesgo.
	Responsables: Líderes de procesos	ROLES: ✓ Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del daño antijurídico. ✓ Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. ✓ Hacer ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.

		✓ Reportar en los indicadores de gestión, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. ✓ Informar a la Oficina estratégica - Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo.
Segunda Línea de Defensa	Responsables: Oficina estratégica - Planeación.	ROLES: ✓ Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. ✓ Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. ✓ Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. ✓ Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. ✓ Supervisar, en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones. ✓ Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por

		la primera línea de defensa. ✓ Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. ✓ Identificar cambios en la administración del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para aprobación del comité institucional de coordinación de control interno.
	Responsables: Líderes de los procesos	ROLES: ✓ Monitorear los riesgos identificados y controles establecidos ✓ Reportar a la Oficina de Auditoria Interna, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar. ✓ Acompañar, orientar y entrenar a los servidores públicos y los trabajadores oficiales de procesos en la identificación análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico.

Tercera Línea de Defensa	Responsable: Oficina de Auditoria Interna.	ROLES: ✓ Evaluar la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. ✓ Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. ✓ Asesorar de forma coordinada con la Oficina Asesora de Planeación y con, la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. ✓ Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI.

7. PRIORIZACIÓN DE RIESGOS A CONTROLAR

7.1 Clases de Riesgos

En la Empresa para la Seguridad y Soluciones Urbanas – ESU y de conformidad con su misión legal, los riesgos se han clasificado de la siguiente manera:

RIESGOS GERENCIALES: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

IMAGEN: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

ESTRATÉGICOS: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización y por tanto impacta toda la entidad.

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

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.

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.

OPERATIVOS: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

RIESGOS DE SEGURIDAD DIGITAL: Posibilidad 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.

7.1.1 De Corrupción

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

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

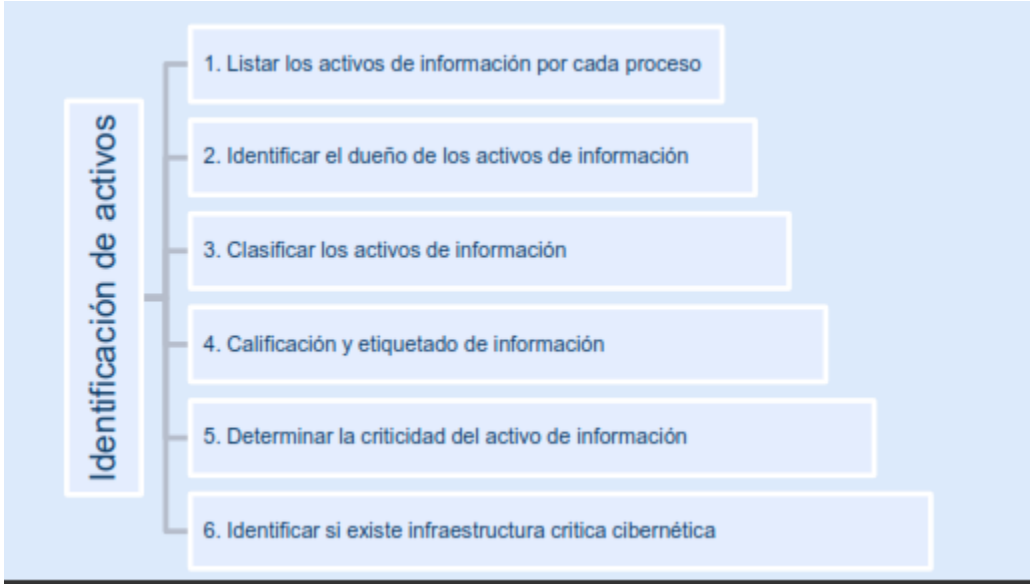
7.1.2 De Seguridad Digital

Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso:

“Integridad, confidencialidad o disponibilidad”

Solo existen tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

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



7.2 Identificación del Riesgo

La identificación del riesgo se realiza a partir de la descripción de los eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso con base en el contexto interno y externo. Es necesario hacer una breve descripción del riesgo refiriéndose a sus características o las formas en que se observa o manifiesta.

Seguidamente se deben identificar las posibles causas, medios, circunstancias, situaciones o agentes generadores del evento (riesgo).

Por último, se deberá identificar la consecuencia, hechos, acontecimientos o el impacto que se derivan o resultan de la ocurrencia o la materialización de un riesgo.

