POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

OFICINA ASESORA DE PLANEACIÓN

2026

Contenido

1. INTRODUCCIÓN

La Fundación Gilberto Alzate Avendaño – FUGA, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), reconoce la gestión del riesgo como un componente estratégico para el logro de sus objetivos institucionales, la generación de valor público y la protección de los recursos a su cargo. En este sentido, esta Política de Administración de Riesgos se establece como una herramienta fundamental para anticipar, identificar, analizar, evaluar y tratar los riesgos que puedan afectar el cumplimiento de su misión y el desarrollo de sus procesos.

La política definida por la FUGA se fundamenta en el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Control Interno con el propósito no solo de dar cumplimiento a los mandatos normativos, sino de identificar de manera anticipada amenazas, reducir la incertidumbre, aprovechar oportunidades y asegurar de manera razonable el logro de sus objetivos estratégicos con eficiencia y transparencia.

Con el fin de garantizar una ejecución técnica y estandarizada, la FUGA adopta los lineamientos definidos por el Departamento Administrativo de la Función Pública- DAFP en la Guía para la Gestión Integral del Riesgo en Entidades Públicas - V7 de agosto de 2025, integrando bajo un mismo marco de actuación los riesgos de gestión, integridad, seguridad digital, fiscales y de sostenibilidad. Generando así, una visión integral, asegurando que todas las dependencias, procesos y niveles de la organización operen bajo lineamientos unificados para la identificación, análisis, valoración y tratamiento de los eventos que puedan afectar el cumplimiento de la misión. Adoptando de esta manera buenas prácticas en materia de control interno, promoviendo una cultura organizacional orientada a la prevención, la transparencia y la mejora continua. Su implementación busca fortalecer la toma de decisiones informadas, optimizar la gestión institucional y contribuir al cumplimiento de los objetivos estratégicos, en coherencia con los principios de eficiencia, eficacia y responsabilidad en la gestión pública.

De igual manera, la política establece un marco claro para el monitoreo, seguimiento y evaluación permanente de los riesgos, asegurando su actualización frente a cambios en el entorno interno y externo. Esto permite a la entidad

adaptarse de manera ágil a nuevos desafíos, fortalecer su capacidad institucional y garantizar la sostenibilidad de sus resultados.

Es así, como con la adopción de esta Política de Administración de Riesgos, la Fundación Gilberto Álzate Avendaño reafirma su compromiso con la integridad, la transparencia y la generación de confianza en la ciudadanía, consolidando una gestión pública orientada a resultados, al control efectivo y a la mejora continua.

2. Objetivo

Establecer el marco general para la adecuada administración de los riesgos de la Fundación Gilberto Álzate Avendaño – FUGA, mediante la definición de lineamientos estratégicos y operativos que orienten la identificación, análisis, valoración, tratamiento, monitoreo y comunicación de los riesgos, con el propósito de que se tomen decisiones oportunas para mitigar la ocurrencia de eventos que afecten el cumplimiento de los objetivos y metas de la entidad y los compromisos con los colaboradores, instituciones y ciudadanos.

3. Alcance

La Política de administración de riesgos es aplicable de manera transversal a todos los procesos de la entidad contenidos en el mapa de procesos de la entidad, abarcando los niveles estratégicos, misional, de apoyo y de evaluación.

Su cobertura integra bajo un mismo marco de actuación los riesgos de Gestión, Seguridad de la Información, Seguridad y Salud en el Trabajo, Gestión Ambiental, Fiscales y de Integridad, estos últimos en el marco del SIGRIP. En consecuencia, sus disposiciones son de obligatorio cumplimiento para todos los servidores públicos y contratistas en el ejercicio de sus funciones legales y obligaciones contractuales, quienes deberán actuar conforme a las responsabilidades asignadas en el esquema de líneas de defensa adoptado.

4. Definiciones y Siglas

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.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022)

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

Apetito del riesgo: es el nivel de riesgo que una entidad está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe gestionar.

Capacidad del Riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. (relacionado con la solvencia y liquidez).

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

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.

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Confidencialidad: Propiedad de la información que garantiza que esta no sea divulgada a personas, entidades o procesos no autorizados.

Conflicto de interés: Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (Tomado de Anexo 2: Glosario Guía para la Gestión Integral del Riesgo en Entidades Públicas V7).

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.

Contraparte: es cualquier persona natural o jurídica con la que el Distrito Capital tiene o planifica establecer algún tipo de relación comercial. En esta categoría se ubican contrapartes como proveedores de bienes y servicios, empleados en cualquier modalidad de contratación y clientes.

Control: medida que permite reducir o mitigar un riesgo.

Debida diligencia: es el proceso mediante el cual la entidad adopta medidas para el conocimiento de la contraparte, de su negocio, operaciones, y productos y el volumen de sus transacciones (Superintendencia de Sociedades de Colombia, 2021).

Fraude: errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (Tomado de Anexo 2: Glosario Guía para la Gestión Integral del Riesgo en Entidades Públicas V7).

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de mantener la protección, exactitud, coherencia, confiabilidad y completitud de la información**.**

Factores de Riesgo: Son las fuentes generadoras de riesgos. Para los riesgos del LA/FT y se deben tener en cuenta como mínimo los siguientes: i) Clientes y usuarios, ii) Prestación de servicios a la ciudadanía, iii) Canales de distribución y iv) Jurisdicciones (Infolaft, 2022).

