



úSAI

Institución Universitaria de San Andrés,
Providencia y Santa Catalina

**MANUAL DE DEBIDA
DILIGENCIA EN EL
CONOCIMIENTO DE LAS
CONTRAPARTES**

INFOTEP 2026

INFOTEPSetransforma

Contenido

1.OBJETIVO	3
2.ALCANCE	3
3.DEFINICIONES	3
4.FUNCION DE CUMPLIMIENTO.....	5
5. RIESGOS ASOCIADOS A LA DEBIDA DILIGENCIA.....	6
6. DETALLE DE LAS ACTIVIDADES PARA LA DEBIDA DILIGENCIA.....	7
6.1 Aplicación de la debida diligencia.....	8
7. DEBIDA DILIGENCIA ANTE UNA OPERACIÓN INUSUAL.....	13
7.1 Flujograma.....	13
8. SITUACIONES EN OPERACIONES INUSUALES.....	17
8.1 Conductas inusuales relativas a los servidores públicos.....	17
8.2 Conductas inusuales en operaciones o actividades relacionadas con el sistema financiero	18
9. ASPECTOS CLAVES DE LA DEBIDA DILIGENCIA RELACIONADAS CON SITUACIONES SOSPECHOSAS DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO.	18
9.1 Medidas de prevención del lavado de activos y financiamiento de delitos, como el terrorismo en las operaciones del INFOTEP.....	19
9.2 Evaluación del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo en las operaciones del INFOTEP	19
9.3 Matriz de verificación en listas restrictivas (LA/FT)	19
10.SEGUIMIENTO Y EVALUACION.	21
11. CONTROL DE CAMBIOS	21

1.OBJETIVO



Brindar lineamientos para la implementación de las medidas de debida diligencia en el conocimiento de las contrapartes, en las que exista una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva en el INFOTEP de conformidad con la normatividad vigente en la materia

2.ALCANCE



Este lineamiento comprende las orientaciones, elementos conceptuales y mecanismos para implementar la debida diligencia en los procesos en que se hayan identificado riesgos de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva, el documento hace parte del proceso de Gestión del Talento Humano y deberá tener en cuenta los sistemas, procesos y documentos con los que interactúa.

3.DEFINICIONES

- **Debida Diligencia:** proceso para evaluar con mayor detalle la naturaleza y alcance del riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva y para ayudar a las organizaciones a tomar decisiones en relación con transacciones, proyectos, actividades, socios

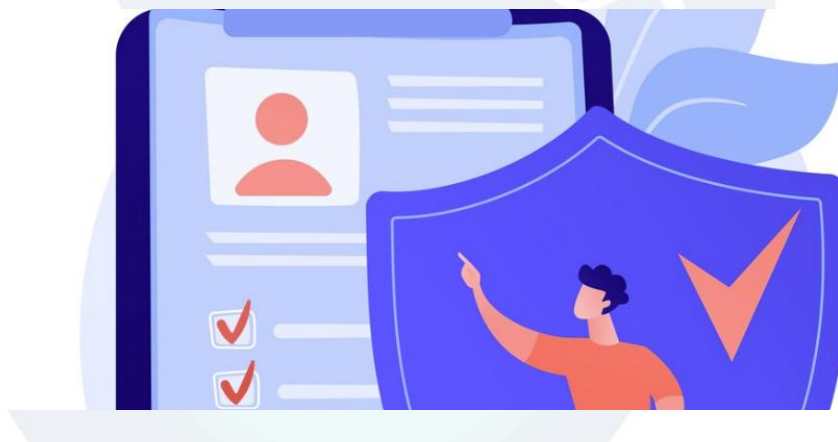
de negocios y personal específico.

