

VICEPRESIDENCIA AUDITORIA CORPORATIVA

GUÍA CORPORATIVA No. 53

CRITERIOS PARA LA GESTIÓN DEL RIESGO DE FRAUDE EN ISA Y SUS EMPRESAS

Aprobada en la Junta Directiva de ISA No. 871 del 25 de julio de 2022

Medellín, 29-JULIO-2022

1. PROPÓSITO

El Gobierno Corporativo de ISA y sus Empresas como parte del Grupo Ecopetrol recoge nuestra filosofía empresarial, las políticas, las reglas, los medios, las prácticas y los procesos, por medio de los cuales estas son dirigidas, operadas y controladas, buscando la eficiencia empresarial, potenciar el crecimiento, fomentar la confianza de los inversionistas en contextos nacionales e internacionales y administrar nuestros negocios con un enfoque de sostenibilidad empresarial, de manera responsable, transparente y ética.

En coherencia con lo anterior y convencidos de que la ética es el eje central de nuestras actuaciones, estructuramos el *Programa Empresarial de Ética y Compliance* que nos permite gestionar los eventos de riesgo de soborno, corrupción, fraude, lavado de activos, financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva que puedan afectar a ISA y/o sus Empresas, promoviendo a través de este, un comportamiento basado en la integridad de sus *Administradores*, trabajadores y *Terceros*, como principal medida de administración. Comportamiento que nos hace visibles como personas rectas, leales, justas, objetivas, honestas y transparentes ante la empresa y la sociedad. Una persona íntegra actúa en forma coherente con las características referidas, la normativa interna y externa aplicable, los principios y las reglas adoptadas por la organización.

Actuar conforme con este comportamiento nos permite afirmar que no se toleran los actos de soborno, corrupción, fraude, lavado de activos, financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva, ni ninguna conducta que falte a la ética.

Conscientes de que hoy en día, las crisis corporativas derivadas de la materialización de eventos de fraude son una realidad, sobrepasando el escenario clásico de hurto de efectivo y trascendiendo a nuevas modalidades como el engaño, el abuso de confianza, el dolo o simulación, potenciadas en el aprovechamiento de las facilidades y vulnerabilidades tecnológicas, se ha definido para ISA y sus Empresas la siguiente Guía para la Gestión del Riesgo Antifraude como un marco de referencia que busca formalizar su voluntad estratégica respecto a la gestión de este riesgo, declarando una cultura de no tolerancia a acciones ilegales o faltas a la ética y estableciendo las instrucciones y lineamientos específicos para su prevención, detección, investigación y respuesta.

2. ALCANCE

Esta guía es de obligatorio cumplimiento para los *Administradores*, trabajadores y *Terceros* con los cuales ISA y sus *Empresas* establezcan cualquier relación comercial y aplica a todos los negocios, procesos y actividades que estén expuestas al riesgo de fraude.

Es deber de los sujetos obligados, conocer y aplicar las modificaciones que se hagan a las instrucciones

y lineamientos aquí previstos una vez se realice su correspondiente divulgación, de acuerdo con los procedimientos previamente establecidos para ello.

En caso de duda en la aplicación de esta guía o ante el conocimiento de alguna situación que pudiera estar en contravía de los criterios definidos, se deberá informar y consultar con el jefe inmediato, la Línea Ética o *el Encargado de Cumplimiento* o quien haga sus veces, y de ser necesario, se solicitará el análisis *del Comité de Ética* u otras instancias adicionales.

Las faltas a las leyes que reglan las temáticas mencionadas en el objetivo y a los criterios incluidos en esta guía, no son aceptables y pueden resultar en acciones disciplinarias o legales, de acuerdo con los procedimientos definidos para el efecto por ISA y sus Empresas y por la *Normatividad Aplicable*.

Las palabras en letra cursiva utilizadas en este documento tendrán el significado indicado en las definiciones.