Lideres de proceso: Funcionarios del nivel directivo designados por el Comité Institucional de Gestión y Desempeño como responsables de la correcta ejecución de los procesos, así como de la pertinencia y mejora continua del Modelo de Operación por Procesos.

Mapa de riesgos: documento que resume los resultados de las actividades de gestión de riesgos, incluye su identificación, análisis, valoración para los riesgos inherentes y residuales, la identificación y evaluación de los controles y los resultados de la evaluación de riesgos.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgos de Seguridad Digital: Son los riesgos asociados a la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como aquellos relacionados con el uso, operación y control de los sistemas de información, plataformas tecnológicas, servicios digitales, datos institucionales y accesos, que puedan afectar el cumplimiento de los objetivos de la entidad.

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.

Riesgos de Gestión: Son los riesgos que puedan afectar tanto el cumplimiento de los objetivos de los procesos estratégicos, misionales, de apoyo y de evaluación, contenidos en el mapa de procesos de la entidad, así como los objetivos estratégicos.

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.

Riesgos para la integridad Pública: Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas. (Tomado de Anexo 2: Glosario Guía para la Gestión Integral del Riesgo en Entidades Públicas V7).

Riesgo residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información haciendo uso de normas, prácticas y herramientas contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción de datos tanto físicos como digitales.

Seguridad Digital: Situación de normalidad y confianza en el entorno digital, mediante la gestión de riesgos, implementación de controles y fortalecimiento de capacidades para proteger los activos digitales de la entidad

Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos. (Tomado de Anexo 2: Glosario Guía para la Gestión Integral del Riesgo en Entidades Públicas V7).

Soborno: 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. (Tomado de Anexo 2: Glosario Guía para la Gestión Integral del Riesgo en Entidades Públicas V7).

Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad

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

5. Marco Normativo

Esta política se formula en concordancia con el siguiente marco legal y técnico:

- ✓ Artículos 209 y 269 Constitución Política de Colombia.
- ✓ Ley 87 de 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 454 de 1998 "Por la cual se determina el marco conceptual que regula la economía solidaria, se transforma el Departamento Administrativo Nacional de Cooperativas en el Departamento Nacional de la Economía Solidaria, se crea la Superintendencia de la Economía Solidaria, se crea el Fondo de Garantías para las Cooperativas Financieras y de Ahorro y Crédito, se dictan normas sobre la actividad financiera de las entidades de naturaleza cooperativa y se expiden otras disposiciones".
- ✓ Ley 2094 de 2021 "Por medio de la cual se reforma la ley 1952 de 2019 y se dictan otras disposiciones".
- ✓ Ley 2195 de 2022 "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones".
- ✓ Decreto 1122 de 2024 "Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.
- ✓ Decreto 1499 de 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".
- ✓ Resolución 2024120007655 del 15 de noviembre de 2024 "por la cual se adopta el Modelo Integrado de Planeación y Gestión y se modifican las funciones del Comité Institucional de Gestión y Desempeño".
- ✓ Guía para la Gestión Integral del Riesgo (Versión 7).
- ✓ Norma Técnica Internacional ISO 31000:2018 "Gestión del riesgo, principios y directrices".
- ✓ Modelo de Seguridad y Privacidad de la Información – MSPI "Lineamientos para la Gestión de Seguridad de la Información en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones (Versión 5 2025).

- ✓ Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- ✓ Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
- ✓ Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- ✓ Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- ✓ CONPES 3995 de 2020 "Política Nacional de Confianza y Seguridad Digital".
- ✓ ISO/IEC 27001 "Norma internacional para sistemas de gestión de seguridad de la información".
- ✓ ISO/IEC 27005 "Gestión de riesgos de seguridad de la información".

5.1. Lineamientos

La Fundación Gilberto Álzate Avendaño FUGA, orienta la gestión del riesgo bajo los siguientes lineamientos:

- ✓ Para determinar la valoración de probabilidad y el impacto debe tenerse en cuenta las orientaciones establecidas en la "GM-GU-03 Guía para Administración del Riesgo" o demás documentos que expida la entidad en la materia.
- ✓ Integrar la gestión del riesgo en la planeación, el control y la toma de decisiones institucionales.
- ✓ Reportar oportunamente la materialización de riesgos a las instancias competentes, conforme a los procedimientos internos.
- ✓ Garantizar que los riesgos críticos sean objeto de seguimiento y control permanente.

- ✓ En cuanto al apetito del riesgo, se establecen que la FUGA define su capacidad de riesgo como el límite máximo no negociable, asociado al cumplimiento normativo, la integridad pública y la continuidad del servicio.
- ✓ Utilizar los resultados de auditorías y evaluaciones como insumo para el fortalecimiento institucional.

6. Desarrollo de la Política

6.1. Declaración de la Política

La Fundación Gilberto Alzate Avendaño – FUGA, en el marco del Modelo Integrado de Planeación y Gestión – MIPG y en coherencia con las directrices del Departamento Administrativo de la Función Pública, adopta la presente Política de Administración del Riesgo como un instrumento estratégico para fortalecer la toma de decisiones, proteger los recursos públicos y asegurar el cumplimiento de su misión institucional. Esta política se fundamenta en un enfoque preventivo, sistemático y basado en procesos, que permite anticipar, identificar, analizar y gestionar los riesgos que puedan afectar la prestación de sus servicios y el logro de sus objetivos.

