"Por medio de la cual se actualiza la Política de Administración de Riesgos y los mapas de riesgos de la Contraloría Municipal de Barrancabermeja"

LA CONTRALORIA MUNICIPAL DE BARRANCABERMEJA

en uso de las atribuciones Constitucionales y Legales, especialmente las conferidas en los artículos 267,268 y 272 de la Constitución Política de Colombia, en las Leyes 42 y 87 de 1993, y,

CONSIDERANDO:

Que la Constitución Política de Colombia en el artículo 209, establece que la administración pública en todos sus órdenes tendrá un control interno que se ejercerá en los términos que señale la Ley.

Que el artículo 269 de la Constitución Política establece que las entidades públicas y autoridades correspondientes están obligadas a diseñar y aplicar según la naturaleza de sus funciones, los métodos y procedimientos de Control Interno de conformidad con lo que disponga la Ley.

Que la Ley 87 de 1993, establece como objetivos del Sistemas de Control Interno, proteger los recursos de la organización buscando su adecuada administración ante posibles riesgos que los afecten, así como definir y aplicar medidas para prevenirlos, y detectar y corregir las desviaciones que se presenten y que puedan afectar el logro de los objetivos institucionales.

Que el literal f) del artículo 2 de la Ley 87 de 1993, establece como uno de los objetivos del Sistema de Control Interno, la definición y aplicación de medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

Que así mismo, el Decreto 1537 de 2001, en su artículo 4°, señala que la Administración del Riesgo es parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas; y que, en ese orden de ideas, las autoridades establecerán y aplicarán políticas de administración de los riesgos.

Que el Acuerdo Municipal 003 de 2004, estableció la estructura de la Contraloría Municipal de Barrancabermeja y determino las funciones de sus dependencias.

Que el Decreto 943 de 2014, adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano, el cual incorporó en el Modelo Control de Planeación y Gestión el componente Administración del Riesgo. Que el Decreto 2641 de 2012, señaló como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida

en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano", en cuyo primer componente incorpora la "Metodología para la identificación de riesgos de corrupción y acciones para su manejo".

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022

Que mediante resolución No 044 de 15 de marzo de 2022 se adopta la Política de Administración de Riesgos y los mapas de riesgos de la Contraloría Municipal de Barrancabermeja.

Que, para dar continuidad al proceso de administración del riesgo, se hace necesario definir criterios orientadores respecto al tratamiento de los riesgos identificados, a fin de mitigar sus efectos en la entidad.

En mérito de lo expuesto.

RESUELVE

ARTÍCULO 1°: ACTUALIZAR la política de administración de riesgo de la Entidad, la cual estará liderada por la Alta Dirección y contará con la participación del Comité Institucional de Coordinación de Control Interno, así como, con el apoyo de los líderes de procesos y sus respectivos equipos de trabajo, quienes gestionarán, orientarán, implementarán y fortalecerán las etapas de administración de todo tipo de riesgos (gestión, corrupción, seguridad de la información), que impidan el logro de los objetivos estratégicos, institucionales y de procesos con base en las orientaciones establecidas en la Guía de Administración del Riesgo definida por la "P*or medio de la cual se adopta la actualización de la Política de Administración de Riesgos y los mapas de riesgos de la Contraloría Municipal de Barrancabermeja"*

Contraloría Municipal de Barrancabermeja para el tratamiento, manejo y seguimiento de los mismos, la cual hace parte integral del presente acto administrativo.

PARÁGRAFO. En el Mapa de riesgos se definirán: identificación del riesgo, controles, estrategias de mitigación, periodicidad de monitoreo por parte de las líneas de defensa.

ARTÍCULO 2°. Objetivo de la política. Establecer los lineamientos para la Administración del Riesgo en la Contraloría Municipal de Barrancabermeja, mediante la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos a los que está expuesta la Entidad, con el propósito de generar una cultura de prevención frente a la ocurrencia de hechos o situaciones que puedan afectar o entorpecer la gestión institucional.

ARTÍCULO 3°. Alcance de la política. Esta política aplica a todos los procesos de la Contraloría Municipal de Barrancabermeja, en el marco del sistema de gestión de calidad,

es establecida por la Alta Dirección en el Comité Institucional de Coordinación de Control Interno y con el fin de garantizar un adecuado conocimiento y control de los riesgos en todos los niveles organizacionales, esta política se hace extensiva a todos los funcionarios de la entidad.

ARTICULO 4°. Estrategias. Establecer como estrategias para la administración de los riesgos en la Contraloría Municipal de Barrancabermeja, las siguientes:

1. Diseñar e implementar una metodología para la Administración de los Riesgos.
2. Realizar monitoreo a los riesgos de los procesos del Sistema de Gestión de Calidad.
3. La comunicación y divulgación de los riesgos se realizará por los líderes de cada proceso y a través de la página web institucional.

