POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

1. INTRODUCCIÓN

La Empresa para la Seguridad y Soluciones Urbanas – ESU, en cumplimiento de su misión institucional y con el propósito de fortalecer la capacidad para alcanzar sus objetivos estratégicos, desarrollar adecuadamente sus procesos y generar valor público, adopta la presente Política para la Gestión Integral del Riesgo, como marco de actuación para identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

La política se fundamenta en los principios y lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno – MECI, el esquema de líneas de defensa, la normatividad aplicable a la gestión pública y los lineamientos establecidos por el Departamento Administrativo de la Función Pública – DAFP en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, así como en las disposiciones aplicables a la gestión de riesgos de gestión, fiscales, seguridad de la información y riesgos para la integridad pública.

La gestión integral del riesgo se desarrollará bajo un enfoque preventivo, sistémico y basado en evidencia, articulado con la planeación institucional, la gestión por procesos, la gestión de proyectos, el control interno, la seguridad de la información, la continuidad de negocio y el Programa de Transparencia y Ética Pública – PTEP.

La presente política reconoce que la gestión del riesgo es una responsabilidad de todos los niveles de la organización y que su adecuada implementación requiere la participación coordinada de la línea estratégica, las líneas de defensa y los demás actores que intervienen en la gestión institucional.

2. DECLARACIÓN DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

La Empresa para la Seguridad y Soluciones Urbanas – ESU se compromete a gestionar integralmente los riesgos que puedan afectar el cumplimiento de sus objetivos estratégicos, institucionales, de procesos, proyectos y planes, mediante la identificación oportuna de eventos y factores de riesgo, el análisis de sus causas y consecuencias, la valoración de los niveles de exposición, el diseño e implementación de controles efectivos, la definición de respuestas y tratamientos adecuados, y el monitoreo, seguimiento, evaluación y comunicación permanente de sus resultados.

La ESU gestionará de manera articulada los riesgos de gestión, riesgos fiscales, riesgos de seguridad de la información y riesgos para la integridad pública, de acuerdo con las disposiciones legales y metodológicas aplicables a cada tipología.

En particular, la Empresa adopta un enfoque de tolerancia cero frente a los riesgos que afecten la integridad pública, incluyendo aquellos asociados con posibles actos de corrupción, fraude, soborno, conflictos de interés gestionados inadecuadamente y demás conductas que puedan afectar la moralidad administrativa y la confianza en la gestión pública.

La gestión integral del riesgo se orientará a la prevención, al fortalecimiento del ambiente de control, a la toma de decisiones basada en información y evidencia, y a la mejora continua de la capacidad institucional para responder ante eventos que puedan afectar el logro de los objetivos.

3. OBJETIVO

Establecer los lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo, y comunicación de los riesgos en la Empresa para la Seguridad y Soluciones Urbanas – ESU, que puedan afectar el logro de los objetivos estratégicos, en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos en materia de riesgos, establecidos por del Departamento Administrativo de la Función Pública - DAFP.

Esta política tiene como propósito fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, asegurando la integridad, la transparencia y eficiencia en la administración de recursos. Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua y la confianza ciudadana.

4. ALCANCE

La presente política es aplicable a todos los procesos, proyectos y programas de la ESU, así como a todos los servidores públicos y demás colaboradores que participen en la gestión institucional, de acuerdo con el ámbito de sus responsabilidades.

La gestión integral del riesgo deberá aplicarse desde la planeación de los procesos, proyectos y objetivos estratégicos y mantenerse durante todo su ciclo de gestión.

La política comprende las siguientes tipologías:

1. Riesgos de gestión.
2. Riesgos fiscales.
3. Riesgos de seguridad de la información.

4. Riesgos para la integridad pública, incluidos los asociados con corrupción, fraude, soborno, conflictos de interés y lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva.

Las particularidades metodológicas de cada tipología se desarrollarán en el procedimiento, instrumentos y demás documentos operativos que adopte la ESU, de conformidad con los lineamientos del Departamento Administrativo de la Función Pública – DAFP.