- **Soborno:** oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directa o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.
- **Operaciones Inusuales:** a las operaciones tentadas o realizadas en forma aislada o reiterada, con independencia del monto, que carecen de justificación económica y/o jurídica, y/o no guardan relación con el nivel de riesgo del cliente o su perfil transaccional, y/o que, por su frecuencia, habitualidad, monto, complejidad, naturaleza y/u otras características particulares, se desvían de los usos y costumbres en las prácticas de mercado.
- **Riesgo Legal:** Es la posibilidad de pérdida en que incurre una compañía al ser sancionada, multada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.
- **Parte Interesada o Grupo de interés:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. Puede ser interna o externa a la organización.
- **Listas de control:** son listas de información nacionales e internacionales utilizadas principalmente por los oficiales de cumplimiento o encargados de las funciones de cumplimiento que, contienen información de diversas fuentes sobre personas naturales o jurídicas. Esta información contribuye a que la Institución tenga conocimiento más amplio de los antecedentes legales de sus contrapartes.
- **Administración del riesgo:** es el proceso a través del cual la institución identifica, cuantifica, controla y monitorea los riesgos a los cuales se encuentra expuesta.
- **Riesgo reputacional:** Es la posibilidad de pérdida en que incurre una Institución por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.
- **Operación o transacción económica inusual e injustificada:** Es aquella operación o transacción que no guarda correspondencia con los patrones regulares de las actividades económicas que habitualmente realiza el cliente, y cuyo origen no puede ser justificado
- **Financiamiento de delitos:** Es el proceso por el cual una persona natural o jurídica, provee o recolecta fondos por el medio que fuere, directa o indirectamente, a sabiendas de que serán utilizados o con la intención deliberada de que se utilicen, en todo o en parte, para cometer un acto o actos delictivos, por parte de una organización criminal o por un delincuente individualmente considerado
- **Financiamiento del terrorismo:** Actividad por la cual cualquier persona deliberadamente provea o recolecte fondos por el medio que fuere, directa o indirectamente, con la intención ilícita de que se utilicen o a sabiendas que serán

utilizados, en todo o en parte para cometer un acto o actos de terrorismo, por una organización terrorista o por un terrorista.

- Lavado de activos: Es el proceso por el cual los bienes y ganancias monetarias de origen delictivo e ilícito, se invierten, integran o transforman en el sistema económico financiero legal con apariencia de haber sido obtenido de forma ilícita y procurando ocultar su verdadera procedencia, así como su real propiedad y el ejercicio de su dominio y control.
- Persona políticamente expuesta (PEP): Son todas aquellas personas naturales nacionales o extranjeras que desempeña o ha desempeñado funciones públicas destacadas en el país o en el exterior, por ejemplo, Jefe de Estado o de un gobierno, político de alta jerarquía, funcionario gubernamental, judicial o militar de alto rango, ejecutivo estatal de alto nivel, funcionario importante de partidos políticos, así como su cónyuge y sus parientes dentro del cuarto grado de consanguinidad o segundo de afinidad y sus colaboradores cercanos.
- Señales de alerta: Son aquellos elementos que evidencian los comportamientos particulares de los clientes o usuarios y las situaciones atípicas que presentan las operaciones o transacciones que pueden encubrir actividades de lavado de activos o de financiamiento del terrorismo. Hay que tener en cuenta que no todas las operaciones que presentan comportamientos atípicos e inusuales son operaciones ilegales, por tal razón, el hecho de identificar señales de alerta no significa que la operación deba ser reportada de forma inmediata a las autoridades.

4.FUNCION DE CUMPLIMIENTO



La función de cumplimiento en el INFOTEP recae internamente en la Alta Dirección (Rectoría, Vicerrectoría Administrativa y Financiera y Vicerrectoría Académica), apoyada por la oficina de Control Interno.

Sus funciones son:

- ✓ Identificación y Evaluación de Riesgos: Reconocer los riesgos de incumplimiento (legales, reputacionales, entre otros) y su impacto.
- ✓ Diseño de Políticas y Procedimientos: Crear códigos de conducta y manuales de cumplimiento (ej. SARLAFT/prevención de lavado de activos).

- ✓ **Monitoreo y Control:** Supervisar las operaciones y los controles internos para asegurar su efectividad.
- ✓ **Capacitación y Sensibilización:** Entrenar a empleados y directivos para fomentar una cultura de cumplimiento.
- ✓ **Investigación y Reporte:** Investigar conductas indebidas y reportar operaciones sospechosas a los reguladores.
- ✓ **Asesoría Consultiva:** Asesorar a la Institución sobre normas vigentes y corregir fallas en el control.

5. RIESGOS ASOCIADOS A LA DEBIDA DILIGENCIA



El INFOTEP realiza evaluación sobre la naturaleza y el alcance de riesgos de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva con relación a las transacciones, proyectos, actividades, colaboradores, proveedores y personal (funcionario y contratista). Esta evaluación se debe realizar mediante la identificación de cargos y actividades críticas de acuerdo con el alcance definido en los procesos priorizados.