3. LINEAMIENTOS

ISA y sus *Empresas* establecen los siguientes criterios generales, que definen la voluntad de actuación frente a la prevención, detección, investigación y respuesta de posibles hechos de fraude. Estos criterios, son de obligatorio cumplimiento y no son discrecionales en su interpretación o aplicación:

- a) Se promueve una cultura de no tolerancia al fraude. Los *Administradores* y trabajadores marcan la pauta, a través de su actuar y sus decisiones, del compromiso irrestricto de ISA y sus *Empresas* con una posición intolerante a los hechos fraudulentos.
- b) El enfoque adoptado organizacionalmente es predominantemente preventivo, de tal forma que las vulnerabilidades son minimizadas desde su origen a través de adecuados criterios de diseño organizacional y fortalecimiento de la cultura empresarial.
- c) La exposición al riesgo de fraude es identificado y actualizado sistemática y periódicamente con base en las definiciones de la gestión integral de riesgos ISA y sus *Empresas*, con el fin de implementar medidas de administración efectivas que permitan su adecuada y oportuna gestión.
- d) ISA y sus *Empresas* generan un ambiente de colaboración y respeto de los intereses comunes, es por ello que desarrolla estrategias antifraude que contribuyan al fortalecimiento de relaciones de largo plazo y el logro de la sostenibilidad empresarial.
- e) Todos los *Administradores* y trabajadores deben reportar a través de la *Línea Ética* cualquier tipo de información, duda o sospecha de actos fraudulentos. Estos reportes serán manejados con absoluta reserva y garantizando su confidencialidad y protección de la identidad de quien reporta.
- f) Toda posible acción fraudulenta, independientemente de las cuantías, características o implicados, tendrá una respuesta de la administración, quien verificará los hechos reportados y tomará las acciones administrativas pertinentes, respetando lo establecido en la *Normatividad Aplicable*.
- g) Las *Empresas*, cuando sea procedente, pondrán en conocimiento de las autoridades competentes toda conducta que contraríe lo previsto en esta guía e igualmente emprenderán y acompañarán las acciones judiciales que sean pertinentes.
- h) En caso de presentarse un fraude, la información que requieran los públicos de interés a través de los canales formales establecidos para ello será transparente, imparcial, objetiva e informada de acuerdo con las definiciones internas aplicables, entre ellas, lo establecido en el protocolo para la gestión de crisis o el que haga sus veces.

4. MARCO CONCEPTUAL

4.1. CONCEPTOS

ISA y sus *Empresas* definen el fraude, como cualquier acto o su tentativa, u omisión realizada intencionalmente para obtener una ventaja indebida para beneficio propio, de la empresa o de *Terceros*, en detrimento de los principios e intereses organizacionales.

A. Factores Generadores de Riesgo de Fraude

El triángulo del fraude¹ es un modelo que explica los factores que llevan a una persona a realizar un fraude.



- **Motivación:** condiciones que motivan a una persona a beneficiarse a través de la empresa sea por: i) necesidad financiera y/o ii) presión para lograr una meta esperada, sea esta para alcanzar una meta de desempeño, obtener bonos o comisiones, mantener el puesto demostrando falsos buenos resultados, entre otros.
- **Oportunidad:** puede presentarse por dos razones: a) controles débiles en la organización: cuando no existen controles fuertes y se genera un entorno favorable para cometer actos irregulares. b) Abuso de confianza: El individuo se encuentra en una posición de confianza que le permite abusar de ella sin levantar sospechas, encontrando entonces una oportunidad para obtener un beneficio indebido a costa de la empresa.
- **Racionalización:** explicación racional que una persona puede formular para justificar una acción indebida, por ejemplo: “Solo estoy tomando prestado el dinero”, “Me lo deben porque me lo merezco”, “Es porque mi familia lo necesita”, “No me pagan lo suficiente para el trabajo que hago”.