ARTICULO 5°. Vigencia y derogatorias. La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

PUBLIQUESE, COMUNIQUESE Y CÚMPLASE

Dada en Barrancabermeja, a los (08) días del mes de agosto de 2024.

DANNY MARCELA GOMEZ PUERTA
Contralora Municipal

Elaboro: Diana Milena León Anteliz, Profesional Externo

Reviso: Víctor Hugo Flórez Salazar, Profesional Universitario responsable de Control Interno

Aprobó: Carlos Arturo Vásquez Aldana, Secretario General

POLITICA DE RIESGOS DE LA CONTRALORIA MUNICIPAL DE BARRANCABERMEJA

CONTRALORÍA MUNICIPAL
BARRANCABERMEJA

Agosto, 2024

Vigilancia y Control Integral, Barrancabermeja Sostenible
Avenida Circunvalar, Calle 67, Estadio Daniel Villa Zapata
Tribuna Oriental, Piso Tercero y Piso Cuarto.
Email: info@contraloriabarrancabermeja.gov.co
Página Web: www.contraloriabarrancabermeja.gov.co

TABLA DE CONTENIDO

INDICE DE TABLAS.

INDICE DE GRÁFICOS.

1. INTRODUCCIÓN

La política para la administración de riesgos del presente documento toma como marco referencial para su elaboración la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, Noviembre del 2022* establecida por el DAFP y otras normas como *ISO 31000: 2018* para la gestión de los riesgos que puedan comprometer el desarrollo de los programas de objetivos, planeación y funcionamiento institucional en aras del cumplimiento de la misión visión y mejoramiento continuo de la entidad.

2. USO DEL DOCUMENTO

El uso del presente documento establecerá un marco de referencia para la actuación de los servidores públicos de la Contraloría Municipal de Barrancabermeja frente a los riesgos y sus posibles impactos que puedan afectar los procesos y objetivos institucionales mediante lineamientos claves para el tratamiento, manejo y seguimiento, a través de esquemas metodológicos integrales en todos los niveles y formalizados en la presente política.

3. OBJETIVO

Mediante los lineamientos referenciales de la presente política implementar acciones, mecanismos y criterios para para el tratamiento y mitigación de los riesgos, teniendo en cuenta los requerimientos normativos establecidos para el cumplimiento de los objetivos y el desarrollo de los procesos asegurando su continuidad.

4. ALCANCE

La presente política se aplicará a todos los once (11) procesos de la Contraloría Municipal de Barrancabermeja, métodos y procedimientos establecidos, así como a todos los funcionarios, contratistas y colaboradores. Será de carácter estratégico bajo la responsabilidad de los lideres de proceso y líneas de defensa su implementación y puesta en práctica.

5. POLITICA

La Contraloría Municipal de Barrancabermeja, a través de su Alta Dirección, en aras de propender por el cumplimiento de su misión, visión y objetivos institucionales se compromete a gestionar y administrar los riesgos de manera efectiva en sus diferentes procesos estableciendo el sistema para la administración de riesgos, utilizando como marco de referencia el Modelo Integrado de Planeación y Gestión (MIPG). Este compromiso será articulado con otras de nuestras políticas de Control

Interno y se implementa con la activa participación de todos los funcionarios de la entidad.

Para asegurar una gestión de riesgos sólida y alineada con las mejores prácticas, adoptamos la guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 6, noviembre de 2022) del Departamento Administrativo de la Función Pública. Complementariamente, cumplimos con los requisitos de los sistemas de gestión y control basados en otras normas internacionales (ISO 31000) que son aplicables y tienen un potencial de mejora a nuestra entidad.

Anualmente, se procederá a la revisión e identificación de los riesgos institucionales, siguiendo la metodología vigente incluida en la presente política, asegurando que los controles estén alineados con los compromisos de cada proceso para una gestión integrada y efectiva de los riesgos contemplando el tiempo, los recursos, los responsables y el talento humano requerido para la evaluación de la implementación efectiva de la política.

6. NIVELES DE ACEPTACIÓN DEL RIESGO

La guía de administración de riesgos del departamento de administración pública propone las siguientes medidas de control:

SE ACEPTAN- SE ASUMEN: Riesgos cuyo resultado de los controles determinen un nivel residual bajo y riesgos moderados con seguimiento periódico por parte de los lideres internos de cada proceso (Los riesgos de carácter fiscal y corrupción no serán aceptados y requerirán de un plan de acción en todos los casos).