5. MARCO NORMATIVO

La gestión integral del riesgo de la ESU se desarrollará teniendo como referencia, entre otras disposiciones que resulten aplicables:

- Constitución Política de Colombia.
- Ley 87 de 1993.
- Ley 1474 de 2011.
- Ley 2195 de 2022.
- Decreto 1083 de 2015 y sus modificaciones.
- Decreto 1499 de 2017.
- Decreto 1122 de 2024, en lo relacionado con los Programas de Transparencia y Ética Pública.
- Modelo Integrado de Planeación y Gestión – MIPG.
- Modelo Estándar de Control Interno – MECI.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, DAFP, 2025.

6. RESPONSABILIDADES Y ROLES

La ESU adopta el Esquema de Líneas de Defensa como marco para definir responsabilidades frente a la gestión integral del riesgo.

6.1. Línea estratégica

Estará conformada por la Junta Directiva, Gerencia, Comité Institucional de Gestión y Desempeño – CIGD y el Comité Institucional de Coordinación de Control Interno – CICCI.

Le corresponde:

- Aprobar y revisar la Política para la Gestión Integral del Riesgo.
- Definir y revisar el apetito, tolerancia y capacidad de riesgo.
- Realizar seguimiento a los riesgos.
- promover una cultura institucional de gestión del riesgo.
- Analizar cambios significativos del contexto.
- Revisar los resultados de los Indicadores Clave de Riesgo - ICR.
- Promover la articulación entre planeación, gestión del riesgo y control interno.

6.2. Primera línea de defensa

Está conformada por los líderes de procesos, responsables de proyectos y servidores que participan directamente en la operación.

Le corresponde:

- Identificar y analizar los riesgos.
- Implementar y ejecutar los controles.
- Realizar el monitoreo periódico de los riesgos y controles.
- Conservar las evidencias de ejecución de los controles.
- Reportar oportunamente riesgos materializados.
- Implementar acciones de tratamiento.
- Actualizar los riesgos ante cambios en el contexto.
- Proponer mejoras a los controles.
- Identificar, formular y reportar información sobre Indicadores Clave de Riesgo - ICR.

6.3. Segunda línea de defensa

Está conformada por el área de Planeación que hace parte de la Oficina Estratégica.

Le corresponde:

- Mantener la metodología institucional.
- Orientar y capacitar a la primera línea de defensa.
- Consolidar la información institucional de riesgos.

- Monitorear la gestión realizada por la primera línea.
- Realizar seguimiento a los controles e Indicadores Clave de Riesgo – ICR.
- Promover el uso de indicadores clave de riesgo.
- Coordinar la actualización de los instrumentos institucionales.

6.4. Tercera línea de defensa

Está conformada por la Dirección de Evaluación y Control.

Le corresponde:

- Evaluar la eficacia de la gestión del riesgo.
- Evaluar el diseño y operación de los controles.
- Verificar la efectividad de las acciones implementadas.
- Evaluar pertinencia y eficacia de si los Indicadores Claves de Riesgo – ICR.
- Realizar auditorías basadas en riesgos.
- Efectuar seguimiento a la gestión de riesgos de acuerdo con el Plan Anual de Auditoría.

7. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DEL RIESGO

La ESU adoptará una metodología institucional única y articulada, ajustada a las particularidades de cada tipología de riesgo.

La metodología comprenderá, las siguientes etapas:

7.1. Establecimiento del contexto

Se analizarán los factores internos y externos de la entidad, objetivos institucionales y de proceso, partes interesadas, entorno, capacidades, recursos, cambios regulatorios, tecnológicos, económicos, sociales y demás factores que puedan generar riesgos.

7.1.1 Contexto Interno: estructura organizacional, cultura institucional, capacidad tecnológica, talento humano, procesos internos, recursos financieros, políticas internas y marco normativo aplicable.

7.2.2 Contexto Externo: entorno político, económico, social, ambiental y tecnológico; actores del sector, reguladores, organismos de control, ciudadanos y partes interesadas, así como riesgos asociados a cambios normativos y eventos externos. Sector donde opera la entidad y su relacionamiento con otras entidades e instancias necesarias para su gestión, así como entorno de desarrollo territorial.

7.2. Identificación y descripción del riesgo

Los riesgos deberán formularse de manera clara, precisa y verificable, identificando el evento, sus causas y sus posibles consecuencias.