Para identificar un riesgo, sus causas y consecuencias, se sugiere formular las siguientes preguntas

¿ Qué puede ocurrir?
¿ Cómo puede ocurrir?
¿ Por qué puede ocurrir?
¿ Qué consecuencias tendría su materialización?

7.3 Análisis del riesgo

Analizar el riesgo permite establecer su probabilidad de ocurrencia y el nivel de consecuencias o impacto con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de Frecuencia o Factibilidad. Bajo el criterio de FRECUENCIA se analizan el # eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Por IMPACTO se entienden las consecuencias que puede ocasionar la ocurrencia del riesgo. Para su determinación se utiliza la tabla de niveles de impacto establecida en la Política de Riesgos.

La estimación del Nivel Inicial del Riesgo se logra a través de la determinación de la probabilidad y el impacto que puede causar la ocurrencia del riesgo, a través de la matriz de calificación del riesgo.

8. NIVELES DE CALIFICACIÓN, PROBABILIDAD E IMPACTO

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

8.1 Probabilidad riesgos de gestión, corrupción, seguridad digital

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

Criterios para calificar la Probabilidad			
Descriptor	**Descripción**	**Frecuencia**	**Nivel**
Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.	1
Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.	2
Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años	3
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.	4
Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año	5

8.2 Impacto riesgos de gestión

Calificación para establecer sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Alcaldía de Medellín

Medición Impacto Riesgos de Gestión			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	* Impacto que afecte la ejecución presupuestal en un valor igual o superior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o superior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor en un valor igual o superior al 50% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o superior al 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.	5
MAYOR	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 20% e inferior al 50% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 20% e inferior al 50% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 20% e inferior al 50% 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 del servicio a los usuarios o ciudadanos	4
MODERADO	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 10% y menor al 20% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 10% y menor al 20% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 10% y menor al 20% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 10% y menor al 20% del presupuesto general de la entidad.	* 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 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.	3
MENOR	* Impacto que afecte la ejecución presupuestal en un valor igual o mayor al 1% y menor al 10% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor igual o mayor al 1% y menor al 10% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor al 1% y menor al 10% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor al 1% y menor al 10% 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.	2
INSIGNIFICANTE	* Impacto que afecte la ejecución presupuestal en un valor menor al 1% * Pérdida de cobertura en la prestación de los servicios de la entidad en un valor menor al 1% * Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor menor al 1% * Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor menor al 1% del presupuesto general de la entidad.	*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.	1

8.3 Impacto riesgos de corrupción

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la Entidad.

Para facilitar la asignación del puntaje es aconsejable diligenciar el siguiente formato:

N	Pregunta Si el riesgo se materializa podria?	Respuesta	
		Si	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia ?		
3	¿Afectar el cumplimiento de misión de la Entidad ?		
4	¿Afectar el cumplimiento de misión del sector al cual pertenece la Entidad ?		
5	¿Generar perdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar perdida 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 perdida del bien o servicios o los recursos públicos?		
9	¿Generar perdida 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 perdida de credibilidad del sector?		
16	¿Ocasionar lesiones fisicas o perdida de vidas humanas ?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Medición de Impacto Riesgo de Corrupción			
Descriptor	**Descripción**	**Nivel**	**Respuestas Afirmativas**
Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad.	5	1 – 5
Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.	10	6 - 11
Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.	20	12 - 19

