INTRODUCCIÓN

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación , tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales, tomando como referencia las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la administración del riesgo de la Función Pública y el Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

DECLARACIÓN DE POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Empresa para la Seguridad y Soluciones Urbanas - ESU, se compromete a administrar adecuadamente los riesgos de gestión, de corrupción, de Seguridad Digital y fiscales, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, acatando la metodología propia para su gestión, determinando las acciones de control detectivos y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables.

OBJETIVO

Establecer el marco general de actuación de todos los servidores públicos de la ESU para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencia negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas y mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la ESU.

ALCANCE

La política de administración de riesgos es aplicable a todos los servicios, procesos, proyectos y planes de la ESU durante el desarrollo de la gestión planificada y a todos los servidores y personal de apoyo en el ejercicio de sus funciones.

TERMINOS Y DEFINICIONES

- **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Probabilidad:** Entendida como la posibilidad del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: Número de veces en un tiempo determinado) o de factibilidad teniendo en cuenta la presencia de factores internos y externos.
- **Impacto:** Consecuencias o resultados de un evento que afecta los objetivos
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.
- **Plan Anticorrupción y de Atención al Ciudadano:** plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.
- **Integridad:** propiedad de exactitud y completitud.
- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Activo:** Elemento que tiene valor para la organización, en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, tecnología de la información TI, Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.
- **Control:** Es una medida que modifica el riesgo. Puede incluir procesos, políticas, programas, proyectos, prácticas u otras acciones para mitigar. Los controles pueden generar efectos sobre las causas (prevenir la materialización) o sobre los impactos (reducir las consecuencias)
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

- **Control fiscal Interno (CFI):** Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público.
- **Control Fiscal Multinivel:** Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación del control social.
- **Riesgo Fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial
- **Efecto:** es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- **Evento Potencial:** Hechos inciertos o incertidumbres, refiriéndonos a riesgos, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. El evento potencial es equivalente a la causa raíz.
- **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo (punto de riesgo). Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- **Control Detectivo:** Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo (punto de riesgo). Estos controles detectan el riesgo fiscal, pero generan reprocesos.
- Control Correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo (punto de riesgo) y después de que se materializa el riesgo fiscal. Estos controles tienen costos implícitos.
- **Identificación del riesgo:** proceso para determinar qué, cuándo, dónde, por qué y cómo podía suceder algo.
- **Analizar los riesgos:** proceso para comprender la naturaleza del riesgo y determinar su nivel.
- **Peligro:** fuente de daño potencial
- **Perdida:** cualquier consecuencia negativa
- **Riesgo:** efecto de la incertidumbre sobre los objetivos (positivos, negativos). hace referencia al evento que podría ocurrir, que tenga un impacto directo sobre el logro de los objetivos. también se define una acción u omisión que podría afectar la capacidad de la empresa para lograr los objetivos de los procesos o sus estrategias.
- **Mapa de riesgos:** herramienta metodológica que permite hacer un inventario de los riesgos de forma ordena y sistemática, definiéndolos, haciendo la descripción de cada uno de está asumiendo las posibles consecuencias.
- **Nivel de riesgo:** magnitud de un riesgo o de una combinación de riesgos, expresadas en términos de la combinación del impacto por la probabilidad
- **Causa:** corresponde a aquellas situaciones, falla o insuficiencia que contribuye a la materialización de un riesgo ya sea de forma aislada o conjunta
- **Evaluación del riesgo:** resultado obtenido en la matriz de calificación, evaluación y respuesta de los riesgos
- **Oportunidad:** es una circunstancia en la cual existe la posibilidad de lograr algún tipo de mejora o de obtener algún beneficio derivado del riesgo. de acuerdo con la nota 2, del numeral 6.1.2 de la ISO 9001, *"las oportunidades pueden conducir a la opción de nuevas prácticas, lanzamientos de nuevos productos, aperturas de nuevos mercados, acercamiento a nuevos clientes, establecimiento de asociaciones, utilización de nuevas tecnologías y otras posibilidades deseables y viables para abordar las necesidades de la organización o de sus clientes"*
- **Acciones:** es la aplicación concreta de las opciones de manejo del riesgo que entran a prevenir o reducir el riesgo y lo harán parte del plan de manejo del riesgo.
- **Responsables:** son los procesos o dependencias encargadas de adelantar las acciones propuestas.
- **Beneficio:** resultado de la gestión de oportunidades reflejado en mejoras, ventajas, rendimientos, aumento del desempeño, utilidades, eficiencia, eficacia, satisfacción, entre otros.
- **Método (matriz de PxI):** Es una descripción cuantitativa de la posibilidad del riesgo por la consecuencia, cuyo análisis depende de diversos grados de detalle (el contexto, necesidades y expectativas de partes interesadas, datos y recursos)