La identificación deberá considerar, entre otras fuentes:

- Objetivos institucionales y de proceso.
- Análisis de contexto.
- Materialización de eventos anteriores.
- Auditorías.
- Informes de control.
- Indicadores.
- Peticiones, quejas y reclamos.
- Incidentes.
- Cambios normativos.
- Cambios tecnológicos.
- Riesgos emergentes.
- Conocimiento de los servidores y expertos.
- Información de las partes interesadas.

7.3. Análisis del riesgo inherente

Se determinará el nivel de exposición al riesgo antes de considerar la efectividad de los controles existentes, utilizando los criterios institucionales de probabilidad e impacto definidos en la metodología vigente.

7.3.1 Probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo y está asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad

inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.

Criterios para definir el nivel de probabilidad

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año.
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año.
Muy Alta - 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.

7.3.2 Impacto

Son las consecuencias que puede ocasionar a la entidad por la materialización de un riesgo. Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Criterios para definir el nivel de impacto

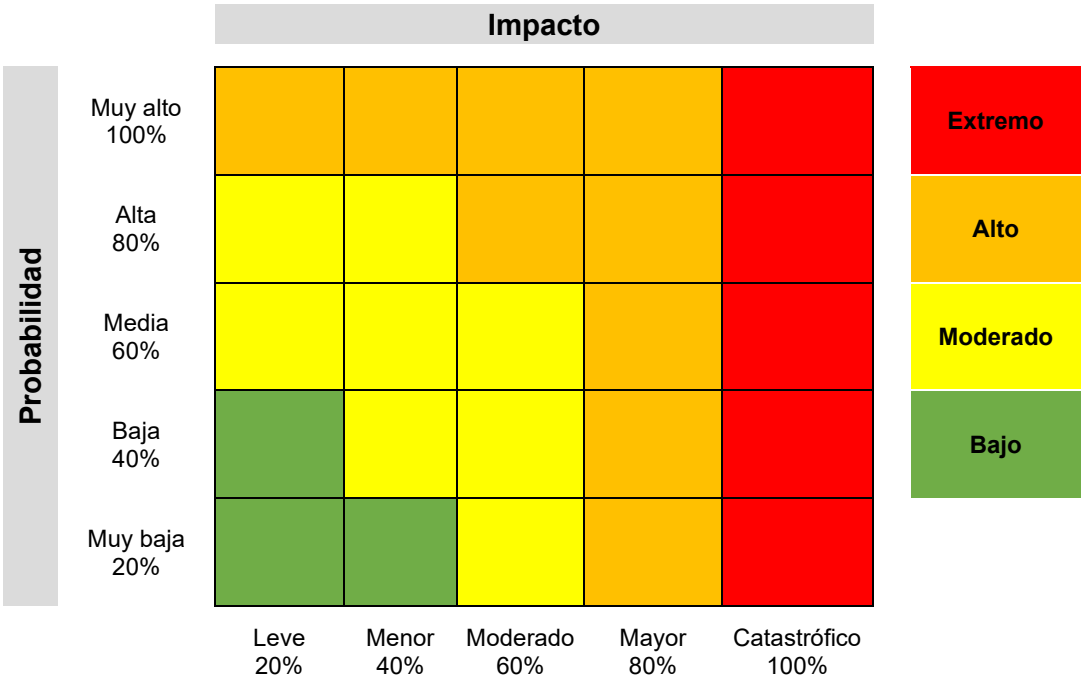
Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 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.

7.3.3 Mapa de calor

Los riesgos identificados y valorados se ubicarán en el mapa de calor, como herramienta gráfica para representar y facilitar la interpretación del nivel de riesgo, a partir de la combinación de los criterios de probabilidad e impacto establecidos en la metodología institucional.

En el mapa de calor, el eje horizontal corresponde al nivel de impacto y el eje vertical al nivel de probabilidad de ocurrencia. La intersección de ambos criterios determina el nivel de riesgo inherente y, posteriormente, el nivel de riesgo residual, una vez considerados los controles existentes y su efectividad.