Es así, como la FUGA se compromete a implementar una gestión integral del riesgo que abarque los riesgos de gestión, fiscales, de seguridad digital y de integridad pública, incluyendo aquellos asociados a prácticas de corrupción como el fraude, el soborno y los conflictos de interés. En este sentido, la entidad promoverá la aplicación de metodologías estandarizadas para la identificación, valoración, tratamiento, monitoreo y comunicación de los riesgos, asegurando su articulación con el direccionamiento estratégico, los planes institucionales y el modelo de operación por procesos.

Como parte del compromiso, además, la FUGA incorporará la gestión de riesgos de seguridad de la información y seguridad digital con el propósito de proteger la confidencialidad, integridad y disponibilidad de los activos de información, fortalecer la continuidad de la operación y prevenir incidentes de seguridad.

Así mismo, la FUGA establece su compromiso con el fortalecimiento de una cultura organizacional orientada a la gestión del riesgo, en la que todos los servidores y colaboradores asumen responsabilidades claras conforme al esquema de líneas de defensa definido por MIPG.

La alta dirección liderará la definición del apetito del riesgo y el seguimiento a su gestión y declara formalmente un apetito cero frente a cualquier riesgo de Corrupción, Fraude, incumplimiento Legal o daño al patrimonio Fiscal, y un apetito bajo a moderado controlado para los riesgos operativos y estratégicos; los líderes de proceso serán responsables de la identificación y control de los riesgos en su ámbito; y las instancias de seguimiento y control garantizarán la evaluación independiente y la mejora continua del sistema. Implementando de esta manera controles preventivos y detectivos que permitan mitigar la probabilidad e impacto de los riesgos, promoviendo la transparencia, la integridad y la adecuada administración de los recursos públicos.

Esta política se revisará periódicamente, en función de los cambios del entorno y del análisis del comportamiento de los riesgos, con el fin de asegurar su pertinencia, efectividad y contribución al fortalecimiento institucional y a la generación de valor público.

6.2. Responsabilidades de la gestión y control del riesgo

A continuación, se establecen los roles y responsabilidades conforme al esquema de líneas de defensa del modelo integrado planeación y gestión MIPG:

6.2.1. Línea Estratégica

Esta línea estratégica establece el liderazgo y compromiso de la Alta Dirección, conocido como "tono desde la cima", además aprueba las políticas y provee los recursos necesarios para la gestión de riesgos. Los órganos que componen esta línea son la Alta Dirección, el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno.

Responsabilidades y compromisos frente al riesgo:

- Asegurar la asignación de los recursos necesarios, sean humanos, financieros o tecnológicos, requeridos para la adecuada implementación de esta política, conforme a la solicitud y justificación presentada por la Oficina Asesora de Planeación.
- Liderar y fomentar una cultura organizacional consciente del riesgo y orientada a la integridad.
- Promover la implementación de lineamientos asociados con seguridad de la información, seguridad digitaly continuidad del negocio.

- Aprobar la Política de Administración del Riesgo
- Analizar el monitoreo realizado por la Oficina Asesora de Planeación, y recomendaciones sobre el mapa de calor y reporte de riesgos materializados.
- Analizar los Informes de Auditoría y/o seguimientos presentados por la Oficina de Control Interno y Entes de Control.
- Evaluar el estado del Sistema de Control Interno de acuerdo con las características propias de la FUGA y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento.

6.2.2. Primera Línea de Defensa

Desarrolla e implementa acciones de control y gestión de riesgos a través de su identificación, análisis, evaluación, monitoreo y acciones de mejora. Esto está a cargo de los líderes de los procesos y colaboradores de la entidad, quienes diseñan, implementan, hacen seguimiento a los controles y gestionar de manera directa los riesgos de la entidad.

Responsabilidades y compromisos frente al riesgo:

- Liderar la gestión integral de los riesgos, incluyendo la identificación, análisis, valoración y tratamiento en sus respectivos procesos, así como en los proyectos e iniciativas estratégicas bajo su responsabilidad.
- Revisar el contexto estratégico de la FUGA con el propósito de identificar cambios que puedan originar nuevos riesgos o modificar los existentes.
- Identificar y controlar los riesgos de seguridad de la información y seguridad digital asociados a los activos de información y servicios tecnológicos utilizados en sus procesos bajo su responsabilidad.
- Identificar amenazas, vulnerabilidades y posibles eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Diseñar, implementar y verificar periódicamente la efectividad de los controles preventivos, detectivos y correctivos, asegurando que estos mitiguen realmente las causas raíz identificadas.
- Presentar en los plazos fijados por la Oficina Asesora de Planeación los reportes de avance de la gestión de riesgos y las evidencias de la ejecución de los controles a la segunda línea.