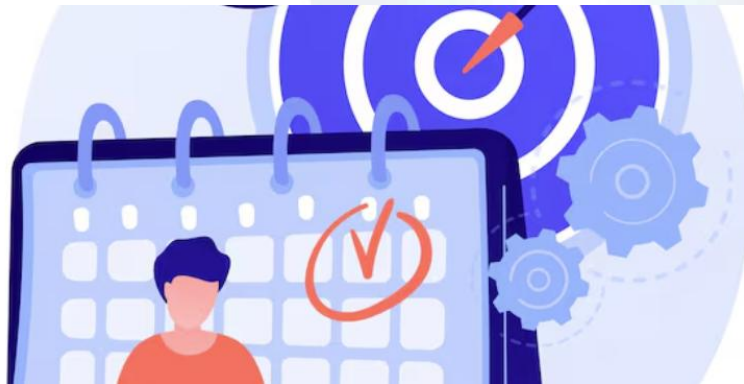
A continuación, se detallan los riesgos asociados a la debida diligencia:

- **Riesgo económico:** está relacionado con la posibilidad de que decisiones o acciones del INFOTEP resulten en pérdidas financieras significativas. Esto puede ocurrir como consecuencia de una mala gestión de recursos, errores en la planificación financiera, fraudes, o la imposibilidad de cumplir con los compromisos económicos, lo que afectaría la sostenibilidad y viabilidad de los proyectos y actividades en curso.
- **Riesgos LA/FT/FP:** Establece medidas para prevenir y detectar posibles actividades ilícitas relacionadas con el lavado de activos, la financiación del terrorismo y la financiación de proliferación de armas de destrucción masiva
- **Riesgo legal:** está relacionado con la posibilidad de que el INFOTEP incurra en incumplimientos normativos, regulatorios o contractuales durante la ejecución de sus proyectos y actividades. La falta de cumplimiento con las leyes y

regulaciones aplicables podría resultar en sanciones, demandas o acciones legales que afecten la integridad institucional y la operatividad de la Institución

- Riesgos medioambientales y sociales: Impactos que las operaciones puedan tener en el medio ambiente o en la comunidad, así como la alineación con las normas sociales y de sostenibilidad.
- Riesgo operativo: se refiere a la posibilidad de que fallos en los procesos internos, ineficiencias en la gestión o deficiencias en la implementación de controles afecten la ejecución adecuada de los proyectos y actividades del INFOTEP. Tales fallos pueden derivar en la interrupción de las operaciones, pérdidas de recursos, o en la imposibilidad de cumplir con los objetivos establecidos.
- Riesgo reputacional: se refiere a la posibilidad de que las prácticas o decisiones del INFOTEP, en el marco de sus transacciones, proyectos y actividades, puedan afectar negativamente su imagen pública o la percepción de la ciudadanía y otras instituciones, comprometiendo su confianza y credibilidad.

6. DETALLE DE LAS ACTIVIDADES PARA LA DEBIDA DILIGENCIA



- Identificación de los riesgos de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva, considerando el mapa de riesgos y los procesos más vulnerables.
- Realizar la revisión de los resultados de la matriz de riesgos considerando: número de riesgos, cantidad de incertidumbres y su rango residual.
- Realizar un análisis que permita identificar las actividades necesarias para evaluar de manera más detallada la naturaleza y el alcance de los riesgos anteriormente mencionados, así como apoyar a la Institución en la toma de decisiones relacionadas con transacciones, proyectos, actividades, colaboradores, proveedores y personal (funcionario y contratista).
- Establecer actividades o controles que permitan aplicar medidas específicas para gestionar y supervisar cada uno de los procesos relacionados con transacciones, proyectos, actividades, colaboradores, proveedores y personal (funcionario y contratista). La información clave necesaria para conocer o investigar las actividades puntuales puede estar documentada en los procedimientos establecidos, lo que facilita el monitoreo y la correcta ejecución de dichos procesos.

6.1 Aplicación de la debida diligencia

Área de Talento Humano – Selección y Vinculación

Debida Diligencia - Altos Directivos: Rector y Vicerrectores

Debida Diligencia para Servidores Públicos: Con el objetivo de que la Institución disponga de un conocimiento adecuado sobre el perfil de riesgo de los servidores, como provisionales, se llevará a cabo la revisión y validación de la información general y específica de cada aspirante y será actualizada cuando se presenten cambios que justifiquen su ajuste. Los resultados de este proceso deberán formar parte de la hoja de vida de cada servidor público, junto con la declaración de bienes y rentas.