Matriz de calor (niveles de severidad del riesgo)



7.4. Diseño, descripción y valoración de controles

Los controles deberán estar directamente relacionados con las causas del riesgo y contar en su descripción, como mínimo con: responsable, acción, documentación, frecuencia y evidencia.

7.4.1 Tipologías de controles

Control preventivo: accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Control detectivo: accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control correctivo: accionado en la salida del proceso y después de que se materializa el riesgo, estos controles tienen costos implícitos. Se debe tener en cuenta que los controles que se contemplan en esta tipología usualmente tienen que ver con pólizas de seguro, copias de seguridad (*backup*), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializad.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: ejecutados por personas.

Control automático: ejecutados por un sistema o software previamente programado o diseñado.

7.4.2 Valoración de los controles

La tabla aplicable para la valoración de controles que se muestra a continuación, determina la forma como se califican los atributos definidos en la tipología de los controles.

Características de eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
Implementación	Automático	25%
	Manual	15%

La estructura de la descripción del control no se aplica valoración, pero se debe analizar para asegurar su diseño.

En cuanto a su efecto sobre el riesgo, los controles preventivos y detectivos están orientados a disminuir la probabilidad de ocurrencia del riesgo, mientras que los controles correctivos están dirigidos a reducir el impacto.

7.5. Valoración del riesgo residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que, estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

7.6. Tratamiento del riesgo

Según el nivel de exposición y los criterios institucionales, se podrán adoptar opciones como:

- Reducir: Implementar controles para reducir la probabilidad o el impacto.

- Compartir: Transferir a un tercero el riesgo, cuando jurídicamente y operativamente resulte procedente.
- Aceptar: Cuando se tolera el nivel de riesgo de una actividad. Para los riesgos asociados con la integridad pública, la ESU establece que no serán aceptables riesgos relacionados con corrupción, fraude, soborno, conflictos de interés gestionados inadecuadamente y demás conductas que afecten la integridad pública.

  La gestión deberá orientarse a prevenir su ocurrencia, fortalecer los controles y adoptar las acciones correspondientes ante cualquier señal, alerta o materialización.
- Evitar: Cuando se decide no ejecutar la actividad que conlleva el riesgo.

8. TIPOLOGÍAS DE RIESGO

8.1. Riesgos de gestión

Los riesgos generales de la gestión corresponden a aquellos eventos potenciales, internos o externos, que pueden afectar el cumplimiento de los objetivos institucionales, estratégicos y de los procesos de la ESU, así como la ejecución de sus planes, programas, proyectos, contratos, productos, servicios y demás instrumentos de gestión.

Estos riesgos se encuentran asociados principalmente a la operación de la entidad y son propios de sus procesos, funciones, actividades y misionalidad. Su identificación y gestión deberán considerar las particularidades de la ESU, su estructura organizacional, modelo de operación por procesos, recursos disponibles, grupos de valor, contexto interno y externo, así como las actividades clave requeridas para el cumplimiento de sus objetivos.

Estos riesgos serán sometidos a las etapas de identificación y descripción, análisis del riesgo inherente, diseño y análisis de controles y valoración del riesgo residual, de acuerdo con la metodología definida en el punto 7 de la presente política y los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo V7 del Departamento Administrativo de la Función Pública – DAFP, la cual mantiene una estructura metodológica común para la gestión integral de las diferentes tipologías de riesgo.

8.2. Riesgos fiscales

Los riesgos fiscales corresponden a aquellos eventos potenciales que, en desarrollo de las actividades de gestión fiscal de la ESU, pueden generar un efecto dañoso sobre los recursos públicos, los bienes públicos o los intereses patrimoniales de naturaleza pública.

Su gestión tendrá especial énfasis en la identificación de puntos de riesgo fiscal, circunstancias inmediatas y causas raíz, así como en la implementación de controles orientados a prevenir la ocurrencia de daño al patrimonio público.