SE REDUCEN- SE MITIGAN: Para los riesgos que, una vez aplicados los controles, generan un resultado Alto o extremo, se requiere un plan de acción para abordar los riesgos, además de un seguimiento por parte de los lideres de los procesos.

SE EVITAN: Aquellos riesgos que luego de aplicados los controles siguen teniendo un resultado alto o extremo, de ser posible no se debe realizar la actividad o plantear una diferente.

7. IDENTIFICACIÓN DE RIESGOS

Los criterios para la identificación de riesgos se presentan mediante la siguiente tabla para su clasificación:

Tabla 1. *Tabla de clasificación de riesgos*

Ejecución y administración de procesos	Perdidas relacionadas con errores en ejecución y gestión de los procesos.
Fraude externo	Perdida ocasionada por fraude por personal que no pertenece a la entidad.
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones u otras herramientas utilizadas por la entidad de carácter tecnológico que pueden verse traducidas en un riesgo o interrupción de las actividades.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y practicas	Negligencia o fallas involuntarias de las obligaciones hacía los usuarios y que impiden el cumplimiento de los requisitos de las partes interesadas.
Daños a activos físicos / eventos externos	Perdida por daños o perdidas de los activos fijos por causas naturales u otras causas externas como vandalismo, orden público o atentados

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, Noviembre del 2022*

La redacción de los riesgos debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso, por este motivo deberá ser redactado con las causas inmediatas y las causas raíz.

8. NIVELES PARA DEFINIR LA PROBABILIDAD E IMPACTO

8.1 Nivel de probabilidad: Para catalogar la probabilidad de que un riesgo se materialice, de primera mano se relaciona la frecuencia de la actividad, sin embargo, este criterio de probabilidad puede adaptarse según se considere a la complejidad de los procesos.

De primera mano se utilizarán los criterios expuestos en la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022,* expuestos en la siguiente tabla:

Tabla 2. *Categorías para medir la probabilidad.*

Categoría	Frecuencia de la actividad	Probabilidad
Muy baja	Actividad en la que el riesgo se ve involucrado mediante la ejecución un límite de 2 veces al año.	20%
Baja	Actividad en la que el riesgo se ve involucrado mediante la ejecución un de 4 a 24 veces al año	40%
Media	Actividad en la que el riesgo se ve involucrado mediante la ejecución un de 4 a 500 veces al año	60%
Alta	Actividad en la que el riesgo se ve involucrado mediante la ejecución un de 501 a 5000 veces al año	80%
Muy Alta	Actividad en la que el riesgo se ve involucrado mediante la ejecución de más de 5001 veces al año	100%

Fuente: Elaboración propia, adaptada de la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

Finalmente, el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente

8.2 Niveles para definir el impacto: Para catalogar el impacto de cada uno de los riesgos identificados de la entidad, se tendrán en cuenta 2 variables (Afectación económica e impacto reputacional).

Tabla 3. *Categorías para medir el impacto.*

Categoría de impacto	Afectación económica	Impacto reputacional
Leve- 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor- 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado- 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor- 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario

		sostenido a nivel de sector administrativo, nivel departamental o municipal.
	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

Cada líder del proceso adaptará, ajustará tomará la categoría del impacto según las necesidades y la complejidad del proceso. Dado se categoricé el impacto reputacional y económico en el mismo nivel de la fila, se contemplará el siguiente nivel para asegurar la implementación de controles más efectivos según lo indicado en la misma guía.

9. NIVELES VALORAR EL RIESGO PRELIMINAR O INHERENTE

El riesgo en todos los casos se calculará mediante la clasificación de probabilidad x impacto, cruzando los datos en la matriz de calor para identificar la severidad de los riesgos de manera inherente.

Tabla 4. *Matriz de calor para medir el riesgo inherente.*

		IMPACTOS				
PROBABILIDAD	Muy alta (100%)					
	Alta (80%)					
	Media (60%)					
	Baja (40%)					
	Muy Baja (20%)					
	Criterios	Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, Noviembre del 2022*

ALTO
MODERADO
BAJO

10. CONTROL DEL RIESGO

Para la medición del riesgo de manera específica y no genérica, no solamente se tendrá en cuenta probabilidad e impacto, sino que también se deben contar los controles que se tienen presentes en los procesos, su peso y cuanto reducen los riesgos presentes; en base a los resultados obtenidos, de no estar dentro de los parámetros de tolerancia del riesgo, se implementaran más controles que permitan reducir el riesgo presente o se evitará en su defecto, la causa raíz.

Para medir de primera mano el peso de controles que se tienen en la institución primero se identificaran y se categorizaran los controles con cada líder de proceso; cada control debe tener en su descripción que se establecerá mediante la siguiente estructura.