B. Fuentes de Fraude

El fraude puede involucrar hechos deshonestos de *Administradores*, trabajadores y/o *Terceros*, por lo tanto, puede contextualizarse a partir de las siguientes fuentes que lo originan:

- **Fraude interno:** hechos fraudulentos realizados al interior de ISA y sus *Empresas* por parte de sus trabajadores y *Administradores*.
- **Fraude externo:** hechos fraudulentos realizados por *Terceros* externos a ISA y sus *Empresas*.
- **Fraude mixto:** hechos fraudulentos cometidos mediante el concurso o la participación de actores internos de las *Empresas* o personas externas, es decir, son aquellos hechos en los cuales uno de estos actores que cuentan con la complacencia o complicidad (por acción u omisión) de otro elemento de la cadena, con el propósito de cometer un fraude.

¹ El triángulo del fraude es un modelo diseñado por Donald R. Cressey.

4.2. TIPOLOGÍAS

El fraude está conformado por cuatro categorías principales, así:

A. FALSEDAD EN INFORMES

Creación, eliminación, modificación, alteración o divulgación de cualquier tipo de información financiera o no financiera tendiente a distorsionar la realidad del desempeño propio, de la empresa, o de *Terceros*. Incluye la supresión de información material (que afecte la toma de decisiones). A continuación, se incluyen algunos casos que no limitan la existencia de otros:

- Suministro de información falsa para encubrir desempeño deficiente o para acceder a bonificaciones.
- Utilizar falsos reportes para engañar a inversionistas, entidades financieras, reguladores o *Terceros* en general.
- Manipulación de estados financieros a través del reconocimiento inapropiado de ingresos, sobreestimación o subestimación de activos, subestimación de pasivos, estimados no acordes con la realidad del negocio, inadecuada clasificación de gastos de la empresa, el pago o no pago de impuestos, distribución de dividendos, reporte de utilidades, adulteración de registros contables, especulación.
- Ocultamiento y violación deliberada a normas cambiarias, impositivas, contables, de seguridad industrial, salud ocupacional, ambientales y en general de la *Normatividad Aplicable a ISA y sus Empresas*.
- Ocultamiento intencional de errores contables o de cualquier otra índole.
- Adulteración de documentos y/o facturas para obtener pagos o desembolsos indebidos.

B. MANEJO INADECUADO DE ACTIVOS DE INFORMACIÓN

Crear, acceder, eliminar, modificar, alterar, divulgar o usar activos de información de manera inapropiada y/o dolosa con fines indebidos o para beneficio personal, de la empresa o de *Terceros*. A continuación, se incluyen algunos tipos de activos de información contemplados en esta categoría, los cuales no limitan la existencia de otros adicionales:

- **Activos digitales de información:** es la información estructurada y no estructurada que reside en o se transmite mediante los elementos de tecnologías de información – TI – o las tecnologías operativas -TO - y a los cuales la empresa asigna un valor, que debe ser protegido.
- **Activos de información en otros medios físicos y/o electrónicos (videos, microfilmes, etc.):** es la información estructurada y no estructurada que reside en otros medios no digitales y que la organización directamente le asigna un valor, por lo cual debe protegerse.
- **Elemento de TI:** productos que soportan la gestión de activos digitales de información. Esto incluye, pero no está limitado a: estaciones de trabajo, sistemas operativos, dispositivos móviles, impresoras, software, medios de almacenamiento, servidores, cuentas de usuarios, navegación en Internet, redes, correo electrónico, servicio de transferencia de archivos, entre otros.

C. APROPIACIÓN O USO INDEBIDO DE RECURSOS FINANCIEROS Y OTROS BIENES DE LA EMPRESA

Cambio ilícito de destinación o uso indebido (malversación de activos) de los recursos financieros y otros bienes de la empresa y/o administrados por ella, para favorecer intereses propios, de la empresa o de *Terceros*. A continuación, se incluyen algunos casos contemplados en esta categoría, los cuales no limitan la existencia de otros adicionales:

- Apropiación o uso indebido de bienes, equipos o inventarios, malversación de fondos.
- Facturación de compañías fantasma, proveedores que no han prestado servicios, facturas sobrestimadas, gastos ficticios.
- Pagos dobles que se soportan en las mismas facturas.
- Uso de efectivo para fines distintos a los previstos o sin realizar el correspondiente registro o legalización.
- Pagos sobre bienes o servicios no recibidos o deficientes o de reembolsables sin justificación.
- Pago de reclamaciones que no tengan un soporte real
- Conceptos ficticios de compensación.
- Sobrepasso de los límites autorizados de gasto.
- Desviación de recursos de terceros administrados por la empresa.