8.2.1. Definición y elementos del riesgo fiscal

El riesgo fiscal se define como el efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Efecto dañoso: es el daño que se generaría sobre los recursos, los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos, los bienes y/o los intereses patrimoniales de naturaleza pública

No se debe confundir el riesgo fiscal con el daño patrimonial. El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

8.2.2. Metodología para el levantamiento del mapa de riesgos fiscales

El levantamiento del mapa de riesgos fiscales de la ESU se realizará de manera articulada con el mapa institucional de riesgos y de conformidad con la metodología establecida en el punto 7 de la presente política y los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo V7 del Departamento Administrativo de la Función Pública – DAFP. Para su construcción, se identificarán los procesos, programas, proyectos y actividades que involucren gestión fiscal, así como los puntos de riesgo fiscal, entendidos como aquellas actividades en las que, por acción u omisión, podría generarse un efecto dañoso sobre los recursos, bienes o intereses patrimoniales de naturaleza pública.

Una vez identificados los puntos de riesgo fiscal, se determinarán las circunstancias inmediatas, área de impacto, efecto económico y causa raíz que podrían propiciar su materialización, el evento potencial y el posible efecto dañoso sobre los recursos o bienes públicos. Posteriormente, se analizarán y valorarán los riesgos considerando los controles existentes, su diseño y efectividad, con el fin de establecer el nivel de riesgo inherente y residual y determinar las medidas de tratamiento requeridas. La formulación deberá diferenciar claramente el riesgo fiscal de sus causas y consecuencias, teniendo presente que la existencia de un riesgo fiscal constituye una situación potencial y no implica por sí misma la ocurrencia de un daño fiscal.

8.3. Riesgos de seguridad de la información

La ESU gestionará los riesgos asociados con la seguridad de la información mediante la identificación y valoración de las amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de la información y de los activos de información.

8.3.1. Metodología para el levantamiento del mapa de seguridad de la información

El levantamiento del mapa de riesgos de seguridad de la información se realizará de manera articulada con el mapa institucional de riesgos y de conformidad con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Guía para la Gestión Integral del Riesgo V7 del Departamento Administrativo de la Función Pública – DAFP. Para su construcción se identificarán los activos de información relevantes para los procesos institucionales, considerando su naturaleza, importancia, propietario o responsable, así como las condiciones que puedan afectar su confidencialidad, integridad y disponibilidad, teniendo en cuenta el contexto interno y externo de la ESU.

A partir de la identificación y valoración de los activos de información, se determinarán las amenazas, vulnerabilidades y demás factores que puedan dar lugar a eventos que comprometan la seguridad de la información. Los riesgos deberán formularse de manera que permitan establecer claramente el evento de riesgo, sus causas y sus posibles consecuencias, considerando, entre otros aspectos, el acceso no autorizado, divulgación, pérdida, alteración, destrucción, indisponibilidad o uso inadecuado de la información y de los sistemas que la soportan. Posteriormente y considerando el punto 7 de la presente política, se analizarán y valorarán los riesgos inherentes y residuales, teniendo en cuenta los controles de seguridad existentes, su diseño, implementación y efectividad.

8.4. Riesgos para la integridad pública

En materia de integridad en el sector público, se espera que los servidores, y en general los colaboradores de las entidades públicas, dentro de un marco ético, se comporten de forma que privilegien el interés general del Estado en todas las decisiones que deben tomar en el ejercicio de sus funciones o del servicio que prestan. Por lo tanto, cualquier decisión que no privilegie ese interés es un incumplimiento de la conducta deseable que constituye una actuación que pone en riesgo a la integridad.

Los riesgos para la integridad pública corresponden a aquellos eventos potenciales derivados de acciones u omisiones que, en desarrollo de las funciones, procesos y actividades de la ESU, puedan afectar la integridad de la gestión pública, propiciar la obtención de beneficios particulares o de terceros, generar conflictos de intereses no gestionados, favorecer prácticas de corrupción, fraude o soborno, o comprometer la transparencia, imparcialidad, moralidad y prevalencia del interés general en las actuaciones de la entidad. Su gestión estará orientada a fortalecer una cultura institucional basada en la

ética, la transparencia, la prevención de conflictos de intereses y el rechazo de cualquier forma de corrupción.