En este sentido, se realizará la verificación y evaluación de antecedentes para garantizar que las personas que ocupan cargos claves actúen con integridad, cumplan con la normativa vigente y no representan un riesgo para la Institución. Este proceso incluye la revisión de su historial laboral y profesional, posibles conflictos de interés y cualquier otra señal de alerta relacionada con conductas ilícitas o inapropiadas. El objetivo es asegurar que los altos directivos estén alineados con los valores y principios del código de integridad, minimizando el riesgo de corrupción o malas prácticas en la gestión institucional.

A continuación, se presenta la lista de documentos de acuerdo con la provisión de empleos:

ITEM	DESCRIPCIÓN	TIPO DE PROVISION DEL EMPLEO			
		ENCARGO	PERIODO DE PRUEBA	LIBRE NOMBRAMIENTO Y REMOCIÓN	PROVISIONAL
1	Copia Cédula de Ciudadanía	X	X	X	X
2	Copia Libreta Militar (si aplica)		X	X	X
3	Copia Diplomas Estudios Formales (para el caso de estudios en el exterior, copia de la solicitud de convalidación o la resolución de convalidación)		X	X	X
4	Copia Tarjeta Profesional (si aplica)	X	X	X	X
5	Certificado de Antecedentes disciplinarios profesionales (si aplica)	X	X	X	X

6	Certificado de vigencia Tarjeta profesional (si aplica)	X	X	X	X
7	Certificaciones laborales (con fecha de inicio y finalización exacta, cargo desempeñado y descripción de las funciones) – Para el caso de certificaciones en otro idioma, deben estar traducidas al idioma español por un traductor oficial.		X	X	X
8	Certificación Bancaria con número y tipo de cuenta para consignar las obligaciones (no mayor a 3 meses de expedición).		X	X	X
9	Copia del Rut actualizado		X	X	X
10	Certificación de afiliación a EPS		X	X	X
11	Certificación de afiliación al Fondo de Pensiones		X	X	X
12	Registro o Actualización de hoja de vida en SIGEP con documentos adjuntos de acuerdo con la información consignada (En caso de no estar registrado, se le enviará clave de acceso mediante correo electrónico).	X	X	X	X
13	Certificación Publicación Ley 2013 de 2019 (Declaración de bienes y Rentas /Conflicto de Intereses)	X	X	X	X
14	Certificado de Registro de Deudores Alimentarios Morosos REDAM	X	X	X	X
15	Consulta de Antecedentes Fiscales (Contraloría)	X	X	X	X

16	Consulta de Antecedentes, Sanciones e Inhabilidades (Procuraduría)	X	X	X	X
17	Consulta de Antecedentes Judiciales (Policía Nacional)	X	X	X	X
18	Consulta de Medidas correctivas (Policía Nacional)	X	X	X	X
19	Copia OCCRE	X	X	X	X
20	Examen médico laboral de ingreso	X	X	X	X
21	Afiliación fondo nacional del ahorro	X	X	X	X
22	Examen de idoneidad de inglés y creole		X	X	X

A continuación, se detalla la verificación de requisitos:

- Antecedentes y capacidades: Se realizará el análisis del historial personal y profesional de los servidores públicos, verificando antecedentes laborales, educativos, fiscales y judiciales, con el fin de detectar posibles irregularidades, conflictos de interés o vínculos con actividades ilegales o no éticas.
- Detección y manejo de conflictos de interés: Se deberán identificar posibles situaciones en las que los servidores públicos puedan tener intereses personales, familiares o económicos que afecten su imparcialidad y objetividad en el ejercicio de sus funciones. En caso de encontrarse tales situaciones, se gestionan de acuerdo con la normativa vigente.
- Capacitación y sensibilización continua: Se implementarán en los procesos de inducción y reinducción programas regulares de formación en ética pública, anticorrupción, buenas prácticas y gestión pública, con el fin de reforzar los principios de transparencia, responsabilidad y compromiso con el servicio público entre los servidores del INFOTEP.
- Monitoreo y seguimiento del desempeño: Se realizará el proceso de evaluación del desempeño a funcionarios (carrera administrativa). Este monitoreo también permitirá tomar medidas correctivas cuando se detectan prácticas inapropiadas.
- Listas restrictivas: como medida preventiva, se realizará una consulta anual masiva del personal vinculado o activo a la Institución. Esta verificación deberá quedar registrada en el expediente de cada servidor público. En caso de identificar alguna novedad, se deberá reportar a la dependencia encargada, conforme al régimen disciplinario de la función pública.

