Contenido

1. INTRODUCCIÓN

La Empresa de Desarrollo y Renovación Urbano Sostenible de Santa Marta (EDUS) se complace en presentar este documento que establece las directrices esenciales para una administración del riesgo robusta y efectiva. Nuestro objetivo es asegurar que la entidad opere con la máxima eficiencia y eficacia, impulsando una mejora continua en cada uno de sus procesos.

Esta iniciativa busca generar una cultura de conciencia entre todos los servidores públicos. Es vital comprender que la materialización de cualquier riesgo puede impactar significativamente nuestras actividades, tanto las de misión fundamental como las administrativas, comprometiendo así el éxito institucional.

En este documento, encontrarán los lineamientos claros y prácticos sobre la gestión del riesgo: cómo identificar, calificar, administrar y proteger los valiosos recursos asignados. Al implementar estas pautas, la EDUS busca minimizar los reprocesos administrativos y garantizar una gestión que sea no solo eficiente, sino también altamente productiva al servicio de nuestros grupos de valor.

Cabe resaltar que esta política se basa sólidamente en el Modelo Integrado de Planeación y Gestión (MIPG) y se alinea con la guía vigente para la administración del riesgo y el diseño de controles en entidades públicas. Esto refuerza nuestro compromiso con el cumplimiento de la misión institucional y el logro de nuestros objetivos estratégicos y de proceso.

La política está estructurada para abordar de manera integral el objetivo, el alcance, los niveles de aceptación del riesgo, los criterios para calificar el impacto, las estrategias de tratamiento de riesgos, el seguimiento periódico según el nivel de riesgo residual y las responsabilidades de gestión para cada línea de defensa.

2. PROPÓSITO

El presente documento tiene como objetivo establecer el marco general de actuación para todos los servidores públicos de la EDUS, con el fin de asegurar la adecuada gestión de los riesgos y los potenciales escenarios de interrupción de la continuidad del negocio. Esto se materializará a través de la identificación de acciones de control, la implementación de respuestas oportunas y el

desarrollo de estrategias institucionales. Dichas medidas están diseñadas para mitigar las situaciones que puedan impactar negativamente el cumplimiento de la misionalidad y el logro de los objetivos institucionales, disminuyendo las potenciales consecuencias, reduciendo las vulnerabilidades frente a amenazas internas y externas, y fortaleciendo las capacidades de respuesta institucional ante eventos previstos o imprevistos que afecten el talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la entidad.

3. OBJETIVOS

3.1 Objetivo General

Establecer los **lineamientos específicos para la gestión del riesgo** en el desarrollo de la misión de la EDUS, asegurando el **logro de los objetivos estratégicos** definidos por la alta dirección.

3.2 Objetivos Específicos

1. Diseñar e implementar una metodología de gestión del riesgo actualizada y adaptada a la EDUS, que incluya procesos claros para la identificación, análisis, valoración, tratamiento y monitoreo de riesgos, en un plazo de 3 meses.
2. Capacitar al 100% de los servidores públicos clave de la EDUS involucrados en la gestión de procesos críticos, en el uso y aplicación de la metodología de gestión del riesgo, antes de 6 meses.
3. Realizar un mapeo y evaluación inicial de los riesgos inherentes a los procesos misionales y administrativos de la EDUS, identificando al menos los 5 riesgos más críticos en cada área, dentro de los 4 meses siguientes a la implementación de la metodología.
4. Desarrollar e implementar planes de tratamiento y control para los riesgos identificados como críticos, asignando responsabilidades claras y estableciendo indicadores de seguimiento, en un plazo de 8 meses.
5. Establecer un sistema de monitoreo y reporte periódico de la gestión del riesgo que permita a la alta dirección tomar decisiones informadas, generando informes trimestrales sobre el estado de los riesgos y la efectividad de los controles, a partir del tercer trimestre del año en curso.

4. ALCANCE

La Política de administración del riesgo inicia con la implementación de los lineamientos establecidos por la alta dirección en relación al tratamiento y manejo de los riesgos terminando en

la verificación y seguimiento de los mismos. Debe ser entendible y aplicable a cada uno de los procesos. Esta política de administración del riesgo contribuye al control interno de la entidad, y fomenta la cultura del autocontrol al interior de los procesos.

5. DEFINICIONES Y TERMINOLOGÍA

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. la gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

RIESGO: Posibilidad de ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impida el logro de sus objetivos.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CAUSA INMEDIATA: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

CAUSA RAÍZ: causa principal o básica, corresponde a las razones por la cuales se puede presentar el 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.

CONTINGENCIA: posible evento futuro, condición o eventualidad.

CONTINUIDAD DEL NEGOCIO: capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.

CRISIS: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

CIGD: Comité Institucional de Gestión y Desempeño.

DISPONIBILIDAD: propiedad de ser accesible y utilizable a demanda por una entidad.

Integridad: propiedad de exactitud y completitud.

MAPA DE RIESGOS: documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

MIPG: Modelo Integrado de Planeación y Gestión.

RESTABLECIMIENTO: capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele

considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

RIESGO 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 Fiscal: efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

RIESGO INHERENTE: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

RIESGO RESIDUAL: el resultado de aplicar la efectividad de los controles al riesgo inherente.

TIC: Tecnologías de la Información y las Comunicaciones.