A continuación, se definen las amenazas para la integridad pública:

Soborno: El Soborno puede ser entendido como *"ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]"* (Definición de soborno según la norma ISO 37001:2025 - Sistemas de gestión antisoborno. Requisitos con orientación para su uso). Y opera en dos niveles: soborno entrante y saliente. Se entiende como entrante el soborno al servidor de la Entidad, y como saliente el soborno por parte de servidores a otros en nombre de la Entidad.

Fraude: ***"****Corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros*" (Concepto construido a partir de los términos y definiciones utilizados por la Organización Internacional de Normalización (ISO, por sus siglas en inglés). El fraude puede ser interno, en cuyo caso involucra a colaboradores, o externo, cuando se realizó por terceros, externos y la organización es la víctima.

Inadecuada gestión del conflicto de interés: Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

Corrupción: Es todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero.

Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP: La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

8.4.1. Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP

Teniendo en cuenta las diferentes amenazas para la integridad pública, que pueden generar peligro o daño, es necesario que, desde un enfoque basado en riesgos, se gestionan los eventos que puedan ocurrir dentro de la ESU.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, se articula con los riesgos generales de gestión, los riesgos fiscales y los de seguridad de la información. Al final, un riesgo de gestión, un riesgo fiscal o un riesgo de seguridad de la información puede tener como causa el soborno, el fraude, un conflicto de intereses gestionado inadecuadamente o la corrupción. Por esta razón, es necesario abordar los riesgos para la integridad pública de forma integral y en estrecha articulación con la gestión institucional del riesgo.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP contempla que la la ESU adopte una serie de instrumentos de gestión del riesgo, que actúe con diligencia en el conocimiento de sus contrapartes y que integre en su operación una función de cumplimiento, todo esto además de la identificación y valoración de los riesgos según la metodología definida en el punto 7 de la presente política y la Guía para la Gestión Integral del Riesgo V7 del Departamento Administrativo de la Función Pública – DAFP.

El SIGRIP se constituye, asimismo, en un mecanismo para implementar y dar cumplimiento a los lineamientos establecidos para la gestión de riesgos del Programa de Transparencia y Ética Pública – PTEP.

8.4.1.1 Operación del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP

El SIGRIP es el conjunto de cuatro elementos que operan e interactúan entre sí: Política para la Gestión Integral de Riesgos y mapa de riesgos, la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo.

Sistema de Gestión de Riesgos para la Integridad Pública



Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

Política para la Gestión Integral de Riesgos: Define los mecanismos mediante los cuales se identificarán y valorarán los diferentes riesgos a los que está expuesta la organización, incluidos los riesgos para la integridad pública.

Debida diligencia en el conocimiento de las contrapartes: La ESU definirá los lineamientos, procedimientos o manuales sobre la debida diligencia con que deben llevar a cabo el conocimiento de sus contrapartes. El resultado de estos mecanismos tiene como único propósito generar insumos para la toma de decisiones, pero no podrá derivar en inhabilidades o incompatibilidades diferentes a las contempladas en la legislación vigente.

Función de cumplimiento: El cargo será asumido por el Jefe de la Oficina Estratégica. La función de cumplimiento implica entre otros aspectos: velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto; Evaluar el SIGRIP y presentar los resultados a la Alta Dirección; Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.

Herramientas de gestión del riesgo: La gestión de riesgos para la integridad pública requiere que la ESU implemente las siguientes herramientas que contribuyen a la integralidad del sistema:

- Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP)
- Política Antisoborno.
- Política Antifraude.
- Procedimiento para la gestión de los conflictos de intereses.
- Procedimiento para el reporte de operaciones sospechosas.
- Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

8.4.2. Monitoreo, evaluación, auditoría y mejora

La **primera línea de defensa** debe realizar monitoreo y valoración cada cuatro meses, de los riesgos para la integridad pública. Los resultados deberán quedar debidamente registrados y soportados en la plataforma dispuesta por la ESU, incluyendo las evidencias que permitan verificar la ejecución de los controles.

La **segunda línea de defensa** evaluará cada cuatro meses el SIGRIP, mediante el seguimiento a los indicadores definidos y el análisis de los reportes y evidencias proporcionados por la primera línea de defensa.