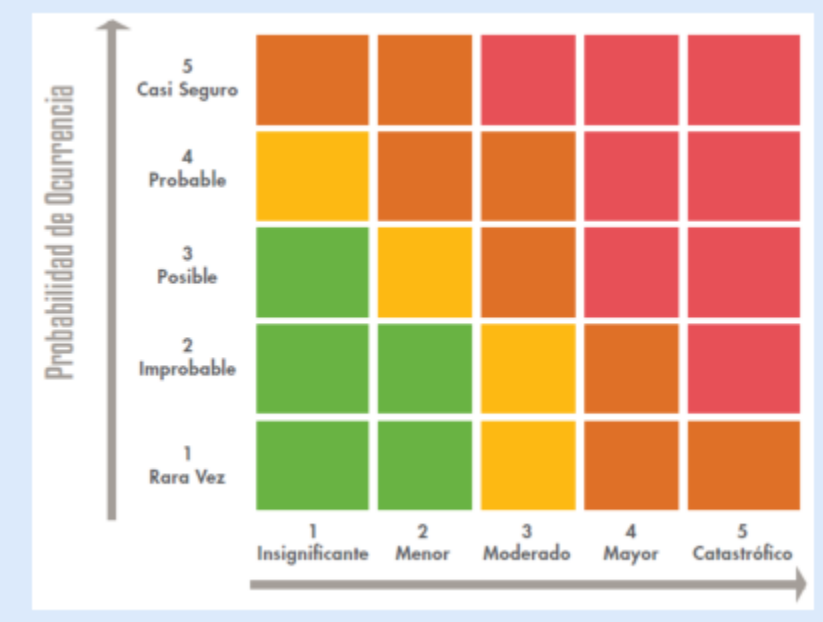
8.4 Impacto riesgos de seguridad digital

El impacto se determina con base a la amenaza, no en las vulnerabilidades.

Criterios de Impacto para Riesgos de Seguridad Digital			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	Afectación de la población en un valor igual o superior al 50% Afectación de la ejecución presupuestal de seguridad digital en un valor igual o superior al 50% Afectación muy grave del medio ambiente que requiere > 3 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	5
MAYOR	Afectación de la población en un valor igual o mayor al 20% e inferior al 50%. Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 20% e inferior al 50% Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.	4
MODERADO	Afectación de la población en un valor igual o mayor al 10% y menor al 20%. Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 10% y menor al 20% Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.	3
MENOR	Afectación de la población en un valor igual o mayor al 1% y menor al 10%. Afectación de la ejecución presupuestal de seguridad digital en un valor igual o mayor al 1% y menor al 10% Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.	2
INSIGNIFICANTE	Afectación de la población en un valor menor al 1% . Afectación de la ejecución presupuestal de seguridad digital en un valor menor al 1% No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad	1

9. NIVEL DE ACEPTACIÓN DEL RIESGO

Acogiendo la Matriz de riesgo sugerida en la Guía de Función Pública en su versión 5 del 2020, la medición de los riesgos de gestión y seguridad digital se hace a través de la tabla de probabilidad e impacto así:



Los riesgos de corrupción se hacen a través de la tabla de probabilidad e impacto así:

Probabilidad de Ocurrencia

Resultado calificación riesgos de corrupción				
Probabilidad	Puntaje	Zonas de riesgo de corrupción		
Casi seguro	5	25 Extrema	50 Extrema	100 Extrema
Probable	4	20 Alta	40 Extrema	80 Extrema
Posible	3	15 Alta	30 Extrema	60 Extrema
Improbable	2	10 Moderado	20 Alta	40 Extrema
Rara vez	1	5 Moderado	10 Alta	20 Alta
Impacto		Moderado	Mayor	Catastrofico
Puntaje		5	10	20

A partir de los criterios ERCA (Evitar, Reducir, Compartir y Aceptar), la Empresa para la Seguridad y Soluciones Urbanas – ESU, establece los siguientes niveles de aceptación a los riesgos identificados:

Zona de Riesgo Residual	Nivel de Aceptación	
	Riesgos Gestión y Seguridad Digital	Riesgos de Corrupción
Bajo	ACEPTAR el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado	Ningún riesgo de corrupción podrá ser aceptado
Moderado	Se establecen acciones de Control Preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo	
Alto	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan EVITAR la materialización del riesgo	Se adoptan medidas para REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Evitar - Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. Se reduce la probabilidad o el impacto del riesgo, TRANSFIRIENDO O COMPARTIENDO una parte del riesgo.
Extremo	se incluye el riesgo en el Mapa de riesgo del Proceso y en el Mapa de Riesgo Institucional, se establecen acciones de Control Preventivas y correctivas que permitan EVITAR la materialización del riesgo.	