RESPONSABILIDADES Y ROLES

La responsabilidad está definida mediante las líneas de defensa y en la ESU se acogen según la siguiente tabla:

líneas de Defensa	Responsable	Responsabilidad Frente al Riesgo
Línea estratégica	Junta directiva Gerente (Alta Dirección) Comité Institucional de Coordinación de Control Interno CICCI. Comité Institucional de Gestión y Desempeño	• Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico. • Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realizar seguimiento y análisis periódico a los riesgos institucionales • Realimentar al Comité Institucional de Gestión y Desempeño CIGD sobre los ajustes que se deban hacer frente a la gestión del riesgo.
Primera Línea de Defensa	Equipo Directivo, Líderes de procesos, servidores públicos en general en todos los	• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del

	niveles de la organización	daño antijurídico. • Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Hacer ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Reportar en los indicadores de gestión, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Informar a la Oficina estratégica - Planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo.
Segunda Línea De Defensa	Jefe Oficina estratégica (Planeación Estratégica y Equipo TI.) Comité de Contratación Subgerente Administrativa y financiera	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño CIGD. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Supervisar, en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones. • Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • 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 de negocio y en la implementación • Secretaría General 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
	Planeación Estratégica	• Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado. • Capacitar al grupo de trabajo de cada dependencia en la herramienta del SIG para la operación y gestión del riesgo. • Liderar las mesas de trabajo de identificación del riesgo • Liderar las mesas de trabajo para determinación del análisis de impacto del negocio, documentación de los escenarios de riesgo y plan de continuidad de negocio institucional. • Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología. • Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SIG. • Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo y socializarlos al interior de la dependencia • Revisar que el cargue de información en el SIG esté acorde con lo aprobado • Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso, con los riesgos altos, extremos y de corrupción.

	Delegados de Riesgos/ Líderes de calidad	• Comunicar al Equipo de trabajo a su cargo la responsabilidad y resultados de la Gestión del Riesgo • Apoyar en el monitoreo los riesgos identificados y controles establecidos • Apoyar en los reportes al Proceso de Evaluación y control, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar. • Asegurar que al interior de su grupo de trabajo se reconozca el concepto de administración del riesgo, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa. • Delegar, por parte del líder de calidad, los servidores que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.
Tercera Línea de Defensa	Dirección de Auditoría Interna.	• Evaluar la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar de forma coordinada con Planeación estratégica y con la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno CICCI. • Recomendar mejoras a la política de operación para la administración del riesgo

ESCENARIOS DE PÉRDIDA 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 ESU adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de negocio.

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.
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a casos fortuitos, fenómenos naturales o fuerza mayor
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios.
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la ESU 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.

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio, la ESU evalúa las características de la emergencia para autorizar la activación de estratégicas para la 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 para dar respuesta a la misma.

ETAPAS PARA LA GESTIÓN DEL RIESGO

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 procedimiento de Gestión de Riesgos.

TABLAS CALIFICACIÓN IMPACTO

Las tablas de calificación del Impacto definidas para los Riesgos de Procesos (Gestión), fiscales y Seguridad Digital se definen así:

PROBABILIDAD				
Nivel	**Frecuencia de la Actividad**	**Mínimo**	**Máximo**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	0	2	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	3	24	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	25	500	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 veces por año	5001	5000	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año	5001		100%

IMPACTO			
Nivel	**% Impacto**	**Afectación Económica**	**Reputacional**
Leve	20%	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.
Catastrófico	100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Las tablas de calificación del Impacto definidas para los Riesgos de corrupción se definen así:

NIVELES DE ACEPTACIÓN DEL RIESGO

De acuerdo con los riesgos residuales aprobados por el Equipo directivo y lideres de proceso y la socialización de estos en el Comité institucional de Coordinación de Control Interno, se define la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados:

- Para los riesgos residuales de Procesos (Gestión) y Seguridad Digital en zonas bajas, la ESU aceptara el Riesgo y no requiere documentar planes de acción; de igual manera se debe realizar monitoreos de acuerdo con las periodicidades establecidas.
- Para los riesgos de corrupción no hay aceptación del riesgo, siempre se realizarán acciones de fortalecimiento.