Área de Contratación

Debida diligencia para contratistas y/o proveedores y colaboradores: implica la investigación y evaluación para asegurar que las empresas o contratistas con los que el

INFOTEP establece relaciones comerciales cumplan con los estándares legales, éticos y de transparencia requeridos. Este proceso incluye la revisión de antecedentes financieros, legales, fiscales, reputacionales y laborales, así como la identificación de posibles conflictos de interés, prácticas de corrupción o irregularidades. El objetivo es mitigar riesgos asociados con contratos públicos, asegurando que los proveedores actúen de acuerdo con las normativas y principios institucionales, garantizando así la eficiencia, legalidad y transparencia en la gestión de los recursos públicos.

En este sentido, la Vicerrectoría Administrativa y Financiera a través de su área de Contratación implementó el formato Lista de Chequeo de Recepción de Documentos el cual recopila los documentos necesarios para la vinculación de los contratos directos, convenios y contratos interadministrativos. En cuanto a las otras modalidades de contratación como la licitación pública, la selección abreviada de menor cuantía y la selección de mínima cuantía; estas son ofertadas mediante la plataforma SECOP II donde se solicita en cada convocatoria los documentos mínimos requeridos para participar.

Asimismo, se establecen los siguientes controles:

- Investigación de antecedentes: verificación de los antecedentes legales, financieros y reputacionales del contratista o proveedor para detectar posibles vínculos con actividades ilícitas, fraudes o conflictos de interés.
- Evaluación de cumplimiento normativo: Se revisa el cumplimiento de la normatividad nacionales e internacionales aplicables y relacionadas con anticorrupción, fiscales y laborales, para asegurar que el proveedor opere dentro del marco legal.
- Análisis de riesgos financieros y operativos: Se evalúan los estados financieros del contratista o proveedor, su solvencia económica y su capacidad operativa para ejecutar los proyectos de manera eficiente y sin comprometer los intereses institucionales.
- Auditoría de prácticas comerciales: Se realiza un análisis de las prácticas comerciales y éticas del proveedor, garantizando que sus políticas y procedimientos no favorezcan la corrupción, el soborno ni ninguna otra conducta ilegal.
- Monitoreo continuo: Después de la contratación, se implementan mecanismos de monitoreo y evaluación para garantizar que el proveedor cumpla con los términos del contrato y las expectativas éticas y legales durante toda la duración de la relación comercial.

El objetivo de estos controles es mitigar los riesgos asociados con la contratación de contratistas, proveedores y/o colaboradores, asegurando que el proceso sea transparente, ético y alineado con las políticas públicas del Ministerio.

Área de relacionamiento con la ciudadanía

Debida Diligencia para Usuarios: Con el fin de asegurar la integridad, transparencia y seguridad en las relaciones con los usuarios y partes interesadas, el Ministerio llevará a

cabo un proceso de debida diligencia que permita garantizar el cumplimiento de las normativas legales y evitar riesgos asociados con actividades ilegales o no éticas.

A continuación, se detalla la verificación de requisitos:

Recolección de información básica:

- Solicitar a los usuarios, la información esencial, como nombre completo, documento de identidad, dirección, número de contacto y otros datos relevantes para su identificación.
- Verificar la autenticidad de los documentos presentados, como cédulas de ciudadanía, pasaportes, comprobantes de domicilio, etc.

Verificación de identidad:

- Validar la identidad del usuario mediante el uso de la información consignada en la plataforma Servicio Atención al Ciudadano- SAC.
- En casos de usuarios extranjeros, realizar la validación de su identidad mediante la información que suministra Migración Colombia.

Evaluación de riesgos de lavado de dinero y financiamiento del terrorismo:

- Realizar una evaluación de riesgo de acuerdo con el perfil del usuario, teniendo en cuenta factores como la actividad económica, ubicación geográfica y posibles vínculos con sectores de alto riesgo.
- Implementar mecanismos para monitorear y detectar actividades sospechosas relacionadas con lavado de dinero o financiamiento del terrorismo.

7. DEBIDA DILIGENCIA ANTE UNA OPERACIÓN INUSUAL



Una operación inusual es cuando efectivamente existe un comportamiento fuera de lo normal y que tiene relación con el sistema de gestión de riesgos LA/FT. En general, una operación inusual es entendida como aquella operación irregular que por su cantidad o características no es acorde a la actividad económica que realiza la persona o se sale de los parámetros normales establecidos para esta o de acuerdo al rol que desempeña.