Gráfico 1. *Como describir los controles.*

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

Y posteriormente se clasificarán los controles según su tipología (Preventivos, detectivos y correctivos), la clasificación se hará según el ciclo del proceso.

Gráfico 2. *Tipología de controles.*

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

Del mismo se valorará de qué manera se realiza la implementación de dichos controles y se les asignará un peso, que ayudará posteriormente a calcular los riesgos residuales; los controles de aplicación en el mapa de riesgo se definen a continuación:

Implementación automática: Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo sin la intervención de personas.

Implementación manual: Controles que son ejecutados por una persona, tiene implícito el error humano

Además de otros atributos información que nos permitirá clasificar la información que, si bien no inciden en su efectividad, complementan los análisis para un control más formal.

Documentación: Se pueden presentar de dos (02) formas. Aquellos controles que están **documentados** en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento y los controles **sin documentar** que refiere a los controles que pese a que se ejecutan en el proceso no se encuentran documentados.

Frecuencia: Si es **continua,** el control se aplica siempre que se realiza la actividad. y si la frecuencia es **aleatoria**, el control se aplica de manera aleatoria**.**

Evidencia: Si cuando se aplica el control se deja un **registro** que sirva como evidencia.

El peso de cada uno de los controles viene siendo valores constantes definidos en la guía del DAFP, y los resultados de la administración de los riesgos serán el resultado del ingreso de todos los datos anteriores en el modelo del mapa de riesgos brindado por la misma entidad.

Los pesos asignados para el cálculo residual se exponen a continuación.

Tabla 5. *Peso de los controles.*

CARACTERÍSTICAS			PESO
Atributos de eficiencia.	**Tipo**	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%
Atributos informativos	**Documentación**	Documentado	N/A
		Sin documentar	N/A
	Frecuencia	Continua	N/A
		Aleatoria	N/A
	Evidencia	Con registro	N/A
		Sin registro	N/A

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

La valoración de los controles se calcula con la sumatoria de los pesos para posteriormente calcular la probabilidad o impacto residual.

La fórmula para calcular la probabilidad o impacto residual de que se manifieste un riesgo con los controles viene descrita a continuación.

Lo primero que se deberá determinar es la probabilidad o impacto según los controles aplicados (Preventivos, Detectivos o Correctivos)

Tabla 6. *Fórmula para calcular el impacto residual.*

Probabilidad o impacto inherente - (Probabilidad o impacto inherente * valoración del control 1) = Probabilidad o impacto residual del control 1
Probabilidad o impacto residual del control 1- (Probabilidad o impacto residual del control 1 * Valoración del control 2) = Probabilidad o impacto residual del control 2

Fuente: Autor

Lo anterior es debido a que los controles tienen un efecto acumulativo sobre las probabilidades o impactos residuales, esto quiere decir que una vez se aplica el

valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

11. TRATAMIENTO DE LOS RIESGOS

El tratamiento de los riesgos se realizará mediante un plan de acción, se efectuara el seguimiento mediante el siguiente formato brindado por la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, Noviembre del 2022* y será responsabilidad de cada líder de procesos su respectivo control y seguimiento.

Para el tratamiento de los riesgos, el DAFP propone 4 alternativas para el tratamiento, que deberán ir encaminados a según los niveles de aceptación de la presente política; estos 4 niveles de tratamiento son:

Aceptar el riesgo: Cuando los controles que se tienen implementados son lo suficientemente efectivos como para aceptar los riesgos, o los riesgos tengan un impacto de carácter irrelevante en la actividad profesional (para lo riesgos de corrupción, no se aceptará bajo ninguna circunstancia)

Reducir el riesgo: Se trabaja sobre su probabilidad e impacto con controles preventivos, detectivos o correctivos.

Evitar el riesgo: De ser posible y necesario, abandonar la actividad, no continuarla o iniciarla para no dar lugar al riesgo.

Compartir el riesgo: Se mantiene la responsabilidad del riesgo, pero transfieren parte de este riesgo con otra parte interesada que pueda gestionarlo con más eficacia.

Tabla 7. *Elaboración de un plan de acción.*

Plan de acción	Responsable	Fecha de implementación	Fecha de seguimiento	Seguimiento	Estado