GESTIÓN DE RIESGOS DE PROCESOS

La empresa para la Seguridad y soluciones Urbanas ESU realizará la gestión del riesgo de procesos de acuerdo con los siguientes lineamientos:

1. Realizará el análisis de contexto interno y externo e identificará las partes interesadas pertinentes (necesidades y expectativas), como elemento de entrada para la identificación del riesgo.
2. Para la gestión del riesgo se dará cumplimiento a los siguientes principios como elementos que enmarcan la gestión efectiva de los mismos:

- Pensamiento basado en riesgos
- Responsabilidad compartida
- Enfoque estratégico
- Gestión transparente y participativa
- Tolerancia cero a la corrupción

3. Establecerá la metodología y herramienta de acuerdo con los lineamientos establecidos por el DAFP, la ISO 31000 e ISO 9001, proporcionando como instrumento de orientación que contemple las etapas de identificación, valoración, análisis y evaluación.
4. Para la identificación de los riesgos por proceso se debe tener presente el objetivo del proceso alcance y actividades del PHVA.
5. La valoración del riesgo estará enmarcada en la probabilidad e impacto de acuerdo con la tabla de valoración y herramientas metodológicas determinadas por el DAFP e ISO 31000, lo cual permite la identificación de controles adecuados establecidos en la operación de cada proceso.
6. Los mecanismos de evaluación y seguimiento se establecerán de acuerdo con los controles establecidos para determinar la eficacia del riesgo inherente en relación con el residual.
7. Los directivos, lideres de procesos y de calidad, con el apoyo de Planeación estratégica, revisara y actualizara periódicamente los riesgos de acuerdo con los cambios o mejoras gestionados en el proceso; al menos una vez al año o cuando las condiciones internas o del entorno lo requieran.
8. En el comité institucional de gestión y desempeño se tomarán decisiones de acuerdo con la gestión de los riesgos de proceso

GESTIÓN RIESGOS DE CORRUPCIÓN

1. La ESU es responsable de identificar los riesgos de corrupción en el marco de su Misión como entidad Industrial y Comercial del Estado
2. La ESU elabora anualmente el mapa de riesgos de corrupción.
3. Planeación estratégica es la responsable de gestionar el riesgo, liderando el proceso de administración de estos, para finalmente consolidar el mapa de riesgos de corrupción.
4. El mapa de riesgos de corrupción de la ESU se publicará en la página web de la entidad, en la sección de transparencia y acceso a la información pública, según lo estipulado en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015, o en otro medio de fácil acceso para los ciudadanos, a más tardar el 31 de enero de cada año
5. El proceso de Planeación Estratégica dará a conocer antes de su publicación a los servidores públicos y contratistas, el mapa de riesgos de corrupción. Planeación estratégica diseña y ejecuta actividades o mecanismos para que estos actores conozcan, debatan y formulen sus propuestas sobre el proyecto del mapa de riesgos de corrupción. Además, la misma oficina deberá facilitar la participación de la ciudadanía y otros interesados externos, permitiendo que conozcan y sugieran modificaciones al documento. Es importante dejar evidencia de la socialización.
6. Después de la publicación y durante el año de vigencia, se podrán realizar los ajustes y modificaciones necesarios para mejorar el mapa de riesgos de corrupción. Estos cambios deberán documentarse por escrito, en el marco del análisis del contexto organizacional.
7. En consonancia con la cultura del autocontrol dentro de la entidad, los líderes de los procesos y sus equipos realizarán un monitoreo y evaluación continua de la gestión de riesgos de corrupción.
8. El Director de Auditoría interna, o quien haga sus veces, debe llevar a cabo el seguimiento de la gestión de riesgos de corrupción. Esto incluye analizar, en los procesos de auditoría interna, las causas y riesgos de corrupción, así como la efectividad de los controles incorporados en el mapa de riesgos de corrupción. De la siguiente manera:

- Primer seguimiento será realizado con corte al 30 de abril, para ser publicado los 10 primero días del 10 de mayo.
- Segundo seguimiento se realizar con corte al 31 de agosto para ser publicado los 10 primeros días del mes de septiembre
- Tercer seguimiento se realizar con corte a 31 de diciembre, para ser publicado los 10 primero días del mes de enero

9. La medición del impacto de los riesgos de corrupción se realiza aplicando la metodología de valoración de acuerdo con los lineamientos establecidos por el DAFP, los cuales establecen criterios desde la etapa de identificación, hasta la evaluación de los controles; Dichos lineamientos se determinan en el procedimiento de la Entidad.
10. En el evento de materialización de Riesgos de corrupción se dará cumplimiento a los siguiente:

- Informar a las autorizades de la ocurrencia del hecho de corrupción
- Revisar el Mapa de riesgos de corrupción en particular, las causas, riesgos y controles
- Verificar si se tomaron las acciones y se actualizó el Mapa de riesgos de corrupción
- Llevar a cabo un monitoreo permanente

Nota: El Director de Auditoría interna debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando de forma oportuna y efectiva.