- Socializar los controles implementados, con el fin de asegurar su comprensión y oportuna aplicación, además de la información y comunicación necesaria que dé cuenta de la gestión de riesgos.
- Reportar oportunamente incidentes de seguridad de la información y seguridad digital, eventos de riesgo y materialización de riesgos que hayan sido identificados en sus respectivos procesos.
- Aplicar los lineamientos definidos en materia de seguridad de la información, seguridad digital protección de datos personales y seguridad digital.
- Identificar las oportunidades para fortalecer la gestión del riesgo en su proceso y proponerlas ante la Oficina Asesora de Planeación.

6.2.3. Segunda Línea de Defensa

Genera el apoyo técnico, define la metodología institucional y ejerce la supervisión continua, consolidando la información para la toma de decisiones mediante la elaboración del Mapa Integral de Riesgos y los informes ejecutivos de monitoreo.

Responsabilidades y compromisos frente al riesgo:

- Mantener actualizada la política de administración de riesgos de la FUGA asegurando que esta cumpla con los lineamientos vigentes dados por los entes rectores.
- Implementar y fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Coordinar actividades relacionadas con seguridad de la información, seguridad digital y continuidad de negocio.
- Asesorar a los líderes de los procesos en las etapas de análisis, evaluación, tratamiento de los riesgos.
- Consolidar el mapa integral de riesgos a partir de las matrices de los procesos, analizando los riesgos de mayor criticidad frente al logro de los objetivos.
- Realizar seguimiento y monitoreo a las etapas de la gestión del riesgo.
- Realizar seguimiento a la gestión de incidentes de seguridad de la información, seguridad digital y vulnerabilidades identificadas.
- Promover la identificación y clasificación de activos de información institucionales.
- Revisar que los controles para gestionar los riesgos estén diseñados e implementados por la primera línea de defensa, e identificar cualquier oportunidad de mejora.

- Solicitar cuando sea necesario la formulación de planes de mejoramiento orientados a fortalecer la gestión del riesgo en los procesos y proyectos de inversión.
- Preparar y presentar cuatrimestralmente los informes consolidados de monitoreo de riesgos ante el Comité Institucional de Gestión y Desempeño, para su análisis y toma de decisiones.
- Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva.
- Validar metodológicamente y, si es necesario, devolver para corrección las matrices de riesgo presentadas por la Primera Línea que no cumplan con los criterios técnicos definidos en la GM-GU-03 Guía para Administración del Riesgo, antes de su consolidación en el Mapa Integral.

Responsable de Cumplimiento (SIGRIP) y Líder de Integridad Pública:

Por su parte, el (la) Jefe de la Oficina Jurídica ejerce el rol de Líder de Integridad Pública y articulador del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), encargándose de proveer:

- Los criterios y señales de alerta para la identificación de operaciones inusuales o sospechosas asociadas al Lavado de Activos y Financiación del Terrorismo (LA/FT/FP).
- Construir el Manual de Debida Diligencia y/o definir la pertinencia de la Política GM-PO-03 Sarlaft, para el conocimiento de contrapartes, el cual debe ser aplicado por los líderes de proceso en la contratación y vinculación de terceros, en cumplimiento del Artículo 73 literal A de la Ley 1474 de 2011.
- Proponer una Plan de implementación de SIGRIP.

6.2.4. Tercera Línea

Genera aseguramiento objetivo e independiente evaluando la eficacia de la gestión de riesgos y la efectividad de los controles implementados por la Primera y Segunda Línea. Su relación con la Segunda Línea es de comunicación y coordinación para asegurar una cobertura adecuada sin duplicar esfuerzos, pero manteniendo total independencia en su evaluación, la cual se rige por la periodicidad establecida en el Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno.

Responsabilidades y compromisos frente al riesgo:

- Evaluar la efectividad de los controles e informar los cambios en la evaluación del riesgo a la alta dirección.
- Comunicar al Comité de Coordinación de Control Interno cambios en la evaluación del riesgo.
- Generar alertar cuando se detecten deficiencias en los controles durante las auditorías de gestión o desempeño.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia en la gestión de los riesgos.
- Establecer un programa anual de auditoria basado en riesgos.
- Proporcionar información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.
- Evaluar el cumplimiento de la Política de Administración del Riesgo y presentar los resultados ante el Comité Institucional de Coordinación de Control Interno.
- Alertar sobre la probabilidad de riesgo de fraude o corrupción, fiscales y lavado de activos y financiación del terrorismo.

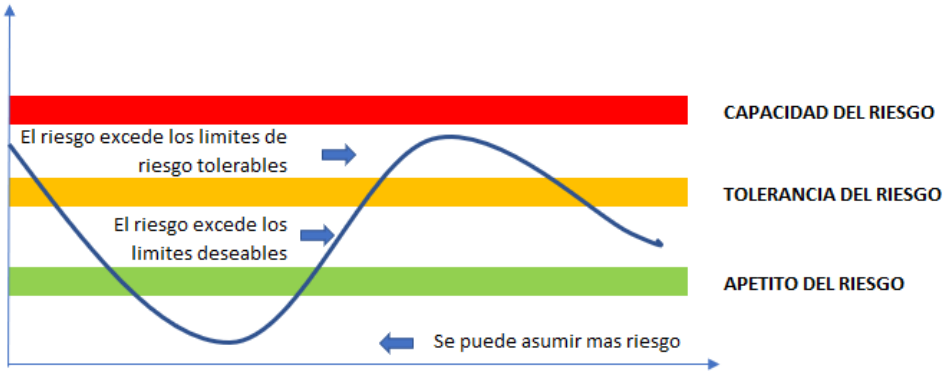
Cada línea actúa de manera coordinada para garantizar la prevención, mitigación y control de riesgos, asegurando la transparencia y la rendición de cuentas en todos los niveles

6.3. Niveles y Apetito del Riesgo

La FUGA adopta la implementación de un sistema de límites el cual está conformado por la siguiente estructura:

- **Límite de apetito al riesgo**: Constituye el nivel de riesgo que la FUGA está dispuesta a aceptar en la búsqueda de sus objetivos misionales. Refleja de alguna manera la filosofía de la entidad en la gestión de los diferentes riesgos a los que se encuentra expuesta.