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto de auditoría, la cual estará a cargo de la **tercera línea de defensa**. La auditoría debe realizar

una evaluación independencia del Sistema para determinar su conformidad y eficacia, tanto del conjunto como de los controles individualmente vistos. La auditoría debe hacerse conforme a las técnicas vigentes, al plan de auditoría de la entidad y desde un enfoque basado en riesgos.

La **línea estratégica** revisará integralmente el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP. Este proceso de mejora debe ser continuo, y nutrirse de los reportes que se generan en el monitoreo, las evaluaciones y las auditorías.

9. APETITO, TOLERANCIA Y CAPACIDAD DE RIESGO

La ESU establecerá un marco de referencia para la toma de decisiones frente a la exposición al riesgo, considerando:

Apetito de riesgo

El apetito de riesgo corresponde al nivel y tipo de riesgo que la ESU está dispuesta a asumir para el cumplimiento de sus objetivos estratégicos y el desarrollo de su objeto social, en el marco de la normatividad aplicable, las directrices de la Alta Dirección y los principios que orientan la gestión institucional.

En consideración a las líneas estratégicas de la Entidad, su objeto social y la naturaleza de los procesos que desarrolla, la ESU establece como apetito de riesgo que los riesgos residuales se mantengan dentro de los niveles de severidad que la entidad considere aceptables para el cumplimiento de sus objetivos.

En consecuencia, los riesgos residuales cuya severidad sea calificada como catastrófica se encuentran por fuera del apetito de riesgo de la ESU y, por tanto, no podrán permanecer en dicho nivel de manera permanente. Cuando un riesgo residual se ubique en esta condición, el responsable del proceso deberá implementar las acciones de tratamiento necesarias para reducir su nivel de exposición, fortalecer los controles existentes y/o establecer controles adicionales, de acuerdo con la metodología institucional de administración del riesgo.

La aceptación de los niveles de riesgo que se encuentren dentro del apetito definido estará condicionada al cumplimiento de las disposiciones legales, reglamentarias e institucionales aplicables y al adecuado funcionamiento de los controles establecidos.

Tolerancia al riesgo

La tolerancia al riesgo corresponde al nivel máximo de variación o desviación que la ESU está dispuesta a aceptar respecto de su apetito de riesgo, sin que ello implique comprometer de manera significativa el cumplimiento de sus objetivos estratégicos, la continuidad de sus operaciones, el desarrollo de su objeto social o el cumplimiento de sus obligaciones legales y contractuales.

Los riesgos residuales cuya severidad sea calificada como catastrófica se encuentran por fuera del nivel de tolerancia de riesgo de la ESU y, por tanto, no podrán permanecer en dicho nivel.

Capacidad de riesgo

Máximo nivel de riesgo que la Empresa puede soportar sin comprometer de manera significativa el cumplimiento de sus objetivos.

La línea estratégica revisará periódicamente estos parámetros y podrá establecer criterios diferenciados de acuerdo con la tipología y criticidad del riesgo.

10. INDICADORES CLAVE DE RIESGO – ICR

Los Indicadores Clave de Riesgo - ICR, son métricas diseñadas con el fin de identificar, estimar y monitorear la ocurrencia y severidad de eventos y posibles amenazas que puedan llegar a afectar el cumplimiento de los objetivos institucionales en los diferentes niveles, por lo que se constituyen en la herramienta para el seguimiento y monitoreo de los riesgos, ya que pueden entregar señales de alerta temprana, así como detectar tendencias o cambios en los niveles de riesgo, lo que facilita que se incorporen acciones correctivas y preventivas para minimizar sus impactos frente a posibles materializaciones.

Los indicadores tienen una función principal que es monitorear los riesgos clave que podrían afectar el cumplimiento de los objetivos y metas establecidos durante las diversas etapas de la gestión institucional, además proporcionan información útil sobre los riesgos emergentes y potenciales que pueden impactar los objetivos estratégicos.

La **primera línea de defensa** deberá Identificar y formular los Indicadores Clave de Riesgo – ICR que pueden alertar sobre la exposición al riesgo para los procesos, programas o proyectos bajo su responsabilidad.

La **segunda línea de defensa** asegurará que los que los Indicadores Claves de Riesgo – ICR estén alineados con los objetivos estratégicos y operativos de la entidad. Además, establecerá la metodología que guíen la medición, seguimiento y monitoreo de los respectivos indicadores.