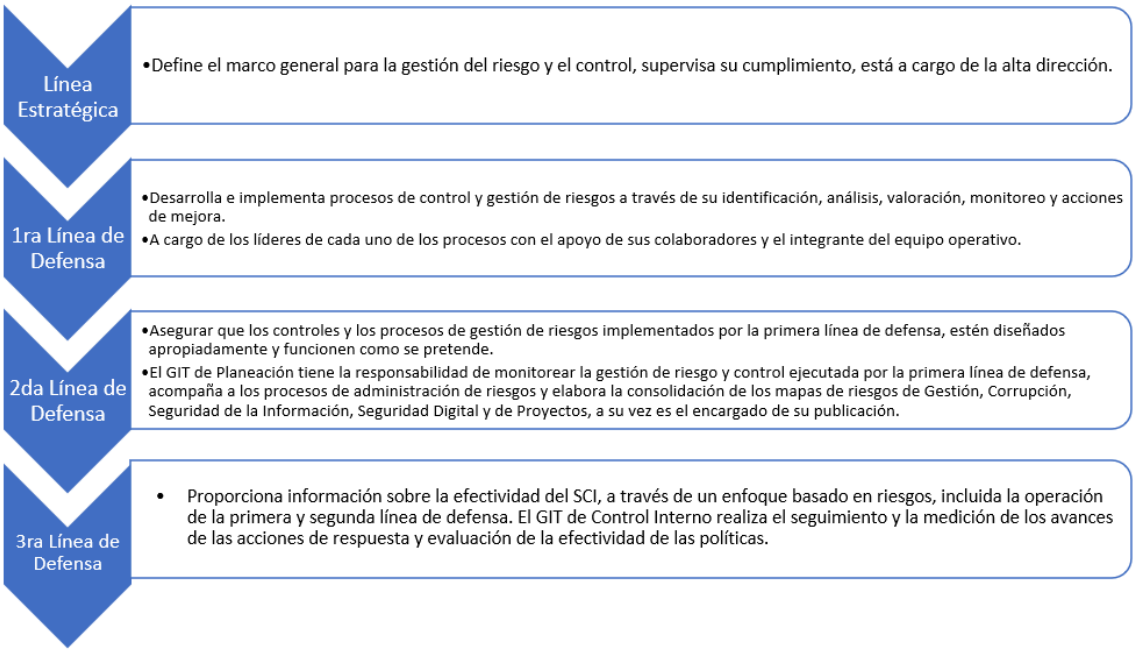
VULNERABILIDAD: representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. NORMATIVIDAD

Ley	**87**	1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones
Ley	1753	2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
Decreto	943	2014	Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015
Decreto	1537	2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado.
Decreto	124	2016	“Por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".

Decreto	1499	2017	"El Modelo Integrado de Planeación y Gestión - MIPG en su versión actualizada mediante el Decreto 1499 de 2017"
Guía	Versión 6	2022	"Guía para la Administración del Riesgo y el diseño de controles en entidades públicas "
Guía	Versión 3	2023	"Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces versión 3 septiembre 2023"

7. RESPONSABILIDADES



8. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgo de la EDUS, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía para la administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación

permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.

• Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

• Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

• Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

• Los riesgos fiscales impiden el daño sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública.

Cabe de destacar que la Función Pública determina que el módulo de riesgos del sistema de gestión institucional – SGI -, es la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, para lo cual la oficina asesora de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, cargue de información y dispone un manual de uso para el servicio de todos los procesos.

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

9. COMPROMISO CON LA POLÍTICA

La EDUS se compromete en el desarrollo de sus actividades a controlar todos aquellos riesgos que pueden impedir el cumplimiento de los objetivos institucionales y misionales por lo cual adoptara mecanismos y acciones tanto preventivas como correctivas para gestionarlos de manera integral mediante una efectiva administración de los mismos.

Estos mecanismos nos permitirán identificar, valorar, evidenciar y administrar los riesgos propios de cada proceso, procedimiento o proyectos contando con la participación activa de los servidores

públicos responsables de cada proceso, quienes serán los encargados para definir las acciones concretas para mitigar la materialización de los riesgos.

La Alta Dirección y sus dependencias adscritas, así como la participación del Comité de Coordinación de Control Interno de la EDUS, serán las encargadas de definir, establecer y mantener actualizada la presente política y llevar a cabo las actividades relacionadas a la valoración y asesoramiento de la gestión a nivel institucional.

Los líderes de cada proceso, responsables de dependencias, programas, planes y proyectos coordinarán el desarrollo e implementación de las metodologías a utilizar para administrar e identificar los riesgos y deberán ser actualizados según las necesidades evidenciadas por ellos.

La alta Dirección y Control Interno evaluarán los aspectos considerados como críticos tanto internos como externos que puedan llegar a representar algún tipo de amenaza para la consecución o logro de los objetivos estratégicos con miras a establecer acciones efectivas de control para la reducción del riesgo.

La Oficina de Planeación y TICS orientarán la metodología utilizada para la administración del riesgo y la consolidación de los mapas y/o matriz de riesgos por procesos de gestión, digitales y de corrupción que se pueden presentar en la Entidad.

10. NIVELES DE ACEPTACIÓN DEL RIESGO

De acuerdo con los riesgos residuales aprobados por los líderes de procesos y socializados en el Comité Institucional de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

Cabe destacar que de acuerdo a los lineamientos del Departamento Administrativo de la Función Pública, los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

11. VALORES:

HONESTIDAD: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.