- **Límite de tolerancia al riesgo:** Corresponde al nivel máximo permitido en la variación de los resultados respecto al nivel apetito de riesgo fijado por la FUGA.



Fuente. Propia 1

Es así, como desde la FUGA se realizó un análisis, teniendo en cuenta el estado de madurez de la gestión de los riesgos en la entidad, considerando el comportamiento de los riesgos durante las vigencias 2024 y 2025, así como su tendencia.

A partir de este análisis, se define el apetito de riesgo institucional, estableciendo como aceptables aquellos riesgos que, de acuerdo con su nivel de probabilidad e impacto, se ubican en las zonas bajas del mapa de calor, siempre que cuenten con controles documentados y permitan hacer seguimiento a través de indicadores clave de riesgo.

No obstante, la entidad establece excepciones específicas al apetito general, definiendo lineamientos particulares para las siguientes tipologías de riesgo:

- La FUGA define y aprueba un apetito de riesgo nulo frente a los riesgos de integridad, corrupción y fraude, por lo que no se acepta exposición residual que comprometa la transparencia, la ética pública y la confianza institucional.
- La FUGA define y aprueba un apetito de riesgo nulo frente a cualquier evento que pueda generar daño patrimonial al Estado.
- La FUGA define y aprueba un apetito de riesgo nulo frente a riesgos fiscales con implicaciones disciplinarias y legales.
- La FUGA define y aprueba un apetito de riesgo nulo frente a eventos que puedan generar afectaciones críticas sobre la protección de datos personales y la reserva de la información.
- La FUGA define y aprueba un apetito de riesgo nulo frente a eventos que puedan generar afectaciones a la reputación e imagen institucional.
- Frente a los riesgos de seguridad de la información, la FUGA establece un apetito de riesgo bajo, en consideración a la criticidad de los activos de

información y la necesidad de garantizar su confidencialidad, integridad y disponibilidad, debido a que son controlados mediante actividades de seguimiento y monitoreo

- Frente a los riesgos asociados a procesos estratégicos e iniciativas de innovación, la FUGA define un apetito de riesgo moderado, permitiendo la asunción de riesgos controlados que contribuyan al fortalecimiento institucional y al cumplimiento de su misión.

NOTA: Los riesgos de seguridad de la información, seguridad digital, relacionados con fuga de información sensible, indisponibilidad crítica de servicios tecnológicos, ciberataques o incumplimiento normativo serán tratados como riesgos prioritarios independientemente de su clasificación inicial.

Tabla 1. Niveles de aceptación del riesgo para la Fundación Gilberto Álzate Avendaño.

Tipo de Riesgo	UBICACIÓN EN EL MAPA DE CALOR (Riesgo Residual)	NIVELES DE ACEPTACIÓN
Riesgos de Gestión **Riesgo de Seguridad de la Información Y Seguridad Digital**	**Bajo**	**Apetito del riesgo**
	Moderado	**Tolerancia del riesgo**
	Alto	
	Extremo	**Capacidad del riesgo**
Riegos de integridad, corrupción y fraude **Riesgo Estratégico** **Riesgos fiscales (con implicaciones disciplinarias y legales)**	**Moderado**	**Apetito al riesgo**
	Alto	**Tolerancia del riesgo**
	Extremo	**Capacidad de riesgo**

Fuente. Propia 2

Mediante la aprobación de la presente política en la instancia del Comité Institucional de Control Interno, se adopta el Marco de Apetito de Riesgo (MAR), en el cual se establecen los niveles de apetito y tolerancia, así como los mecanismos para su monitoreo y control, garantizando una adecuada gestión del riesgo en la entidad.

6.4. Indicadores Claves de Riesgos (KRI)

La FUGA establece que la gestión del riesgo no debe basarse únicamente en valoraciones cualitativas o subjetivas. Por tanto, define el diseño, medición y monitoreo de Indicadores Clave de Riesgo (KRI).

Los Indicadores Clave de Riesgos (KRI), hacen referencia a los datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos.
No necesariamente indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente.

Teniendo en cuenta que los indicadores clave de riesgos requieren, al igual que los indicadores de gestión el desarrollo de los siguientes temas: Nombre del indicador, una descripción de lo que se va a medir, la fórmula de cálculo, la fuente de información para el cálculo del indicador la frecuencia de medición y seguimiento y los umbrales de alerta, estos indicadores se formularán en el marco de los indicadores por proceso, estando definidos de esta manera por los lideres que deben hacer su seguimiento y garantizando de esta manera que están siendo monitoreados.