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

12. NIVELES DE RESPONSABILIDAD FRENTE A LOS RIESGOS

LINEA DE DEFENSA	RESPONSABLES	RESPONSABILIDAD
Línea estratégica	Comité institucional de gestión y desempeño.	• Definir las directrices para gestionar los riesgos que puedan influir en el cumplimiento de la misión,

		los objetivos estratégicos y los procesos. • Solicitar a los responsables de los procesos que adopten las medidas necesarias conforme al Informe de seguimiento preparado por la Oficina de Control Interno. • Generar recomendaciones de mejora a la política de administración del riesgo con enfoque a procesos institucionales.
	Comité institucional de coordinación de control interno	• Aprobar la política de administración del riesgo. • Evaluar la eficacia de la política en relación con la gestión del riesgo institucional, con enfoque a la prevención y detección de fraude y mala conducta • Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad
Primera línea de defensa	Lideres de cada proceso	• Identificar, valorar, evaluar y actualizar, cuando sea necesario, los riesgos que pueden impactar los objetivos, programas, proyectos y planes asociados a su proceso, además de realizar un seguimiento continuo al mapa de riesgos del proceso a su cargo. • Supervisar la ejecución de los controles implementados por el

		equipo de trabajo en la gestión diaria, detectar deficiencias en dichos controles así como determinar las acciones de mejora necesarias. • En caso de que se materialice un riesgo no identificado, este debe ser gestionado de acuerdo con la política de administración de riesgos de la entidad y ser incorporado en el mapa de riesgos institucional • Revisar las acciones y planes de mejoramiento establecidos para cada riesgo materializado, con el objetivo de tomar medidas oportunas y eficaces. • Asegurar que se documenten las acciones de corrección o prevención suscritas en plan de mejoramiento • Comunicar al equipo de trabajo los resultados de la gestión del riesgo.
	Equipos de trabajo	• Participar en el diseño de los controles que tienen a cargo. • Ejecutar los controles a su cargo de la forma como están diseñados • Proponer mejoras a los controles existentes
Segunda línea de defensa	Secretario general. Coordinadores de sistemas de gestión	• Asesorar a la línea estratégica en cuanto a los lineamientos para la gestión de riesgos que puedan impactar el logro de los objetivos y metas institucionales.

		• Efectuar seguimiento a los controles aplicados por la 1ª línea de defensa • Revisar el adecuado diseño de los controles a través de la metodología aplicada en el sistema de gestión institucional para la mitigación de los riesgos y recomendar acciones para el fortalecimiento de estos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo • Asesorar a los lideres de procesos sobre la materialización de riesgos y velar por su gestión conforme a la presente política.
Tercera línea de defensa	Oficina de control interno.	• Informar a la dirección sobre nuevos posibles riesgos de carácter institucional. • Cuando se considere necesario asesorar a los lideres de procesos con la segunda línea de defensa sobre diseños de controles efectivos. • Realizar seguimiento a los riesgos identificados en el mapa de riesgos conforme al plan anual de auditoría. • Revisión de los planes de acción para controlar los riesgos y recomendar mejoras. • Revisar los cambios en el "Direccionamiento estratégico" o en el

		entorno, y establecer de ser necesario, cómo estos pueden generar nuevos riesgos o modificar los riesgos ya identificados en cada uno de los procesos para la actualización del mapa de riesgos.

Fuente: Autor

13. LINEAMIENTOS PARA TRATAR EL RIESGO FISCAL.

La definición del riesgo fiscal es un hecho incierto o incertidumbre ocasionada por una potencial acción u omisión que podría generar un efecto de carácter dañoso sobre los recursos públicos, bienes o intereses de naturaleza pública.

Para la gestión de estos riesgos primeramente se identificaran los puntos críticos de riesgo fiscal, con sus causas inmediatas, estos puntos serán identificados según las situaciones que generen riesgos fiscales refiriéndonos al Artículo 3 Ley 610 de 2000 tales como: administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, así como otras actividades con advertencias, alertas o hallazgos fiscales o con responsabilidad fiscal del mismo modo se tendrán en cuenta los hallazgos y fallos fiscales así como los planes de mejoramiento institucional e históricos generados en los últimos 3 años.

.

Finalmente se hallarán de los fallos y de los riesgos identificados, las causas inmediatas y causas raíz, para que la gestión del control de los riesgos fiscales permita trabajar los potenciales hechos generadores de las causas que pueden verse traducidos como un daño al recuso público en caso de no contemplarse ya que deberán de ser acorde a las causas identificadas.

El tratamiento de los riesgos y controles se manejará según los criterios de los NIVELES VALORAR EL RIESGO PRELIMINAR O INHERENTE.

La diferencia con respecto a los riesgos de procesos radica en que el impacto en todos los casos y dada la misma definición de riesgo fiscal será de tipo de **económico** dado que el efecto corresponderá a una consecuencia en todos los casos económicas sobre el patrimonio público.

14. LINEAMIENTOS PARA TRATAR RIESGOS DE CORRUPCIÓN

Los riesgos de corrupción son la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, por ende los riesgos de corrupción al ser de carácter significativo; las circunstancias que se involucran en materia de responsabilidad administrativo-penal, tendrán criterios de valoración de las probabilidades e impactos distintos a los lineamientos anteriores correspondientes a los riesgos de corrupción inherentes al desarrollo de los procesos de la entidad pública.