RESPETO: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

COMPROMISO: Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

DILIGENCIA: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.

JUSTICIA: Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

12. PRINCIPIOS:

VOCACIÓN DE SERVICIO: Tengo la disponibilidad de atender a mis compañeros y al ciudadano, para serles útil y siempre estar con disposición para satisfacer y atender sus necesidades.

EQUIDAD: Me comprometo a trabajar activamente para desafiar y responder a los prejuicios, el acoso y la discriminación, acatando las políticas de igualdad de oportunidades para todas las personas.

LENGUAJE CLARO: Me comunico de forma clara, fluida, precisa, completa, confiable y afable con una actitud abierta y comprensiva al informar y dialogar con las personas, facilitando y garantizando la comprensión y su satisfacción.

INCLUSIÓN: Comprendo, respeto y actúo para integrar a todas las personas en la sociedad, con el objetivo de que puedan participar y contribuir en ella, beneficiarse; y realizarse como individuos.

DIVERSIDAD: Promuevo la participación e integración en la sociedad de la pluralidad de personas, sin distingo de diferencia étnica, cultural, sexual, biológica, etc.

13. LINEAS DE DEFENSA

En el modelo de las Tres Líneas de Defensa, el control de la gerencia es la primera línea de defensa en la gestión de riesgos; las varias funciones de supervisión de riesgos, controles y cumplimiento establecidas por la administración, son la segunda línea de defensa; y el aseguramiento

independiente es la tercera. Cada una de estas "líneas" juega un papel distinto dentro del marco amplio de gobernabilidad de la organización.

Modelo Línea de Defensa.

En el sistema de gestión de riesgos se considera que las funciones esenciales de la alta dirección son los principales interesados en ser atendidos por las "líneas", y son las partes que mejor están posicionadas, en donde la alta dirección debe rendir cuentas y son responsables por la fijación de objetivos de la entidad, la definición de estrategias para alcanzar dichos objetivos, y el establecimiento de estructuras de gobierno corporativo y procesos para gestionar mejor los riesgos en el cumplimiento de esos objetivos.

El modelo de las Tres Líneas de Defensa se implementa mejor con el apoyo activo y guía de alta dirección de la Entidad.

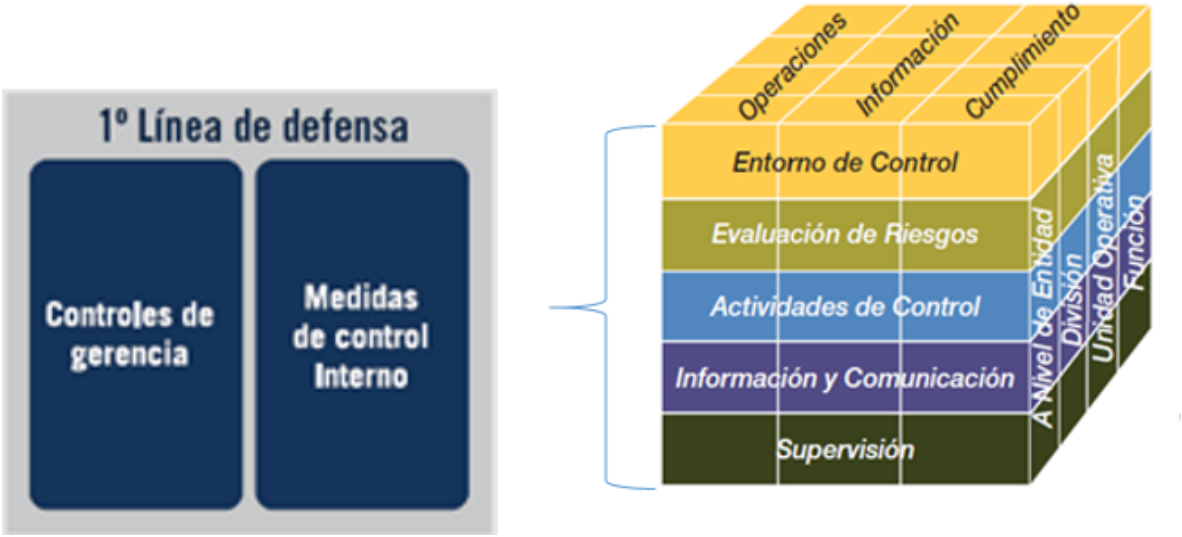
13.1 LA PRIMERA LINEA DE DEFENSA: LA GESTION OPERATIVA

Como primera línea de defensa, las gerencias operativas son propietarias de los riesgos y los gestionan, también son responsables de la implementación de acciones correctivas para hacer frente a deficiencias de proceso y control; y, de mantener un control interno efectivo y de ejecutar procedimientos de control sobre los riesgos de manera constante en el día a día.

Así mismo identifica evalúa, controla y mitiga los riesgos, guiando el desarrollo e implementación de políticas y procedimientos internos que aseguren que las actividades efectuadas son consistentes con las metas y objetivos.

A través de una estructura de responsabilidad distribuida en cascada, los gerentes de nivel medio diseñan e implementan procedimientos detallados que sirven como controles y supervisan la ejecución de tales procedimientos por parte de sus empleados; además sirve naturalmente como primera línea de defensa porque los controles están diseñados dentro de los sistemas y procesos bajo su dirección como administración operacional.