Cuando se tiene un caso de una operación inusual, es importante:

1. Analizar las fuentes de información internas y externas. Se debe involucrar a la persona que inicialmente detectó la señal de alerta para que en su relación con la persona objeto de la investigación, le solicite más información o documentación que sirva para justificar la operación.
2. Realizar una indagación a la persona involucrada en referencia a lo detectado; es importante consultar y verificar información en listas, también es necesario analizar el comportamiento transaccional que ha tenido la persona para conocer qué tanto se salió de lo normal y si la justificación que da es aceptable o no.
- 3- Generar una resolución. Después de analizar la operación inusual y recoger la evidencia, si la justificación de esta es la adecuada, se debe cerrar el caso. Si, por el contrario, es una operación injustificable, debe presentar de forma inmediata un reporte de operación sospechosa- ROS ante la Unidad de Análisis de Información Financiera (UIAF), para lo cual se ejecuta de acuerdo al procedimiento de **operaciones sospechosas** de la entidad.

7.1 Flujograma

Este procedimiento permite analizar las inusualidades, recopilar información adicional, analizar la información de conocimiento de la persona involucrada, su operación con la entidad, detectar posibles inusualidades adicionales y determinar si se está ante una operación sospechosa o no.

No	ACTIVIDAD	DESCRIPCION	RESPONSABLE	REGISTRO
1	Cualquier funcionario o colaborador puede reportar la irregularidad en el formato de reporte de operaciones inusuales en un plazo no mayor a 72 horas desde que se detecta la situación	Identificar y reportar posibles operaciones inusuales o situaciones de riesgo de LA/FT en las operaciones de la entidad incluyendo la falta de coincidencia con los antecedentes verificados, la inclusión en listas restrictivas o la detección de actividades sospechosas	Funcionarios y/o contratistas de la entidad	Reporte de operación inusual y sospechosa
2	Enviar el formato a los servidores encargados de la función de cumplimiento	Enviar el reporte de la operación inusual a los servidores encargados de la función de cumplimiento para su gestión. La notificación deberá ir acompañada de los documentos relacionados con la operación o transacción, en dicho formato se incluirá un	Funcionarios y/o contratistas de la entidad	Reporte de operación inusual y sospechosa

		resumen detallado de la operación o transacción, junto con las razones por las cuales se considera que presenta características de inusualidad		
3	Analizar la información de la posible operación inusual o sospechosa	Realizar las investigaciones respectivas y dar respuesta a la persona involucrada o contraparte cerrando el caso siempre que la justificación sea la adecuada Nota: En caso de que, como resultado del análisis realizado, se determine que la operación no puede ser razonablemente justificada por la contraparte o presente indicios de posible relación con conductas asociadas al lavado de activos o la financiación del terrorismo (LA/FT),	Servidores responsables de la función de cumplimiento	Reporte de operación inusual y sospechosa Evidencia asociada a la investigación

		deberá activarse el procedimiento interno para el tratamiento y reporte de operaciones sospechosas,		
4	Reportar a los servidores responsables de la función de cumplimiento dentro de los primeros cinco (5) días de cada mes, una notificación que indique que no se registraron operaciones con características de inusualidad durante el mes inmediatamente anterior	Reportar por parte de las áreas sujetas a los mecanismos de control de prevención de lavado de activos y financiación del terrorismo, la ausencia de operaciones con características de inusualidad Las áreas sujetas a los mecanismos de control de prevención de LA/FT en la Institución son: Talento humano, área financiera, contratación y compras, admisiones y registro, almacén, internacionalización, extensión, bienestar, investigación y académica	Áreas sujetas a los mecanismos de control de prevención de lavado de activos y financiación del terrorismo	Reporte de operación inusual y sospechosa