10. EVALUACIÓN DEL RIESGO

Su objetivo es comparar los resultados del análisis de riesgos con los controles establecidos, para determinar la zona de riesgo final, los pasos a seguir son:

10.1 Diseño redacción de un control

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, un control debe tener:

10.2 Análisis y evaluación del diseño del control

De acuerdo a las variables del diseño que debe tener cada control se pondera el peso o porcentaje que debe tener cada variable para la adecuada mitigación del riesgo, de acuerdo a la siguiente tabla:

Controles de riesgos						
Descripción del Control	Naturaleza del Control		Criterios para la Evaluación	Evaluación		
	Preventivo	Detectivo	Aspectos a evaluar en el diseño del control			
			¿Existe un responsable asignado a la ejecución del control ?	Asignado	No Asignado	
				15%	0%	
			¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado	
				15%	0%	
			¿ 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	
				15%	0%	
			¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir	Detectar	No es control
				15%	10%	0%
			¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo. ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo.	Confiable	No Confiable	
				15%	0%	
			¿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	
				15%	0%	
			¿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
				10%	5%	0%
Total				100		

Cada control va a tener la misma importancia, por lo tanto, el consolidado de los controles para mitigar un riesgo, se realizará promediando el número de controles asociados al riesgo Función Pública.

El resultado de las calificaciones del control o promedio en el diseño de los controles, que este por debajo de 96 %, se debe establecer un plan de acción, para el adecuado diseño del control.

Calificación diseño de los controles	Definición
Fuerte 96% - 100%	El control o controles están bien diseñado para mitigar el Riesgo
Moderado 86% - 95%	Con Observaciones en la evidencia del control.
Débil 0% - 85%	El control tiene debilidades en su diseño para mitigar el riesgo.

Se debe confirmar por parte de los líderes de proceso la ejecución de cada control, de acuerdo a la siguiente tabla:

Calificación ejecución de los controles	Definición
Fuerte	Siempre se ejecuta por parte de los responsables
Moderado	Algunas veces se ejecuta por parte de los responsables
Débil	Nunca se ejecuta el control.

Cuyo resultado será:

Ponderación Diseño de Controles	Ejecución Controles	Solidez del Control
Fuerte	Fuerte	Fuerte
	Moderado	Moderado
	Débil	Débil
Moderado	Fuerte	Moderado
	Moderado	Moderado
	Débil	Débil
Débil	Fuerte	Débil
	Moderado	Débil
	Débil	Débil

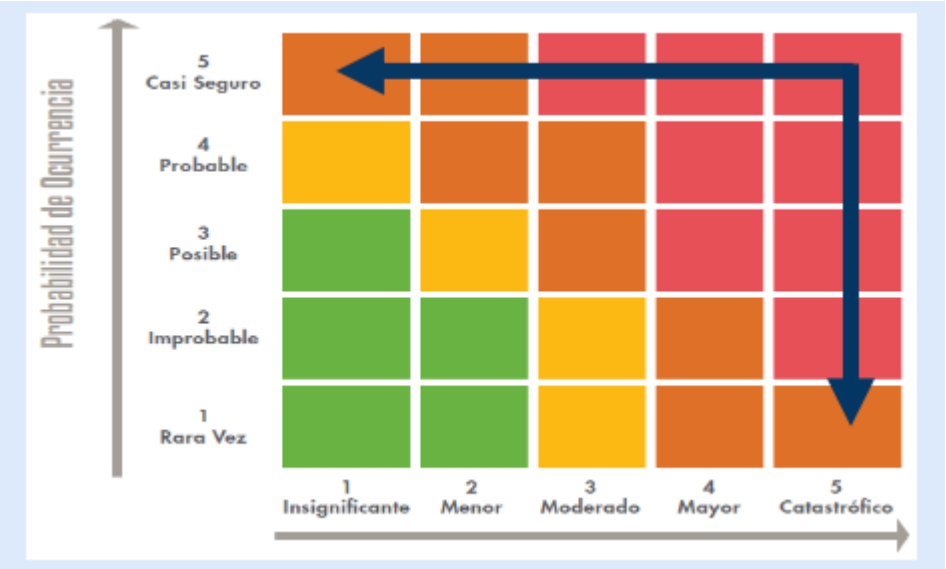
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, y considerando si lo controles ayudan o no a la disminución de impacto o la probabilidad,

procedemos a la elaboración del Mapa de Riesgo Residual (después de los controles) Función Pública.

La solidez del conjunto de controles se define acorde a la tabla por cada riesgo. Con la calificación obtenida se realiza un desplazamiento en la matriz, así: si el control afecta la probabilidad se avanza hacia abajo. Si afecta el impacto se avanza a la izquierda.