Los riesgos de corrupción de la entidad según el (Conpes N° 167 de 2013) 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; por lo que es necesario que para la identificación de los riesgos sobre los procesos se tenga en cuenta su definición y las siguientes generalidades para su cronograma.

- Su elaboración será de periodicidad anual y será responsabilidad de los lideres de los procesos internos junto con su equipo de trabajo.

- Se difundirá según lo establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 el mapa de riesgos será publicado en la página web como medio de fácil acceso a la ciudadanía estableciendo las condiciones de reserva de la información basándose en lo establecido en los artículos 18 y 19 de la Ley 1712 de 2014

- Antes de su publicación los servidores públicos y contratistas deberán conocer el contenido y conformidad del mapa de riesgos de corrupción con los mecanismos necesarios que aseguren su participación en pro del enriquecimiento del mapa de riesgos de corrupción.

- Se llevará la trazabilidad de los ajustes y las modificaciones luego de cada año de vigencia dejando por escrito las acciones realizadas alineadas en la mejora del mapa de riesgos de corrupción.

- El responsable de auditorías internas analizará las causas establecidas en los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

Para la elaboración del mapa de riesgos, se deberán tener en cuenta los criterios para la valorización de los riesgos de corrupción; estos son el resultado de el impacto del riesgo de corrupción y su frecuencia de materialización del riesgo o factibilidad de materialización del riesgo (como un conjunto de factores interno y externos que son propicios para materialización de los riesgos) que define su

probabilidad. La intersección de la matriz será el riesgo inherente resultante de la valorización de los riesgos de corrupción, las matrices anteriormente mencionadas de cada una de las variables se definen a continuación.

Tabla 8. *Cálculo de la probabilidad para riesgos de corrupción.*

PROBABILIDAD			
Nivel	**Probabilidad**	**Factibilidad**	**Frecuencia**
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos una vez en el último año
3	Posible	El evento podrá ocurrir en cualquier momento	Al menos una vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir en circunstancias excepcionales	No se ha presentado en los últimos 5 años

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

El impacto se debe calificar según las consecuencias identificadas en la descripción del riesgo, la guía del DAFP proporciona una serie de criterios que facilita calificar el impacto que se tomará como referencia para el cálculo de la evaluación de los riesgos de corrupción inherentes; los criterios se adjuntan en la siguiente tabla:

Tabla 9. *Cuestionario para medir el impacto de riesgos de corrupción.*

N°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		

Nivel de impacto MAYOR

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

Es decir que por cada riesgo identificado se deberá realizar la ponderación mediante la diligencia de la tabla anteriormente adjunta y se aplicarán los resultados a la matriz de calor de **NIVELES VALORAR EL RIESGO PRELIMINAR O INHERENTE** apreciando las circunstancias que implican un riesgo de corrupción. La matriz para analizar el riesgo inherente de los riesgos de corrupción con las apreciaciones se realizará de la siguiente manera:

Tabla 10. *Matriz de calor para hallar el riesgo inherente.*

PROBABILIDAD	IMPACTOS					
	Muy alta (100%)	NO APLICA				
	Alta (80%)					
	Media (60%)					
	Baja (40%)					
	Muy Baja (20%)					
	Criterios	Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022*

EXTREMO
ALTO
MODERADO
BAJO

Es importante resaltar que estos riesgos siempre serán significativos y no se aplican impacto leve y menor, solo se implementarán los controles para disminuir su probabilidad (Preventivos y Detectivos) y no de carácter correctivo por lo que se deberá tener en cuenta como se pueden tratar los riesgos y dada su necesidad de monitorización será responsabilidad de la primera de línea de defensa gestionar de primera mano en sus procesos lo riesgos presentes y en caso de materialización su protocolo de actuación será de la siguiente manera:

1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4) Llevar a cabo un monitoreo permanente asegurando que los controles sean efectivos, le apunten al riesgo sean oportunos y estén funcionando conforme lo indica el mapa mediante las siguientes opciones:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para
- prevenir o mitigar los riesgos de corrupción.

- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

15. ADMINISTRACIÓN DE RIESGOS TI.

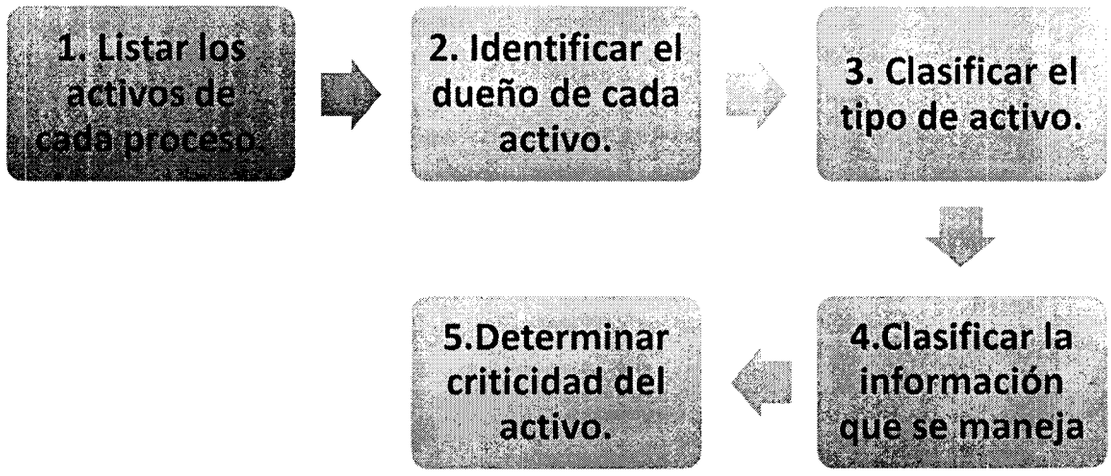
Un activo es definido como cualquier elemento que tenga valor para una organización, sin embargo, cuando nos referimos a seguridad digital y su contexto, las entidades de carácter público cuentan con servicios Web, redes, información física o digital, Tecnologías de la Información y en algunos casos sus procesos dependen de tecnologías operativas.

Teniendo en cuenta los criterios anteriores, para la administración de los riesgos TI, es necesario que la entidad identifique los activos y los documente, no solamente para saber que es lo más importante que cada entidad y sus procesos poseen, sino saber que se debe proteger para garantizar su continuidad internamente y su funcionamiento de cara al ciudadano y propender por la confianza de la ciudadanía en usar los entornos digitales para interactuar con el estado.

15.1 Identificación y valoración de los activos.

La identificación y valoración de los activos, al ser utilizado en los procesos de la entidad, será responsabilidad de la primera línea de defensa, en dónde se apliquen medidas para gestionar los riesgos orientados por el responsable de la seguridad digital o de seguridad de la información, para realizar la identificación de los riesgos se utilizará la siguiente metodología dada por el Ministerio de Tecnologías de la Información y las Comunicaciones:

Gráfico 3. *Pasos para caracterizar los activos.*



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Y se hará de la siguiente manera:

1. **Listar los activos de cada proceso:** Los activos deben listarse, pero además deberán ir con un consecutivo, nombre y descripción de manera breve de cada uno.
2. **Identificar dueños de cada activo:** Cada activo deberá tener un dueño designado, de no tenerlo nadie se hará responsable ni lo protegerá debidamente.
3. **Clasificar los activos:** Según su tipología, para ello se hará uso de la siguiente tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo que servirán como guía para su mapeo y control.

Tipo de activo	Definición	Ejemplo de vulnerabilidad	Ejemplo de amenaza
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información	Almacenar medios sin protección.	Hurto de medios o documentos

Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades	Ausencia de parches de seguridad	Abuso de los derechos
Red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red	Líneas de comunicación sin protección	Escucha encubierta
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), esta información puede ser: : Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión	Falta de controles de acceso físico	Hurto de información
Personal	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información	Falta de capacitación en las herramientas	Error en el uso
Organización.	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018

4. **Clasificar la información:** Conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos y la Norma ISO 27001:2013, su clasificación será la siguiente:

Tabla 11. *Clasificar información de los activos.*

Ley 1712 de 2014	Ley 1581 de 2012
Información reservada.	Contiene datos personales
Información pública.	No contiene datos personales
N/A	N/A

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

5. **Determinar la criticidad del activo:** cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información su criticidad de valorará siguiendo los criterios de la *Guía para la Gestión y Clasificación de Activos de Información No 5 de 2016.*

Tabla 12. *Matriz para hallar la criticidad del activo.*

Criticidad de confidencialidad.	Criticidad de la integridad	Criticidad de la disponibilidad
(ALTA) si es información reservada al público	**(ALTA)** si Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones de manera severa.	**(ALTA)** La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas
(MEDIA) si es información clasificada.	**(MEDIA)** si Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones de manera moderada	**(MEDIA)** La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen de manera moderada

(BAJA) si es información pública.	**(BAJA)** Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo	**(BAJA)** La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales

Fuente: *Guía para la Gestión y Clasificación de Activos de Información No 5 de 2016.*

Su criterio para su nivel de criticidad se valorará en la tabla anterior según los siguientes criterios:

Tabla 13. *Matriz para hallar la criticidad final del activo.*

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: *Guía para la Gestión y Clasificación de Activos de Información No 5 de 2016.*

La identificación de activos será documentada de la siguiente manera:

Tabla 14. *Información documentada de los activos.*

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestion financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Elaborado en la *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, noviembre del 2022,* Información de *Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.*

15.2 Identificación de los riesgos

Los riesgos se clasificarán según la criticidad del punto anterior y la lista de activos que debe estar realizada hasta este punto, la clasificación de los riesgos, son los siguientes:

a. Perdida de la integridad.
b. Perdida de la disponibilidad.
c. Perdida de la confidencialidad.