En lo referente a seguridad de la información y seguridad digital, se implementarán indicadores orientados a la medición de exposición a amenazas, vulnerabilidades, incidentes y afectaciones sobre los activos de información y servicios tecnológicos institucionales.

Los indicadores deberán permitir el monitoreo oportuno de riesgos tecnológicos, de seguridad de la información, seguridad digital y continuidad operativa. Deberán ser revisados periódicamente por Gestión TI, con el fin de identificar tendencias, vulnerabilidades emergentes y necesidades de fortalecimiento de controles.

6.5. Accionar ante riesgos materializados

Cuando el riesgo se materializa, se deben implementar inmediatamente las acciones de contingencia; y posteriormente identificar las causas que lo llevaron a esta instancia de materialización, con el propósito de formular acciones correctivas para evitar su recurrencia; de otra parte, la segunda línea "gestiona los eventos[1]" integrando al mapa de riesgos los riesgos materializados y controla la trazabilidad

Tabla 2 Acciones ante riesgos materializados

Zona de Riesgo "Residual"	TIPO DE RIESGO	
	RIESGOS DE GESTION y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	**RIESGOS DE CORRUPCION**
Baja	**1. Identificación:** Quien detecte la materialización de un riesgo de gestión y/o de seguridad de la información seguridad digitalreportará al líder del proceso respectivo.	1. Toda persona, servidor o colaborador que tenga conocimiento o sospecha de la comisión del delito de soborno y/o conducta asociada con corrupción y/o que detecte la materialización de un riesgo de corrupción y/o posible
Moderada		

[1] Gestionar Eventos: Controlar registro de riesgos materializados y datos históricos que permiten revisar si el riesgo fue identificado y qué sucedió con los controles.

-

Alta y Extrema	**2. Análisis:** El líder de proceso y su equipo evalúan el impacto y alcance. **3. Contención y Tratamiento:** El líder del proceso y su equipo implementan las **acciones correctivas inmediatas** de acuerdo a los tiempos definidos en el GM- PD-01 Procedimiento de Plan de Mejoramiento y ejecutarán las acciones necesarias para la corrección y mitigación. En caso de ser necesario ejecutarán las acciones que permitan recuperar o restablecer la operación y/o servicios.. **4. Reporte Segunda Línea:** El líder de proceso informa a la Oficina Asesora de Planeación (segunda línea) sobre el hallazgo y las acciones tomadas. Posteriormente, verifican la **calificación y ubicación del riesgo** para su actualización en el mapa de riesgos, con la asesoría metodológica de la Oficina Asesora de Planeación.	acto de corrupción, así como la existencia de inhabilidades, incompatibilidades o conflicto de intereses, podrá informarlos mediante los canales dispuestos para la recepción de denuncias : Línea 195, Oficina de Atención al Ciudadano, Oficina de Correspondencia, Página web institucional (https://www.fuga.gov.co/atencion-servicios-ciudadania/punto-de-atencion-y-defensor-del-ciudadano) o Intranet (https://intranet.fuga.gov.co/quejas-y-conflictos-de-intereses) , los cuales serán canalizados por el Proceso de Servicio al Ciudadano, y radicados en el Sistema Distrital para la Gestión de Peticiones Ciudadanas – "*Bogotá te escucha*" 2. Una vez radicados en "*Bogotá te escucha"* se clasifican por la tipología "Denuncia por acto de corrupción "y se direcciona automáticamente al Proceso de Control Interno Disciplinario quien garantizará la gestión eficiente de las denuncias por actos de corrupción que ingresan a

	5. **Reporte Línea Estratégica:** La Oficina Asesora de Planeación, informa al Comité Institucional de Coordinación de Control Interno CICCI sobre la materialización del riesgo e integra al mapa de riesgos, la gestión de los eventos asociados. 6. **Seguimiento y Mejora:** La Oficina de Control Interno, verifica que se tomaron las acciones correctivas y evalúa su ejecución, realizando un análisis de causas, lecciones aprendidas y con ello define acciones preventivas, correctivas y de mejora orientadas a evitar la recurrencia. ***Nota 1:*** Cuando la Oficina de Control Interno, detecte en el marco de Auditorias, la materialización del riesgo, lo informará al Comité Institucional de Coordinación de Control Interno CICCI. ***Nota 2:*** Ante la materialización de Riesgos de Seguridad de la Información, el Proceso	la FUGA y generara los informes correspondientes a la Dirección Distrital de Asuntos Disciplinarios de la Secretaría Jurídica Distrital y demás entidades relacionadas. Lo anterior, conforme a los lineamientos de la GS-*GU-06 Guía Gestión de Conflicto Intereses y GS-CA-01 Proceso Gestión de Talento Humano – Control Interno Disciplinario* *3.* Surtido el conducto regular y los procesos disciplinarios particulares; el Proceso de Control Disciplinario, generará las alertas e informará al Comité Institucional de Coordinación de Control Interno CICCI, sobre los hechos encontrados. 4. El Comité Institucional de Coordinación de Control Interno – Comité de Dirección, emitirá lineamientos para la adopción de las Acciones Correctivas correspondientes, de acuerdo a los tiempos definidos en el GM- PD-01 Procedimiento de Plan de Mejoramiento; así como la revisión y/o