Deberían estar implementados adecuados controles de gestión y supervisión para asegurar su cumplimiento y para destacar excepciones de control, procesos inadecuados y eventos inesperados.



Primera Línea de Defensa

13.2 SEGUNDA LINEA DE DEFENSA: FUNCIONES DE GESTIÓN DE RIESGOS Y CUMPLIMIENTO

La entidad establecerá diversas funciones de gestión de riesgos y cumplimiento para ayudar a crear y/o monitorear los controles de la primera línea de defensa. Las funciones típicas de esta segunda línea de defensa comprenden:

- Una función de gestión de riesgos (y/o comité) que facilita y monitorea la implementación de prácticas efectivas de gestión de riesgos por parte de la gerencia operativa y que asiste a los propietarios del riesgo en la definición del objetivo de exposición al riesgo y en la presentación adecuada de información relacionada con riesgos a toda la organización.

- Una función de cumplimiento para monitorear diversos riesgos específicos tales como el incumplimiento de leyes y regulaciones aplicables. Con esta capacidad, esta función independiente reporta directamente a la alta dirección.

- Una función de contraloría que monitorea riesgos financieros y la emisión de la información financiera.

Cada una de estas funciones tiene algún grado de independencia respecto de la primera línea de defensa, pero son por naturaleza funciones gerenciales. Como funciones gerenciales, pueden intervenir directamente en la modificación y desarrollo de los sistemas de control interno y riesgos.

Por lo tanto, la segunda línea de defensa tiene un propósito vital, pero no puede ofrecer análisis del todo independientes a los organismos de gobierno corporativo respecto a la gestión de riesgos y a los controles internos.

Las responsabilidades de estas funciones varían según su naturaleza específica, pero pueden incluir:

• Apoyar en la administración de políticas en cuanto a la definición de roles y responsabilidades y el establecimiento de objetivos para su implementación.

• Proporcionar marcos para la gestión de riesgos.

• Identificar asuntos conocidos y emergentes.

• Identificar cambios en el apetito de riesgo implícito de la organización.

Asistir a la administración en el desarrollo de procesos y controles para la gestión de riesgos y problemas.

• Proporcionar guía y entrenamiento en procesos de gestión de riesgos.

• Facilitar y monitorear la implementación de prácticas efectivas de gestión de riesgos por parte de la gerencia operativa

• Alertar a la gerencia operativa de asuntos emergentes y de cambios en los escenarios regulatorios y de riesgos.

• Monitorear la adecuación y efectividad del control interno, la exactitud e integridad de la información, el cumplimiento de las leyes y regulaciones, y la remediación oportuna de deficiencias.

Segunda Línea de Defensa

13.3 TERCERA LINEA DE DEFENSA: AUDITORIA INTERNA

Los auditores internos proporcionan un aseguramiento comprensivo basado en el más alto nivel de independencia y objetividad al interior de la Entidad. Los auditores internos proveen aseguramiento sobre la efectividad del gobierno corporativo, la gestión de riesgos y el control interno, incluyendo la manera en que la primera y segunda línea de defensa alcanza sus objetivos de gestión de riesgos y control.

El alcance de este aseguramiento, que es reportado a los organismos corporativos de gobierno y alta dirección, usualmente cubre:

• Un amplio rango de objetivos, incluyendo la eficiencia y efectividad de las operaciones, salvaguarda de activos, confiabilidad e integridad de los procesos de reporte, y cumplimiento con leyes, regulaciones, políticas, procedimientos y contratos.

• Todos los elementos de los marcos de gestión de riesgos y control interno, que incluyen: ambiente de control interno, todos los componentes del marco de gestión de riesgos de la organización (por ejemplo, identificación de riesgos, evaluación de riesgos y respuesta), información y comunicación, y monitoreo.

• La entidad en su conjunto, divisiones, subsidiarias, unidades operativas y funciones – incluyendo procesos de negocios, tales como ventas, producción, marketing, seguridad, funciones de clientes, y operaciones – como también funciones de soporte (por ejemplo, contabilización de ingresos y gastos, recursos humanos, adquisiciones, remuneraciones, presupuestos, gestión de infraestructura y activos, inventario, y tecnología de la información).

Auditoría interna contribuye activamente a la efectividad del gobierno corporativo organizacional proporcionando ciertas condiciones – fomentando su independencia y profesionalismo – que se cumplan. La mejor práctica es establecer y mantener una función de auditoría interna independiente con personal adecuado y competente, lo cual incluye:

• Actuar en concordancia con las normas internacionales reconocidas para la práctica de la auditoría interna.

• Reportar a un nivel suficientemente alto para ser capaz de desempeñar sus funciones de manera independiente.

• Tener una activa y efectiva línea de reporte con los organismos de gobierno corporativo.

13.4 COORDINACION DE LAS TRES LINEAS DE DEFENSA

Debido a que cada organización es única y puede variar según situaciones específicas, no hay una forma "correcta" para coordinar las Tres Líneas de Defensa. Sin embargo, al asignar las responsabilidades específicas y de coordinación entre las funciones de gestión de riesgos, puede ser útil tener en cuenta el papel fundamental de cada grupo en el proceso de gestión de riesgos.