Para la identificación de estos riesgos es necesario identificar en cada proceso, aquellas amenazas y vulnerabilidades que pueden significar un riesgo para la entidad, para esta actividad la UNE ISO/IEC 27005:2009 identifica posibles amenazas y vulnerabilidades para que cada entidad en base a sus circunstancias implemente los controles:

Las amenazas más comunes son:

Tabla 15. *Amenazas TI comunes.*

Tipo	Amenaza
Daño físico	Fuego
	Agua
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua
	Fallas en el suministro de aire acondicionado
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
Compromiso de la información	Intercepción de servicios de señales de interferencia comprometida
	Espionaje remoto
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
Compromiso de las funciones	Error en el uso o abuso de derechos
	Falsificación de derechos

Fuente: ISO/IEC 27005:2009

Las amenazas de tipo humano son:

Tabla 16. *Amenazas TI de tipo humano.*

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto	Piratería
	Ego	Ingeniería social
Criminal de la computación	Destrucción de la información	Crimen por computador
	Divulgación ilegal de la información	Acto fraudulento
Terrorismo	Chantaje	Ataques contra el sistema
	Destrucción	DDoS
		Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva	Ventaja de defensa
	Espionaje económico	Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad	Asalto a un empleado
	Ganancia monetaria	Chantaje

Fuente: ISO/IEC 27005:2009

Las identificables en las siguientes áreas según el tipo de activo son las siguientes:

Tabla 17. *Tipos de activo y sus vulnerabilidades.*

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de concienciа en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005:2009

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad puesto que para se pueda materializar un daño, es necesario que una amenaza pueda explotar esa debilidad, esto quiere decir, que las vulnerabilidades que no tienen una amenaza asociada pueden no requerir la implementación de controles.

15.3 Valoración de los riesgos TI

Para la valoración de los riesgos TI se asociarán las tablas de probabilidad del apartado de lineamientos para tratar riesgos de corrupción y de impacto del apartado de valoración del riesgo de la presente política y el cálculo de los riesgos inherentes. Los riesgos inherentes que no tengan controles implementados serán considerados como riesgos residuales.

15.4 Control de los riesgos TI

Para el control de los riesgos TI, se darán conforme al *Anexo A del estándar ISO/IEC 27001:2013, p.29* que serán ajustados a la entidad mediante la aplicación de *lineamientos para la gestión de riesgos de seguridad digital en entidades públicas del ministerio de tecnología e información*: se documentará su opción de tratamiento (reducir, evitar, aceptar, compartir), su actividad y soporte (ver anexo a), y se asignará un indicador para la eficacia y efectividad.

La persona encargada de gestionar en primera instancia los riesgos TI en la marco del quehacer y su saber será responsable sistemas TI de la entidad y en segunda instancia serán los lideres de los procesos.

16. SEGUIMIENTO Y EVALUACIÓN DEL MAPA DE RIESGOS Y CONTROLES

Los líderes de proceso monitorean constantemente los controles definidos para los riesgos y las acciones del plan de acción, cuando haya lugar. Además, registran con periodicidad anual en el seguimiento de los mismos.

La Secretaria General, podrá cumplir acciones de monitoreo de acuerdo con las responsabilidades como segunda línea de defensa, y de acuerdo con la política. La Oficina de Control Interno lleva a cabo el seguimiento a la administración del riesgo, de conformidad con lo indicado en los documentos "Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces" y como se determina en el título precedente de Roles y Responsabilidades.

La Oficina de Control Interno presentará un informe anual sobre los resultados de la evaluación de la efectividad del Sistema de Control Interno - SCI, acorde con la evaluación de los controles definidos en los mapas de riesgos y de los riesgos de procesos, en el cual se consigne, cuando sea el caso, la materialización, la creación, la modificación o la eliminación de alguno de los riesgos.

ANEXOS

1. FORMATO DE MAPEO DE RIESGOS OPERATIVOS Y FISCALES.
2. FORMATO DE MAPEO DE RIESGOS DE CORRUPCIÓN.
3. FORMATO PARA MAPEO DE ACTIVOS
4. FORMATO DE MAPEO DE RIESGOS TI.