Contro 1	Control 2	Control 3	Solidez del Control
Fuerte	Fuerte	Fuerte	**Fuerte**
Fuerte	Moderado	Moderado	**Moderado**
Fuerte	Débil	Débil	**Débil**
Moderado	Fuerte	Moderado	**Moderado**
Moderado	Moderado	Moderado	**Moderado**
Moderado	Débil	Débil	**Débil**
Débil	Fuerte	Débil	**Débil**
Débil	Moderado	Débil	**Débil**
Débil	Débil	Débil	**Débil**

Calificación de los controles	Puntaje a dismunir
Debil	0
Moderado	1
Fuerte	2



11. MONITOREO Y REVISIÓN – Rol de las Líneas de Defensa

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión de Control Interno del MIPG, que se desarrolla a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores públicos y los trabajadores oficiales de la entidad así:

Línea Estratégica

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección (Comité de Gestión y Desempeño), el equipo directivo y el Comité de Coordinación de Control Interno.

1ª. Línea De Defensa

A cargo de los Directivos y líderes de procesos de la entidad.

2ª. Línea de Defensa

Conformada por los Coordinadores de Calidad, Líderes SIGI, responsables de monitoreo y evaluación de controles y gestión del riesgo, Director(a) de la Oficina Estratégica - Planeación o quien haga sus veces, supervisores o interventores de contratos o proyectos, coordinadores de otros sistemas, servidores públicos, los trabajadores oficiales y particulares que ejercen funciones públicas responsables de la aplicación de los controles y acciones de prevención y mitigación.

3ª. Línea de Defensa

Conformada por la oficina de Auditoria Interna o quien haga sus veces.

12. COMUNICACIÓN Y CONSULTA.

Tal como se expone en la quinta dimensión: Información y Comunicación del Modelo Integrado de Planeación y Gestión - MIPG, "... la comunicación hace posible difundir y transmitir la información de calidad que se genera en toda la Empresa para la Seguridad y Soluciones Urbanas – ESU...". Siendo este un ejercicio sistémico y de relación directa con la gestión de riesgos, se hace necesario, en cuanto a la comunicación de resultados, la revisión, el monitoreo y la evaluación, priorizando

- Cambios en el entorno
- Alertas por cambios en niveles esperados de desempeño
- Resultados del monitoreo, revisión y evaluación de riesgos.

- Cambios asociados a: el ciclo de reporte, evaluación y valoración, controles, acciones, la determinación o no de tratar un riesgo, las actividades definidas, el o los responsables, etc.

La información resultante de la gestión, monitoreo y evaluación, debe ser publicada en la página Web, según los compromisos vigentes, Así:

- 31 de enero de cada año, se publica el mapa de riesgos institucional incluyendo los riesgos de seguridad Digital y el mapa de riesgos de corrupción y de procesos. (Oficina estratégica - Planeación o quien haga sus veces).
- 30 de abril de cada año, posterior al primer **ciclo de monitoreo y evaluación** a los riesgos de seguridad Digital y el mapa de riesgos de corrupción y de procesos, publicar dentro de los 10 primeros días de mayo del mismo año. (Oficina estratégica - Planeación o quien haga sus veces – Oficina de Auditoria Interna o quien haga sus veces).
- 30 de junio de cada año, posterior al segundo **ciclo de monitoreo y evaluación** a los riesgos de seguridad Digital y el mapa de riesgos de corrupción y de procesos, publicar dentro de los 20 primeros días de Julio del mismo año. (Oficina estratégica - Planeación o quien haga sus veces – Oficina de Auditoria Interna o quien haga sus veces).
- 31 de agosto de cada año, posterior al segundo **ciclo de monitoreo y evaluación** a los riesgos de seguridad Digital y el mapa de riesgos de corrupción y de procesos, publicar dentro de los 10 primeros días de septiembre del mismo año. (Oficina estratégica - Planeación o quien haga sus veces – Oficina de Auditoria Interna o quien haga sus veces).
- 31 de diciembre de cada año, posterior al tercer **ciclo de monitoreo y evaluación**: a los riesgos de seguridad Digital y el mapa de riesgos de corrupción y de procesos, publicar dentro de los 10 primeros días de enero del siguiente año. (Oficina estratégica - Planeación o quien haga sus veces – Oficina de Auditoria Interna o quien haga sus veces).