PRIMERA LINEA DE DEFENSA	SEGUNDA LINEA DE DEFENSA	TERCERA LINEA DE DEFENSA
Propiedad/Gestión de Riesgos	**Control de Riesgos y Cumplimiento**	**Aseguramiento de Riesgos**
• Gerencia operativa	• Independencia Limitada • Reportes principalmente a la gerencia	• Auditoría Interna • Mayor Independencia • Reportes a los organismos de gobierno corporativo

13.5 RESPONSABILIDADES DE LAS LINEAS DE DEFENSA

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE DEL RIESGO
Línea Estratégica	Comité Directivo Comité de Gestión y Desempeño Institucional	Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo en diferentes ámbitos institucionales. Generar recomendaciones de mejora a la política de administración del riesgo para su análisis e inclusión.
	Comité Directivo Comité de Gestión y Desempeño Institucional	Aprobar la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización. Evaluar la eficacia de la política frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. Monitorear los riesgos críticos identificados (aquellos definidos en los niveles de

		severidad Alto y Extremo, independientemente de su nivel de probabilidad), mediante el análisis de eventos o materializaciones u otra información aportada por las instancias de 2ª línea identificadas. Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios, a partir de la información aportada por las instancias de 2ª línea identificadas. Garantizar el cumplimiento de los planes institucionales, estratégicos y sectoriales de la entidad.
	Líderes de Procesos	El líder del proceso debe: Promover al interior de su equipo de trabajo el concepto de “administración de riesgo”, iniciando por la socialización de la política, su metodología allí desplegada y el marco de referencia de Función Pública aprobado por la línea estratégica. Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos.

Primera Línea	Responsable del proyecto Servidores en general	Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. Revisar de acuerdo con su competencia y alcance la documentación del plan continuidad del negocio. Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. En caso de materialización de un riesgo identificado, Informar a la oficina de planeación (segunda línea) y aplicar las acciones correctivas o de mejora necesarias. En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional, con el acompañamiento de la Oficina de Planeación.

		Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. Comunicar al equipo de trabajo los resultados de la gestión del riesgo. Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. Revisar y actualizar el mapa de riesgos con el acompañamiento de la Oficina de Planeación. Los servidores en general deben: · Participar en el diseño de los controles que tienen a cargo. Ejecutar los controles a su cargo de la forma como están diseñados. Informar a su superior jerárquico sobre riesgos materializados o posibles situaciones de afectación al proceso, a fin de incorporar las acciones a que haya lugar, incluyendo el informe a la Oficina de Planeación. Proponer mejoras a los controles existentes. El responsable del proyecto debe: Realizar la identificación de los riesgos del proyecto.

		Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Segunda Línea	Oficina Asesora de Planeación	Asesorar a la línea estratégica en el análisis del contexto interno y externo, incluyendo su actualización, acorde con los cambios en el entorno, la definición de la política de riesgo, el establecimiento de los riesgos al proceso de Direccionamiento acorde con los procesos definidos en el Nivel Estratégico de Función Pública del esquema de procesos actual, o bien el que lo actualice o sustituya cuando existan cambios en dicho esquema de operación. Identificar cambios en el entorno (interno o externo) que afecten el apetito del riesgo en la entidad, para su análisis en el Comité de Control Interno y se adelanten los ajustes que correspondan a este aparte dentro de la presente política. Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo con la asesoría de la Dirección de Gestión y Desempeño Institucional como líder de la política de control interno. 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 que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad. Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SGI. Revisar que el cargue de información en el SGI esté acorde con lo aprobado por el líder del proceso. Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CGDI. Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. Coordinar con los líderes de proceso el responsable de reporte de seguimiento a

		los riesgos, controles y planes de acción en el aplicativo SGI. Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso) y generar un reporte ejecutivo que permita establecer alertas a la Línea Estratégica sobre retrasos, incumplimientos u otras fallas detectadas. Socializar y publicar el mapa de riesgos institucional. Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados que se adelanten al interior de la entidad. Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional.

		Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SGI. Revisar que el cargue de información en el SGI esté acorde con lo aprobado por el líder del proceso. Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CGDI. Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y planes de acción en el aplicativo SGI. Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso.

		Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso) y generar un reporte ejecutivo que permita establecer alertas a la Línea Estratégica sobre retrasos, incumplimientos u otras fallas detectadas. Socializar y publicar el mapa de riesgos institucional. Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados que se adelanten al interior de la entidad. Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional. Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las

		acciones pertinentes para reducir la probabilidad o impacto de los riesgos.
Segunda Línea	Coordinador del Área de Planeación	El coordinador del Área de Planeación (o a quien delegue), mensualmente consolidará el avance sobre la planeación institucional de manera articulada con los temas asociados a los proyectos de inversión y otros requerimientos externos, generando alertas en semáforo sobre retrasos o posibles incumplimientos; al tiempo articulará la información sobre eventos (materializaciones de riesgo) asociados a los mismos permitiendo el análisis integral de la gestión del riesgo. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el coordinador del Área de Planeación como gestor del proceso de direccionamiento estratégico.
Segunda Línea	Secretaria General en articulación con el Área de Contratación	El coordinador de contratos mensualmente, consolida los avances del Plan Anual de Adquisiciones, de acuerdo a cada modalidad de contratación, generando alertas en semáforo frente a retrasos o posibles incumplimientos en los planes, programas o proyectos a los cuales se encuentran asociados los contratos analizados. La fuente para el análisis se basa en los informes de supervisión o interventoría (según corresponda) de los contratos en ejecución. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la