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Empresa para la Seguridad y Soluciones Urbanas ESU:

1. Determina lineamientos para la Gestión del Riesgo de le Seguridad de la información de acuerdo con los lineamientos de la Política de Seguridad digital y Gobierno Digital en el marco de MIPG, alineando esto a la arquitectura de TI, la cual se encuentra soportada en la seguridad de la información, arquitectura, servicios ciudadanos digitales
2. Identificará activos de seguridad de la información, debido a su compromiso en proteger y garantizar el funcionamiento interno y de cara al ciudadano, para aumentar su confianza en el entorno digital; como primer paso para la Gestión del riesgo, teniendo en cuenta los siguientes pasos:

- Listar activos por cada proceso

- Identificar el responsable del activo
- Clasificar activos
- Clasificar la información
- Determinar la criticidad del activo
- Identificar infraestructura critica cibernética

3. Para la identificación del riesgo inherente la orientación estará enmarcada en:

- Perdida de confidencialidad
- Perdida de la Integridad
- Perdida de disponibilidad

4. Analizará las posibles amenazas y vulnerabilidades que podría causar la masterización del riesgo identificado, la entidad podrá remitirse al Modelo nacional de gestión de riesgos de Seguridad de la información para entidades públicas, como material de apoyo para el análisis de amenazas comunes, amenazas dirigidas por el hombre y vulnerabilidades comunes.
5. Realiza la valoración del riesgo de acuerdo con las tablas de probabilidad e impacto, teniendo en cuenta para la probabilidad las frecuencias de la actividad y para el impacto la afectación económica y reputacional, lo cual se establece en el procedimiento de Gestión de Riesgo.
6. Determinará controles asociados a la Seguridad de la información, para lo cual se podrá apoyar en lineamientos establecidos en la ISO 27001 y el Modelo nacional de gestión del riesgo de Seguridad de la información en entidades públicas. Estos controles deben estar alineados a los procedimientos operacionales y responsables.
7. Se debe realizar seguimiento a los controles establecidos para determinar eficacia de estos, en caso de identificar debilidades se deberán fortalecer de acuerdo con la probabilidad y el impacto.
8. El equipo responsable de Tecnologías de la información realizará monitoreos y evaluaciones periódicas en el marco de los planes, estrategias y acciones establecidas para evitar la materialización de estos.
9. En el comité institucional de gestión y desempeño se tomarán decisiones de acuerdo con la gestión de los riesgos de seguridad de la información, tendiendo además en cuenta lo establecido en el decreto 612 de 2018.

GESTIÓN DE RIESGOS FISCALES

La Empresa para la Seguridad y Soluciones Urbanas ESU en aras de prevenir el daño al patrimonio público, representado en menoscabo, disminución, perjuicio, detrimento, perdida o deterioro, de los bienes o recursos públicos a los intereses patrimoniales del estado y la base de responsabilidad fiscal establecida en la ley 610 del 2000, se determina los siguientes lineamientos:

1. Para identificar el riesgo fiscal, se establecerán los puntos de riesgo fiscal y las circunstancias inmediatas. Los puntos de riesgo son situaciones en las que potencialmente se genera riesgo fiscal. Estas situaciones incluyen actividades relacionadas con: administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de bienes o recursos públicos, así como la recaudación, manejo e inversión de las rentas.
2. Para la identificación de puntos de riesgo fiscal y causas inmediatas la entidad se podrá apoyar en las metodologías establecida en la guía DAFP, además de tener claro el concepto de patrimonio público, bien público, recursos públicos e interés patrimonial.
3. Se debe identificar la causa raíz o potencial de hecho generador la cual se enmarca en la acción, omisión o acto lesivo. Esta identificación de causas debe ser objetiva y rigurosa, toda vez que lo controles se diseñan e implementan para acatar las mismas, y así prevenir la ocurrencia del daño fiscal
4. La redacción de riesgo fiscal debe tener en cuenta los siguientes parámetros:

- Posibilidad del evento potencial
- Impacto: corresponde al que/efecto dañoso sobre el recurso público bien o interés patrimonial
- Circunstancia inmediata: corresponde al cómo/situación por la que se presenta el riesgo
- Causa raíz: corresponde al porque/es el evento (acción u omisión)