8. SITUACIONES EN OPERACIONES INUSUALES



8.1 Conductas inusuales relativas a los servidores públicos

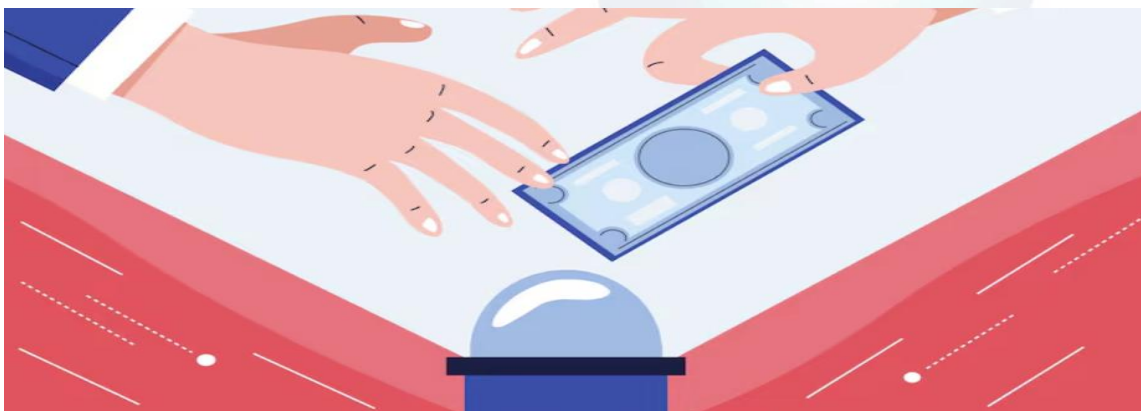
1. El estilo de vida del servidor público no guarda relación con sus ingresos, o presenta un cambio notable e inesperado en su situación económica.
2. El servidor público evita constantemente o se niega a tomar vacaciones.
3. El servidor público presenta ausencias frecuentes e injustificadas.
4. El servidor público permanece con frecuencia en la oficina fuera del horario laboral, sin una causa justificada.
5. El servidor público utiliza su domicilio personal para recibir documentación de los usuarios.
6. El servidor público insiste en realizar reuniones con usuarios del INFOTEP en lugares distintos a las oficinas o fuera del horario laboral, sin justificación, para llevar a cabo operaciones comerciales o financieras.
7. El servidor público está vinculado a organizaciones sin fines de lucro, como fundaciones, asociaciones, comités, ONG, entre otras, cuyos objetivos, debidamente demostrados, están relacionados con la ideología, reclamos o demandas de una organización terrorista nacional o extranjera, siempre que esto esté debidamente comprobado.
8. Se observa un crecimiento inusual o repentino en el número de operaciones bajo la responsabilidad del servidor público.
9. Se registra un cambio notable o inesperado en los negocios de carácter comercial de propiedad del servidor público.
10. Se confirma que el servidor público no ha comunicado o ha ocultado al área o persona delegada para la función de cumplimiento información relevante sobre cambios en el comportamiento de algún usuario.

8.2 Conductas inusuales en operaciones o actividades relacionadas con el sistema financiero

1. Transacciones incompatibles con el perfil del cliente: Operaciones cuyos valores no concuerdan con la ocupación profesional y la situación financiera declarada del cliente.
2. Estructuración de transacciones para eludir reportes: Transacciones diseñadas para evitar los umbrales de reporte establecidos, como dividir grandes sumas en depósitos más pequeños.
3. Uso de cuentas con múltiples firmantes no relacionados: Cuentas con varias personas autorizadas para firmar, entre las cuales no existe una relación aparente, ya sea familiar o comercial.

La detección de estas y otras conductas inusuales requiere un monitoreo constante y un análisis detallado, al identificar patrones atípicos, se pueden implementar medidas preventivas y, de ser necesario, reportar las operaciones sospechosas a las autoridades competentes para su investigación.

9. ASPECTOS CLAVES DE LA DEBIDA DILIGENCIA RELACIONADAS CON SITUACIONES SOSPECHOSAS DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO.



Es de resaltar que la operación sospechosa, es aquella operación inusual que no puede ser razonablemente justificada por la contraparte y que puede estar asociada con algún delito LA/FT, es decir, una operación significativa que no tiene relación con los comportamientos habituales y conocidos de la contraparte. Por lo anterior, a continuación, se detallan algunos aspectos claves para la debida diligencia relacionadas con LA/FT:

1. El usuario se niega a proporcionar la información solicitada o la información proporcionada es inconsistente o de difícil verificación por parte del INFOTEP
2. El usuario solicita ser excluido del registro de operaciones sin causa aparente o justificada.
3. El usuario insiste en encontrarse con el personal del INFOTEP en un lugar distinto al de las instalaciones para realizar una operación o pago en efectivo aun cuando existe los medios electrónicos.
4. El usuario trata de presionar a un servidor para no llenar los formularios requeridos por el INFOTEP.

5. El usuario realiza constantemente operaciones fraccionadas de pagos mediante dinero en efectivo como único medio de pago en lugar de utilizar los canales electrónicos o bancarios.