D. CORRUPCIÓN Y OTROS ACTOS ILÍCITOS

Abuso de posiciones de poder o de confianza, para beneficio propio, de la empresa o de *Terceros*. A continuación, se incluyen algunos casos contemplados en esta categoría, los cuales no limitan la existencia de otros adicionales:

- Ofrecer, solicitar, prometer, dar, autorizar o recibir un *Beneficio Económico* a cambio de acciones, decisiones u omisiones para favorecimiento propio, de la empresa o de *Terceros*.
- Aceptar dádivas, para el empleado o sus familiares o *Terceros*, cuyo tipo y monto hayan sido expresamente prohibidas en el Código de Ética y Conducta u otro documento institucional.

5. ESTRUCTURA DE GOBIERNO

A continuación, se definen las responsabilidades específicas de los diferentes actores en la aplicación de esta guía:

JUNTA DIRECTIVA Y/O SUS COMITÉS

La Junta Directiva y/o los comités de junta que tengan esta responsabilidad, estarán encargados de:

- Aprobar la presente guía y sus actualizaciones.
- Dotar a los directivos de recursos que les permitan gestionar el riesgo del fraude.
- Dar lineamientos respecto de las medidas de administración o controles que se deban establecer para la gestión adecuada del riesgo de fraude.

COMITÉ DE AUDITORÍA O QUIEN HAGA SUS VECES

Complementariamente con lo definido en los Acuerdos de Junta Directiva (cuando aplique), el Comité de Auditoría o quien haga sus veces, tendrá las siguientes responsabilidades:

- Supervisar que la evaluación del riesgo de fraude se haga de manera adecuada y acorde con las características del negocio y se implementen las medidas efectivas de prevención, detección, investigación y respuesta.
- Supervisar los planes de acción tendientes a minimizar las vulnerabilidades de ISA y sus *Empresas* en términos de fraude.
- Conocer y hacer seguimiento sobre las denuncias de corrupción, soborno, fraude contable y financiero recibidas por ISA y sus *Empresas*.
- Recomendar mejoras para una adecuada gestión del riesgo de fraude.
- Supervisar el cumplimiento de la presente guía.
- Informar a la Junta Directiva y/o al Comité de Auditoría sobre los hechos de fraude.

COMITÉ DE ÉTICA

Complementariamente con las responsabilidades generales definidas en los *Comités de Ética* de cada compañía, tendrá las siguientes responsabilidades:

- Fomentar al interior de la organización una cultura de prevención del riesgo de fraude en cualquiera de sus tipologías.
- Dar a conocer al *Encargado de Cumplimiento* o a quien haga sus veces, las denuncias que sean puestas en su conocimiento relacionadas con posibles hechos fraudulentos, con el fin de acompañar en la gestión de estas y brindarle el apoyo necesario para ello.

DIRECTIVOS

Complementariamente con lo definido en la normatividad interna, la alta gerencia tendrá las siguientes responsabilidades:

- Propender por la implementación de mecanismos adecuados de prevención, detección, investigación y respuesta al fraude.
- Tomar las decisiones pertinentes en cuanto a las acciones administrativas y jurídicas necesarias respetando lo establecido en la *Normatividad Aplicable*.