	de Gestión de Tecnologías, orientan a las áreas en la aplicación de los pasos anteriores, y en paralelo se aplican los lineamientos del "Procedimiento de Gestión de Incidentes, amenazas y debilidades de seguridad GT-PD-09", y formato GT-FT-04, y proyecta un "Informe de incidentes de seguridad de la información, seguridad digital" a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre otros), conforme lo estipulan los entes y las buenas prácticas en seguridad de la información[2] **Nota 3:** Cuando la materialización del riesgo pueda afectar la continuidad de la operación de la FUGA, los servicios tecnológicos o la prestación de los servicios objeto de su	actualización de los riesgos de corrupción identificados. Lo anterior, con la asesoría metodológica de la Oficina Asesora de Planeación. 5. Control Interno, verifica que se tomaron las acciones correctivas y evalúa su ejecución. ***Nota 1:*** En todos los canales de atención al ciudadano, y los procesos disciplinarios particulares, deberá garantizarse la protección de identidad del denunciante y la reserva de la información suministrada. ***Nota 2:*** Cuando la oficina de Control Interno, detecte la materialización de riesgos, en el marco de Auditorias, informará lo correspondiente al Comité Institucional de Coordinación de Control Interno CICCI y a la Autoridad competente.

[2] Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en Entidades Públicas V2 de agosto de 2019.

	misionalidad, se activarán los mecanismos y planes de contingencia, continuidad del negocio y recuperación ante desastres definidos institucionalmente.	

6.7. Periodicidad de seguimiento sobre los riesgos y socialización de la Política

Desde la dirección se define que los lideres de proceso deben realizar seguimiento a la aplicación de los controles existentes, la implementación de nuevos controles y de acuerdo con el nivel residual de cada riesgo y su nivel de aceptación establecido en esta política, a las actividades de plan de acción sobre los riesgos.

Los riesgos tendrán una periodicidad de seguimiento, monitoreo y evaluación cuatrimestral. Las fechas del reporte la establece y comunica la Oficina Asesora de Planeación al inicio de cada vigencia. Sin embargo, en cualquier momento de la vigencia pueden solicitar a los procesos envío de información de la gestión de sus riesgos.

En relación a los riesgos de seguridad de la información, seguridad digital, la Oficina Asesora de Planeación realizará seguimiento continuo a los riesgos asociados a los activos de información, infraestructura tecnológica, servicios digitales, vulnerabilidades, incidentes de seguridad y controles implementados, con el fin de fortalecer la prevención, detección y respuesta ante amenazas tanto internas como externas.

La Oficina de Control Interno realiza el seguimiento de acuerdo con las directrices y fechas definidas por la ley.

Adicionalmente, en cuanto a la política como tal se deberán tener en cuenta los siguientes criterios:

Se deberá realizar revisión y actualización en los casos que sea pertinente, de la Política de Administración de Riesgos, con el propósito de evidenciar los ajustes que sean pertinentes de acuerdo con los cambios normativos aplicables que se puedan presentar.

La Política de Administración de riesgos deberá ser socializada por los canales internos con los que cuenta la Entidad a todos los servidores públicos, contratistas y terceros que participen en la operación misional de la FUGA o tengan acceso a los activos de información de la entidad, promoviendo una cultura organizacional orientada a la gestión preventiva, el autocontrol y la seguridad de la información y seguridad digital.

La FUGA desarrollará actividades periódicas de sensibilización, capacitación y fortalecimiento de capacidades relacionadas con gestión del riesgo, seguridad de la información, seguridad digital y protección de datos personales.

La presente política deberá revisarse y actualizarse periódicamente, o cuando se presenten cambios significativos en el entorno institucional, normativo, tecnológico, operacional o en el nivel de exposición a riesgos de la FUGA.

7. Documentos Asociados

- GM-FT-10 Mapa Riesgos de Gestión
- GM-FT-13 Mapa Riesgos de Corrupción
- GM-FT-14 Matriz Integral de Riesgos
- GM-FT-03 Matriz y Fichas Técnicas de Indicadores
- GM-GU-03 Guía para Administración del Riesgos
- GM-PO-01 Política Antisoborno

8. Referencias

Alcaldía Mayor de Bogotá. Directiva 015 de 2015 "Directrices para la atención y gestión de denuncias por posibles actos de corrupción, y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses y protección de

identidad del denunciante" octubre de 2015. Disponible en: (https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=63146)

Veeduría Distrital. Guía de Lineamientos Antisoborno del D.C. noviembre de 2018. Disponible en; (https://old.integracionsocial.gov.co/anexos/documentos/2019paac/12022019_b2_Guia%20de%20lineamientos%20antisoborno%20para%20el%20Distrito%20VF%20(29%20dic%2018).pdf)

Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP) V2 de agosto de 2019. Disponible en: (https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499)

Ministerio de Tecnologías de la Información y las Comunicaciones- MINTIC. Registro de Activos de Información. Registro de activos de información | Vigencia 2020 / Resolución 318 de 2019 - Instrumentos de gestión de la información / Registro de activos de información | Vigencia 2019 / Registro de activos de información / Disponibles en: (https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion)