		Secretaria General como líder del proceso de gestión de recursos.
Segunda Línea	Secretaria General en articulación con el Coordinador de Talento Humano	El coordinador de TH, bimestralmente consolidará el avance sobre PIC, Bienestar, Incentivos y temas de convivencia laboral, mediante un análisis de variables relacionadas con la ejecución de cada uno de estos mecanismos, que permita generar alertas en la ejecución de recursos. En el tema de convivencia generar información sobre quejas reiteradas de acoso laboral, conflictos internos que no ha sido posible resolver y aquellos que llegan a instancia disciplinaria. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta la Secretaria General como líder del proceso de gestión del Talento Humano.
Segunda Línea	Coordinador de Servicio al Ciudadano	El coordinador del Grupo de Servicio al Ciudadano trimestralmente, evalúa la prestación del servicio a los grupos de valor, mediante el análisis de las PQRD y la evaluación de percepción de los usuarios por los diferentes medios de atención, generando alertas en semáforo sobre incumplimiento en términos, reiteraciones de consultas, quejas, denuncias y tutelas que se hayan presentado o que estén en curso. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Coordinador de Servicio al Ciudadano como líder del proceso de gestión del Servicio al Ciudadano.

		Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Segunda Línea	Área Jurídica	El coordinador del Área Jurídica, mensualmente, verifica el seguimiento a la gestión judicial adelantada por los abogados asignados, generando información sobre alertas en los procesos que se encuentran abiertos y las cuantías asociadas. La fuente de información es el sistema para la consulta de procesos de la Rama Juridicial, el sistema e-Kogui y los informes de los abogados responsables. El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Director Jurídico como líder del proceso de Defensa Jurídica. Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo.

		Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
Segunda Línea	Coordinador de la Oficina de Tecnologías de la Información y las comunicaciones TIC	Mensualmente verifica el avance en los programas y proyectos desagregados por tema y recursos asociados, generando alertas sobre retrasos o posibles incumplimientos, a fin de tomar las acciones o intervenciones necesarias. La fuente para el análisis son los informes de los supervisores o interventores de los programas a proyectos (según corresponda). El reporte se analiza en el Comité de Coordinación de Control Interno para definir acciones de mejora o intervenciones necesarias, información que aporta el Jefe de TIC como líder del proceso de Tecnologías de la Información.
Segunda Línea	Planeación TICs Gestión Administrativa Gestión de Talento Humano	Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando los escenarios. Actualizar la documentación que soporta la estrategia de continuidad del negocio. Identificar, valorar, evaluar y gestionar los riesgos de pérdida de continuidad del negocio. Liderar mesas de trabajo para la determinación del análisis de impacto del negocio, documentación de los escenarios de riesgos y plan de continuidad de negocio institucional. Actualizar, según se requiera, los escenarios de riesgos de continuidad y la documentación asociada al plan de

		continuidad de negocio bajo su responsabilidad. Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio.
Segunda Línea	Contratación Área Administrativa Área Financiera, Servicio al Ciudadano Gestión Documental, Talento Humano Jurídica	Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. Participar en las pruebas del plan de continuidad del negocio y en la implementación. El Coordinador del Grupo de Defensa Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
		Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de

Segunda Línea	TICS PLANEACIÓN	controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. Participar en las pruebas del plan de continuidad del negocio y en la implementación.
Segunda Línea	ÁREA DE PROYECTOS	Identificar y documentar un manual de gerencia de proyectos para el DAFP que contenga la guía para la gerencia de los proyectos institucionales, conjunto de buenas prácticas y estándares para la dirección de los proyectos. Identificar, documentar y formalizar políticas, procedimientos, instructivos y formatos para el adecuado funcionamiento de las labores de dirección de proyectos. Generar espacios de transferencia y gestión de conocimiento que faciliten el desarrollo de competencias y habilidades en el personal encargado de la gestión de proyectos en la Entidad.

		Generar espacios de trabajo para que los directores de proyecto compartan recursos de conocimiento para mejorar las posibilidades de éxito de los proyectos. Apoyar a las dependencias en las actividades de formulación, planificación, seguimiento y control a la ejecución y cierre de los proyectos bajo su responsabilidad, así como la identificación, diseño de controles y gestión de los riesgos de los proyectos y sus seguimientos. Monitorizar el avance global de los proyectos de la entidad para identificar amenazas y oportunidades que puedan afectar el cumplimiento de los objetivos de proyecto. Mantener información actualizada sobre el avance, logros, dificultades y necesidades de los diferentes proyectos y presentar informes consolidados para el comité directivo institucional.
TERCERA LÍNEA	OFICINA DE CONTROL INTERNO	Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.

		Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. Recomendar mejoras a la política de operación para la administración del riesgo.

14. ESCENARIOS DE PERDIDA DE CONTINUIDAD

Los escenarios de riesgo corresponden a descripciones de situaciones que agrupa la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales. La Empresa de desarrollo y renovación urbano sostenible (EDUS), adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de la misionalidad de la Entidad.

Cuando

Escenario	Descripción
Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómenonatural o fuerza mayor.
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicioso generar los productos.
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

se presentan eventos que materializan uno o más de los escenarios de continuidad de la misionalidad de la Entidad, evalúa las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en los mapas de riesgos para dar respuesta a la misma.