ENCARGADO DE CUMPLIMIENTO O QUIEN HAGA SUS VECES

- Acompañar en conjunto con el área de riesgos, a los dueños de procesos en la identificación de posibles situaciones de riesgo y en la definición de las medidas de administración necesarias para su tratamiento.
- Realizar seguimiento al cumplimiento de lo aquí dispuesto por parte de los *Administradores*, trabajadores y *Terceros*.
- Aplicar rutinas de monitoreo que permitan identificar de manera temprana señales de alerta o eventos materializados de fraude
- Identificar y recomendar la incorporación de nuevos controles o mejoría a los existentes, con el fin mitigar la ocurrencia de eventos de riesgos de fraude o minimizar su impacto para ISA y sus *Empresas*.

- Coordinar con el área jurídica o quien haga sus veces, la atención de cualquier requerimiento, solicitud o diligencia de la autoridad competente judicial o administrativa en esta materia.
- Diseñar e implementar en conjunto con las áreas responsables de promover la cultura y realizar las comunicaciones, planes de capacitación y divulgación para dar a conocer lo aquí definido y las modificaciones a que hubiere lugar.
- Reportar a la Junta Directiva y/o sus comités, al *Comité de Ética* y otras instancias internas requeridas la gestión del riesgo de fraude.
- Reportar de manera oportuna al Comité de Auditoría, *Comité de Ética* y/o a la alta gerencia sobre cualquier posible situación de fraude que sea identificada para establecer el plan de tratamiento que sea aplicable. Una vez ejecutado dicho plan, reportar el resultado de este y realizar seguimiento a las acciones de mejora establecidas.
- Realizar (o soportarse en externos) las investigaciones necesarias para aclarar posibles eventos de fraude de forma independiente y mediante el empleo de recursos competentes, respetando siempre lo establecido en la *Normatividad Vigente*, para lo cual deberá adoptar un protocolo para este fin.

AUDITORÍA

Complementariamente, con lo definido en la normatividad interna, el Auditor Interno o quien haga sus veces, tendrá las siguientes responsabilidades:

- Planificar y llevar a cabo la evaluación del diseño y la efectividad de los controles antifraude.
- Participar activamente en la gestión integral del riesgo de fraude y emitir recomendaciones en cuanto a las estrategias más apropiadas para mitigarlos.
- Informar al Comité de Auditoría o quien haga sus veces, sobre las evaluaciones de control interno, auditorías, y actividades relacionadas.

TRABAJADORES

Es deber de los trabajadores acogerse a las disposiciones establecidas en el *Programa Empresarial de Ética y Compliance*, de igual manera en cumplimiento de este documento tienen como responsabilidad:

- Saber qué es un fraude y reconocer sus señales de alerta.
- Conocer, comprender y aplicar lo definido en esta guía.
- Mantener y ejecutar los controles antifraude en los procesos y actividades a su cargo y dejar evidencia de su cumplimiento.
- Todos los trabajadores son responsables de la correcta aplicación de la gestión integral de riesgos, mediante la identificación, evaluación, manejo, monitoreo, comunicación y divulgación de los riesgos asociados a sus procesos y de implementar mecanismos de verificación dentro del mismo proceso.
- Cooperar con las investigaciones relacionadas con fraude.
- Conocer y gestionar los riesgos de fraude de los procesos en los que participa.
- Participar en las actividades de divulgación y capacitación relacionadas con el *Programa Empresarial de Ética y Compliance* y mantenerse actualizado de sus modificaciones.

- Entregar a las instancias aquí señaladas, información completa, oportuna y veraz sobre riesgos de fraude asociados a su proceso o hechos fraudulentos de los que tenga conocimiento y reportarlos a través de la *Línea Ética*.

TERCEROS

- Comprometerse, entender y dar cumplimiento a lo aquí establecido en razón de las actividades relacionadas con el objeto de la relación comercial con ISA y/o sus *Empresas*.
- Informar a través de la *Línea Ética* de cada empresa, sobre posibles riesgos de fraude o de hechos fraudulentos de los cuales tenga conocimiento en razón del desarrollo de sus funciones objeto de la relación comercial con estas.