9.1 Medidas de prevención del lavado de activos y financiamiento de delitos, como el terrorismo en las operaciones del INFOTEP

- Cumplir y hacer cumplir por parte de los servidores, las disposiciones establecidas en la normativa vigente.
- Observar los convenios, tratados y acuerdos internacionales suscritos y ratificados por el Estado relacionados con el lavado de activos, las recomendaciones de la Unidad de Investigación de Análisis Financiero- UIAF, entre otras, así como las mejores prácticas internacionales, siempre que no contravengan la legislación nacional.
- Aplicar los lineamientos que adoptará la Institución frente a los factores de riesgo de exposición al lavado de activos, para la identificación, aceptación, permanencia y terminación de relaciones comerciales con usuarios o relaciones contractuales con contratistas o colaboradores estratégicos.
- Implementar los controles de debida diligencia para la selección y contratación de personal.
- Proteger la imagen del INFOTEP mediante el análisis y reporte de posibles operaciones de lavado de activos y financiamiento del terrorismo.

9.2 Evaluación del riesgo de lavado de activos y financiamiento de delitos, como el terrorismo en las operaciones del INFOTEP

- Identificar las categorías específicas de riesgos asociadas con los servicios, clientes o usuarios, Instituciones adscritas o vinculadas, contratistas o proveedores, así como la ubicación o localización geográfica, derivadas del perfil de cada uno.
- Realizar un análisis detallado de la cantidad, montos y tendencias de los diferentes factores de riesgo identificados, con el fin de analizarlos de manera eficaz.

9.3 Matriz de verificación en listas restrictivas (LA/FT)

La matriz que se presenta a continuación, sirve para verificar contrapartes en listas restrictivas cuando se analiza una operación inusual y sospechosa (ROS).

Lista / Base de datos	Entidad que la administra	Tipo de riesgo que identifica	Qué verificar	Acción si hay coincidencia
Lista OFAC – SDN (Lista Clinton)	Office of Foreign Assets Control	Narcotráfico, lavado de activos, crimen organizado,	Nombre de persona natural o jurídica, número de	Activar debida diligencia reforzada y analizar posible

		sanciones económicas	identificación, país	operación sospechosa (ROS)
Lista de sanciones ONU	Consejo de Seguridad de las Naciones Unidas	Terrorismo internacional, financiamiento del terrorismo, proliferación de armas	Coincidencias de nombre y nacionalidad	Suspender relación contractual y evaluar reporte
Notificaciones de Interpol	Interpol	Personas buscadas internacionalmente por delitos graves	Nombre completo y país de origen	Reportar internamente y evaluar relación con actividades ilícitas
Lista de sanciones Unión Europea	Unión Europea	Sanciones económicas, terrorismo, financiamiento ilícito	Persona o empresa sancionada	Realizar análisis de riesgo y documentar el hallazgo
Listas de Personas Expuestas Políticamente (PEP)	Autoridades nacionales y bases de datos especializadas	Riesgo de corrupción, soborno o conflictos de interés	Cargo público actual o pasado, familiares cercanos	Aplicar debida diligencia reforzada
Listas judiciales nacionales	Policía Nacional de Colombia	Órdenes de captura, investigaciones penales	Número de identificación y antecedentes	Analizar riesgo reputacional y documentar resultado

10. SEGUIMIENTO Y EVALUACION.



El seguimiento y evaluación de los procesos de debida diligencia deberán realizarse de manera periódica por la Oficina de Control Interno, con el fin de verificar la adecuada aplicación de los controles orientados a la prevención del lavado de activos, la financiación del terrorismo y otros riesgos asociados.

En cumplimiento de lo dispuesto en la Ley 87 de 1993, la Ley 1474 de 2011, la Ley 2195 de 2022 y la Resolución 1122 de 2021, la entidad deberá efectuar evaluaciones periódicas, como mínimo una vez al año, sin perjuicio de los seguimientos adicionales que se requieran según el nivel de riesgo identificado o los hallazgos detectados en los procesos de control interno.

El Comité Institucional de Gestión y Desempeño será el encargado de aprobar y/o modificar las directrices con respecto a la debida diligencia.

11. CONTROL DE CAMBIOS

Versión	Fecha de entrada en vigencia	Naturaleza del cambio
1	27/02/2026	Se elabora el manual con el fin de brindar lineamientos para la implementación de las medidas de debida diligencia en los distintos niveles de riesgo identificados en el INFOTEP de conformidad con la normatividad vigente en la materia