15. ETAPAS PARA LA GESTIÓN DEL RIESGO

PROBABILIDAD		IMPACTO		
Categoría	**Descripción**	**Categoría**	**Descripción Cuantitativa**	**Descripción Cualitativa**
NIVEL 5. CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias - Más de 1 vez al año.	**NIVEL 5. 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 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.
NIVEL 4. PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias - Al menos 1 vez en el último año.	**NIVEL 4. 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.
NIVEL 3. POSIBLE	El evento podrá ocurrir en algún momento - Al menos 1 vez en los últimos 2 años.	**NIVEL 3. 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.
NIVEL 2. IMPROBABLE	El evento puede ocurrir en algún momento - Al menos 1 vez en los últimos 5 años.	**NIVEL 2. 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 ≤1% del presupuesto general de la entidad.	* Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
NIVEL 1. RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). - No se ha presentado en los últimos 5 años	**NIVEL 1. 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 ≤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.

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. Las diferentes etapas con sus entradas, instrumentos y resultados se describen en el Manual Metodología de Riesgos.

16. MEDICIÓN DE IMPACTO DE RIESGOS DE CORRUPCIÓN:

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con las preguntas la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

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

17. VALORACIÓN DE IMPACTO DE RIESGO DE SEGURIDAD DIGITAL:

Criterios de Impacto para Riesgos de Seguridad Digital			
Categoría	**Descripción Cuantitativa**	**Descripción Cualitativa**	**Nivel**
CATASTRÓFICO	Afectación en un valor igual o superior al 50%de la población. Afectación en un valor igual o superior al 50% del presupuesto de seguridad de la información en la entidad. Afectación muy grave del medio ambiente que requiere > 3 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particularde los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interésparticular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interésparticular de los empleados y terceros. Interrupción de las operaciones de la Entidad por más de cinco 5 días	5
MAYOR	Afectación en un valor igual o mayor al 20% e inferior al 50% de la población. Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de seguridad dela información en la entidad. 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 delos empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particularde los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interésparticular de los empleados y terceros. Interrupción de las operaciones de la Entidad entre 2 y 4 dias	4
MODERADO	Afectación en un valor igual o mayor al 10% y menor al 20% de la población. Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad dela información en la entidad. Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afectación moderada de la integridad de la información debido al interés particularde los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interésparticular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interésparticular de los empleados y terceros. Interrupción de las operaciones de la Entidad por un (1) día.	3
MENOR	Afectación en un valor igual o mayor al 1% y menor al 10%de la población. Afectación en un valor igual o mayor al 1% y menor al 10%del presupuesto de seguridad de lainformación en la entidad. 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. Interrupción de las operaciones de la Entidad hasta por 8 horas (1 jornada laboral)	2
INSIGNIFICANTE	Afectación en un valor menor al 1% de la población. Afectación en un valor menor al 1% del presupuesto de seguridad de la información en laentidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad No hay interrupción de las operaciones de la entidad	1

18. CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de la misionalidad se realiza mediante la valoración del

impacto percibido por los coordinadores de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de estos primeros a los que tienen un mayor impacto y de manera secuencia a los de menor impacto percibido.

Criterio	Descripción
Financiero	Nivel de pérdidas económicas
Reputacional	Nivel de pérdida de la confianza de los grupos de valor en la entidad
Legal / Regulatorio	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
Contractual	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales
Misional	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales.

19. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Tipo de Riesgo	Responsable	Acción

Riesgo de Corrupción	Líder de Proceso	● Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado. ● Una vez surtido el conducto regular establecidopor la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), tramitar la denuncia ante la instancia de control correspondiente. ● Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento. ● Efectuar el análisis de causas y determinar acciones preventivas y de mejora. ● Actualizar el mapa de riesgos.
	Oficina de Control Interno	● Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. ● Una vez surtido el conducto regular establecidopor la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. ● Informar a la segunda línea de defensa con el finde facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos

Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)	Líder de Proceso	● Proceder de manera inmediata a aplicar el plande contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso), documentar en el Plan de mejoramiento. ● Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso. ● Analizar y actualizar el mapa de riesgos. ● Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.
Riesgos de Gestión y Seguridad digital (Zona Baja)		● Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
Riesgos de Gestión y Seguridad digital (Zona Extrema, Alta y Moderada)	Oficina de Control Interno	● Informar al líder del proceso sobre el hecho encontrado. ● Informar a la segunda línea de defensa con el finde facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos ● Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. ● Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