5. Se realizará la valoración del riesgo fiscal de acuerdo con la probabilidad de ocurrencia, consecuencia o impacto inherente, teniendo presente la frecuencia de la actividad establecida a nivel de procedimiento y el impacto se debe definir con relación a la afectación económica y reputacional
6. La valoración de los controles debe estar orientadas a prevenir y detectar la materialización de los riesgos, los cuales pueden ser preventivos, detectivos o correctivos; además de asignar la responsabilidad del control.
7. Se debe determinar el nivel de riesgo residual, el cual corresponde a la evaluación del control relacionado al riesgo inherente.
8. El monitoreo y revisión de la gestión de riesgos, se realiza través de la asignación de responsabilidades y roles, en el marco de las líneas de defensa.
9. En el comité institucional de gestión y desempeño se tomarán decisiones de acuerdo con la gestión de los riesgos fiscales.

ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Frente a la materialización de un riesgo se debe medir el impacto y las consecuencias que pueden ocasionar afectación los objetivos de la ESU, se revisaran y ajustaran los controles asociados determinando el grado de efectividad, eficiencia o eficacia que asegure la mitigación de la ocurrencia. Para realizar el análisis de riesgos y sus controles se consideran los siguientes aspectos:

- Calificación del Riesgo: Estimación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo
- Bajo el criterio de probabilidad: Se mide el riesgo a partir de la cantidad de veces que se ejecuta cada una de sus acciones

En primera instancia se tomarán correcciones o medidas para disminuir la ocurrencia, lo cual se logra cuando en los procesos se realizan cambios sustanciales por mejoramiento, rediseño o eliminación, se ajustan controles y se ejecutan acciones.

COMUNICACIÓN Y CONSULTA

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

1. Cambios en el entorno
2. Alertas por cambios en niveles esperados de desempeño
3. Resultados del monitoreo, revisión y evaluación de riesgos.
4. Cambios asociados a: el ciclo de reporte, evaluación y valoración, controles, acciones, la determinación o no de tratar un riesgo, las actividades definidas, el o los responsables, etc.
5. La información resultante de la gestión, monitoreo y evaluación se realizará como minino dos veces en el año y debe ser publicada en la página web de la Entidad. Es de aclarar que se mantiene los periodos para el monitoreo y evolución de los Riesgos de corrupción por parte de Evaluación y control, cada cuatro meses.

CONTROL DE CAMBIOS

Versión	Fecha	Usuario	Comentario
2	18/02/2019	Marcela Salazar Valencia	Actualización periodo de evaluación
3	08/09/2021	Marcela Salazar Valencia	Revisión por parte del comité del SIG
4	07/02/2022	Marcela Salazar Valencia	Actualización versión 5 Guía administración del riesgo DAFP
5	18/11/2022	Luisa Rosalía Ríos Jorge	Actualización con nueva versión de la Guía del DAFP (Guía para la administración del riesgo y el diseño de controles en entidades públicas V5)
6	23/03/2023	Alvaro Torres	Se actualiza de acuerdo a la Guia rol de las oficinas de control interno o quienes hagan sus veces Versión 3.
7	02/01/2025	Juan Camilo Rincón Montoya	Actualización de política de administración del riesgo según los lineamientos del DAFP, actualización de riesgos fiscales ejemplificación de la valoración del riesgo.
8	05/02/2025	Valeria Mejia	Se actualiza por cambios en el mapa de procesos, cambiando el nombre de mejora continua a administración del sistemas integrados
9	04/06/2025	Valeria Mejia	Se eliminan los lineamientos del punto 2: Declaración de Política de Administración de Riesgos. - Se ajusta el alcance, delimitando a quiénes es aplicable la política. - Se actualizan los términos y definiciones. - Se modifican las responsabilidades y roles de acuerdo con el modelo de las líneas de defensa. - Se incorporan los escenarios de pérdida y continuidad. - Se alinea el contenido con los lineamientos del Departamento Administrativo de la Función Pública (DAFP).

ELABORÓ	REVISÓ	APROBÓ
Nathalia Sanchez Bedoya **Profesional Universitario Grado 1 - Comercial y Mercadeo** **Fecha de elaboración:** 26/05/2025	Valeria Mejia **Profesional Universitario Grado 1 - Gestión de Proyectos** **Fecha de revisión:** 30/05/2025	Lina Marcela Gomez Rendón **Jefe de Oficina Estrategica** **Fecha de aprobación:** 04/06/2025