La **tercera línea de defensa** evaluará si los Indicadores Claves de Riesgo – ICR son pertinentes y eficaces y verificará que sean aplicados por parte de los responsables.

La **línea estratégica** realizará seguimiento y análisis periódico a los Indicadores Claves de Riesgo - ICR.

11. CONTINUIDAD DE NEGOCIO

La gestión de riesgos se articulará con la estrategia de continuidad de negocio de la ESU.

La Empresa identificará los procesos, servicios y recursos críticos y desarrollará estrategias para mantener o recuperar su operación ante eventos disruptivos.

Los escenarios de continuidad podrán comprender, entre otros:

- Fenómenos naturales.
- Emergencias sociales.
- Fallas o pérdida de infraestructura.
- Incidentes tecnológicos o cibernéticos.
- Interrupciones de servicios esenciales.
- Crisis sanitarias.
- Indisponibilidad de recursos críticos.
- Otros eventos que puedan afectar significativamente la operación.

La identificación y gestión de estos escenarios deberá guardar correspondencia con el análisis de impacto al negocio, los planes de continuidad y las pruebas que establezca la ESU.

12. ACCIONES ANTE LA MATERIALIZACIÓN DE RIESGOS

Cuando se materialice un riesgo, el responsable deberá reportarlo de manera oportuna al líder del proceso, quien, a su vez, informará al Subgerente, Secretario General o Jefe de Oficina, según corresponda, y a la segunda línea de defensa (Oficina Estratégica), con el propósito de coordinar y adoptar las acciones necesarias para contener sus efectos, mitigar las consecuencias y prevenir su recurrencia. La gestión deberá comprender, como mínimo:

- Reporte del evento.
- Análisis de las circunstancias de materialización.
- Identificación de las causas.
- Evaluación de los controles existentes.
- Determinación de las consecuencias.
- Adopción de medidas de contingencia y corrección.
- Definición de acciones para evitar su recurrencia.
- Actualización del riesgo y sus controles cuando corresponda.
- Seguimiento a la implementación de las acciones.

Cuando la materialización pueda constituir un hecho relacionado con corrupción, fraude u otra afectación a la integridad pública, se deberán activar adicionalmente los mecanismos institucionales y legales correspondientes.

13. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

La gestión integral del riesgo será monitoreada de manera permanente bajo el esquema de líneas de defensa.

La **primera línea** realizará el monitoreo y valoración de los riesgos y controles a su cargo, por lo menos una vez cada semestre. Los resultados deberán quedar debidamente registrados y soportados en la plataforma dispuesta por la ESU para la gestión de riesgos, incluyendo las evidencias que permitan verificar la ejecución de los controles. El monitoreo y valoración de los riesgos para la integridad pública, se hará mínimo cada cuatrimestre.

La **segunda línea** realizará seguimiento y análisis consolidado, verificará la aplicación de la metodología y generará alertas a la línea estratégica.

La **tercera línea** realizará evaluación independiente mediante auditorías y demás actividades previstas en el Plan Anual de Auditoría.

Los resultados deberán utilizarse para fortalecer los controles, actualizar los riesgos y mejorar la toma de decisiones.

14. COMUNICACIÓN Y CONSULTA

La ESU promoverá una comunicación oportuna, clara y transparente de la información relacionada con la gestión del riesgo.

La comunicación deberá considerar, entre otros:

- Cambios en el contexto.
- Nuevos riesgos.
- Riesgos emergentes.
- Materialización de eventos.
- Resultados del monitoreo, revisión y valoración de riesgos.

La información relacionada con la gestión de riesgos que deba ser divulgada públicamente se hará de acuerdo con las disposiciones legales aplicables y los instrumentos de transparencia de la ESU. Los mapas de riesgos se deberán publicar en la página web mínimo una vez al año.

La presente Política para la Gestión Integral del Riesgo fue aprobada por la Junta Directiva de la ESU el día [29] de octubre de 2026 y entrará en vigencia a partir de la fecha de su aprobación, siendo de obligatorio cumplimiento para todos los procesos de la Entidad.