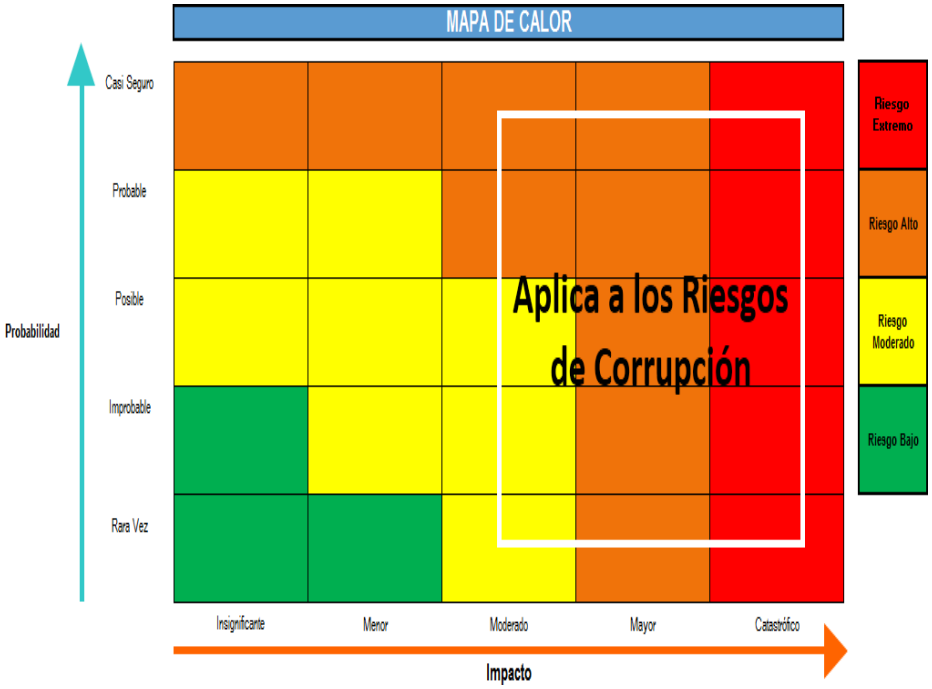
Riesgos de Proceso y Seguridad digital (Zona Baja)		• Informar al líder del proceso sobre el hecho. • Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, pararevisar el mapa de riesgos • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

20. ESTRATEGIAS PARA LA ACEPTACIÓN DEL RIESGO RESIDUAL

Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, así:

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de tratamiento
Riesgos de Gestión y Seguridad digital	Baja	Se **ACEPTA** el riesgo y se administra por
		medio de las actividades propias del proyecto
		o proceso asociado y se realiza en el reporte
		mensual de su desempeño.
		Se establecen acciones de control preventivasque
		permitan **REDUCIR** la probabilidad o el
	Moderada	impacto de ocurrencia del riesgo, se hace
		seguimiento **BIMESTRAL** y se registran sus
		avances en el Módulo de Riesgos- SGI
		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
	Alta y Extrema	materialización del riesgo. Se monitorea **MENSUALMENTE** y se registra en el Módulo de Riesgos – SGI
	Baja	Ningún riesgo de corrupción podrá ser aceptado. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos.
Riesgos de Corrupción	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra en el Módulo de Riesgos - SGI
		Se adoptan medidas para:
	Alta y Extrema	**REDUCIR** la probabilidad, el impacto o ambosfactores del riesgo; la estrategia conlleva a la implementación de controles. **EVITAR** Se abandonan o modifican las actividades que dan lugar al riesgo, decidiendono iniciar, no continuar o modificar de forma segura la actividad que causa el riesgo. **COMPARTIR** con un tercero el tratamiento de una parte del riesgo para reducir la probabilidad, el impacto o ambos factores. Periodicidad de seguimiento **MENSUAL** para evitar a toda costa su materialización por partede los procesos a cargo de estos y se registra en el Módulo de Riesgos - SGI



21. SEGUIMIENTO A LAS ACCIONES DE CONTROL DEL RIESGO A CADA PROCESO

- Según la periodicidad definida para cada riesgo, el delegado de riesgos en cada proceso y el líder de este verifica las acciones preventivas y registra el avance junto con la evidencia en el SGI.

- El delegado de riesgo en cada proceso y el líder de este analizan los resultados del seguimiento y establece acciones inmediatas ante cualquier desviación

- El líder del proceso comunica las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.

- El líder del proceso se asegura que se documenten las acciones de corrección o prevención en el plan de mejoramiento.

- El delegado de riesgo en cada proceso y el líder de este revisa y actualiza, con el acompañamiento de la OAP, el mapa de riesgo cuando se modifique las acciones o la ubicación del riesgo.

22. PERIODO DE REVISIÓN RIESGOS INSTITUCIONALES

Los riesgos se identifican y/o validan en cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción institucional, asegurando la articulación de éstos con los compromisos de cada proceso.

23. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

Función Pública determina que el Módulo de Riesgos del SGI es la herramienta para identificar, valorar, evaluar y administrar los riesgos, de corrupción y de seguridad digital, por tanto, toda información asociada con los riesgos es provista por dicha herramienta, para lo cual el área encargada identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información y dispone un manual de uso para el servicio de todos los procesos.

24. EVALUACIÓN

La evaluación del riesgo nos permitirá comparar los resultados de calificación dado al riesgo a través de los criterios definidos por el equipo de trabajo de cada proceso para establecer el grado de exposición en la entidad de esta forma es posible clasificar los riesgos en aceptables o inaceptables, tolerables, moderados y así poder fijar las prioridades que se deben tomar para su tratamiento.

En relación a preservar los recursos públicos se deberá verificar y evaluar los riesgos de corrupción y fraude consolidados en la matriz de corrupción cada tres meses con el fin de contar con una trazabilidad respecto al tema y así conocer la eficacia de los diferentes controles adoptados por cada líder de proceso.

25. BITÁCORA

	Nombre	Cargo	Firma
Elaboró	Jorge De La Hoz Codina	Contratista	

EDUS Empresa de Desarrollo y Renovación Urbano Sostenible — ALCALDÍA DE SANTA MARTA Distrito Turístico, Cultural e Histórico	Macroproceso Estratégico	Código: MCO-G01
		Versión: 1
	POLITICA ADMINISTRACIÓN DE RIESGO 2025	Fecha: Enero 2025

Aprobó	Jorye Luis Sarmiento	Gerente	
Revisó	Carlos Marchena Acosta	Jefe Control Interno	