Departamento Administrativo de la Función Pública DAFP. Guía para la Gestión Integral del Riesgo (Versión 7). Disponible en: (https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf)

Alcaldía Mayor de Bogotá. Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales V1 diciembre de 2020. Disponible en: (https://secretariageneral.gov.co/transparencia/informacion-interes/lineamientos-distritales/ruta-metodologica-la-implementacion-del-sarlaft-las-entidades-distritales)

Decreto Distrital 189 de 2020 "Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones". Disponible en: (https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=95985)

Alcaldía Mayor de Bogotá. Lineamientos para la identificación de riesgos de corrupción en Trámites, OPA y consultas de información distritales 2021. Facilitado por: Subsecretaria de Servicio al Ciudadano y Secretaría Jurídica Distrital Circular 006 de 26abr2021

Alcaldía Mayor de Bogotá. Directiva 001 de 2021 "Directrices para la atención y gestión de denuncias por posibles actos de corrupción, y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses y protección de identidad del denunciante" marzo 2021. Disponible en: (https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=108172)

9. Control de versiones:

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
23//08/2018	1	Versión inicial, aprobada en Comité Institucional de Coordinación de Control Interno	Sonia Córdoba Alvarado – jefe Oficina Asesora Planeación
30/04/2019	2	Se actualiza la Política de riesgos, adoptando la Guía de administración de riesgos DAFP versión 4 2018.	Luis Fernando - jefe Oficina Asesora de Planeación Deisy Estupiñán – Contratista Equipo SIG
24/06/2021	3	Se actualiza la Política de riesgos, adoptando la Guía de administración de riesgos DAFP versión 5 2020, así como los lineamientos "particulares" emitidos por la Alcaldía Mayor de Bogotá y órganos generadores de política para riesgos de corrupción en Trámites y/o OPAs, y Lavado de Activos	Luis Fernando Mejía- jefe Oficina Asesora de Planeación y Deisy Estupiñán – Contratista Equipo SIG

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
29/09/2022	4	Se actualiza la Política de riesgos en los numerales 2 Alcance, 3 Tipologías riesgos (Corrupción), Paso 2 Identificación de riesgos, 6 Conceptos Clave, 8 Referencias, integrando lineamientos preventivos de cohecho y soborno, articulados con la GM-PO-02 Política Antisoborno de la FUGA, conforme a la Guía de Lineamientos de la Veeduría Distrital. De otra parte, se integran en el Numeral 3 Tipología riesgos (Seguridad Información) la relación de activos críticos identificados, formalizarlos y priorizados, en el marco del Modelo de Seguridad y Privacidad de la Información) conforme al Orfeo 20222900090123, como lo dicta el paso 7 de la guía de activos de información Fuga.	Luis Fernando Mejía- jefe Oficina Asesora de Planeación y Deisy Estupiñán – Contratista SIG Alba Rojas - Contratista MIPG
20/08/2024	5	Se realizar actualización de la Política de Administración de Riesgos de acuerdo con la actualización de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad de la información - Versión 6 de noviembre de 2022, expedida por el Departamento Administrativo de la Función Pública – DAFP y el Documento técnico. Adaptación de medidas de prevención y mitigación del riesgo del lavado	Luz Mery Pongutá - Jefe Oficina Asesora de Planeación e Ingrid Dalila Mariño Morales – Contratista MIPG

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
		de activos, financiación del terrorismo en las entidades del Distrito Capital – diciembre 2022, expedida por la secretaria general (Alcaldía de Bogotá). Se realizo la actualización del documento incluyendo lineamientos para los riesgos de tipo: riesgos de gestión, riesgos de posibles actos de corrupción, riesgos de seguridad de la información, riesgos de continuidad de negocio, riesgos del LA/FT/FPADM y riesgos fiscales. Además, se revisó todo el documento, con el propósito de detallar, complementar y fortalecer su contenido	
16/04/2026	6	Actualización integral y reestructuración de la Política, alineándola con los requisitos de la Guía para la Gestión Integral del Riesgo (Versión 7) del DAFP y la norma ISO 31000:2018. Las modificaciones sustanciales incluyen: • Se unifican bajo un mismo marco de gobernanza los riesgos de Gestión, Seguridad Digital, Integridad (SIGRIP), Fiscales y Sostenibilidad. • Declaración explícita del Apetito de Riesgo (Cero/Bajo/Moderado) y establecimiento de la	Anggie Lorena Ramírez - Jefe Oficina Asesora de Planeación Ingrid Dalila Mariño Morales – Contratista MIPG

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
		obligatoriedad de los Indicadores Clave de Riesgo (KRI) para riesgos críticos.	

Elaboró:	**Revisó:**	**Aprobó:**
Ingrid Dalila Mariño Morales Contratista Planeación MIPG – SIG Fecha: abril del 2026	**Magda Yusef Rojas Diaz** Contratista Planeación MIPG – SIG **Anggie Lorena Ramírez** Jefe Oficina Asesora de Planeación **Angélica Hernández Rodríguez** Jefe Oficina Control Interno **Linda Pedraza** Contratista Gestión de Tecnologías Fecha: junio del 2026	**Comité Institucional de Coordinación de Control Interno CICCI** Fecha: 25/06/2026 Expediente. 2026FUGA00206E