6. MECANISMOS DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y RESPUESTA

La evaluación de la exposición al riesgo de fraude es fundamental para lograr una gestión efectiva del mismo. Su análisis ayuda a:

- Comprender los posibles riesgos específicos de fraude a los que la empresa se ve expuesta.
- Identificar posibles deficiencias en su administración.
- Establecer e implementar mecanismos efectivos para su prevención, detección, investigación, y respuesta.

Dicha evaluación debe realizarse en forma sistemática y periódica tanto a nivel estratégico como de los procesos.

La evaluación del riesgo de fraude deberá estar enmarcada en la Política de Gestión Integral del Riesgo e incluir como mínimo la evaluación de escenarios o esquemas de fraude relevantes para la empresa, su probabilidad y severidad, determinando medidas de prevención, detección y protección. Esta evaluación deberá establecer planes de tratamiento adicionales (en caso de ser necesarios) para minimizar la vulnerabilidad en cada empresa.

Dicha evaluación será realizada por los responsables de los procesos con el soporte y acompañamiento del equipo de riesgos y/o el *Encargado de Cumplimiento* o quien haga sus veces, en caso de ser necesario.

A continuación, se exponen los mecanismos mínimos de prevención, detección, investigación y respuesta que ISA y sus *Empresas* deben implementar acorde con los criterios expuestos en esta guía:

A. PREVENCIÓN

Los mecanismos de prevención están destinados a minimizar la probabilidad de ocurrencia de casos de fraude y de esta manera, limitar la exposición a estos.

En este sentido es importante adoptar un enfoque coherente e integrado que tenga en consideración todo lo definido en ISA y sus *Empresas* desde las definiciones estratégicas, así como las operativas. De esta manera, se adopta una sólida estrategia de prevención del riesgo de fraude, y se propende por incorporarla en la gestión del día a día. A continuación, se describen algunos elementos relevantes que se deben considerar para esta gestión:

TONO DE LA GERENCIA

Se establece una cultura de no tolerancia al fraude y el compromiso de fortalecer el sistema de control interno a través de la incorporación y cumplimiento de las medidas necesarias para su prevención, detección, investigación y respuesta, entre las cuales se encuentran algunas de las que se mencionan a continuación.

PRÁCTICAS DE GESTIÓN DEL TALENTO HUMANO

Dada la importancia del factor humano en la prevención de los riesgos, en particular de fraude, es necesario que cada empresa evalúe los mecanismos existentes, relacionados con los procesos para la gestión del talento humano y se establezca la suficiencia y pertinencia de los mismos en este propósito.

PROGRAMAS DE AUTOCONTROL

Un criterio fundamental en la gestión del riesgo de fraude es el autocontrol, de tal forma que todos los trabajadores ejecuten en forma efectiva y eficiente las actividades y procesos que administran en su gestión diaria.

PRÁCTICAS DE CONTRATACIÓN

De acuerdo con los principios para la contratación, la transparencia entendida como llevar a cabo los procesos de contratación con base en los procedimientos de selección objetiva que garanticen la calidad, imparcialidad e igualdad de oportunidades, es un criterio clave para la prevención del riesgo de fraude.

Con respecto a la gestión específica del riesgo de fraude, es necesario que cada empresa considere lo definido en la Directriz Corporativa para el Gobierno y Gestión de la Cadena de Aprovisionamiento y evalúe los mecanismos existentes, relacionados con los procesos para la adquisición de bienes y servicios, con el fin de que se considere la prevención del riesgo de fraude, se determine su suficiencia y pertinencia en este propósito, y se establezcan otros elementos adicionales, en caso de requerirlo.

Adicionalmente, se deberán ajustar los procedimientos existentes en cada empresa, de tal forma, que lo aquí definido sea de obligatorio cumplimiento, tanto cuando se actúa como contratante y contratista.

PROGRAMA EMPRESARIAL DE ÉTICA Y COMPLIANCE

Las definiciones contenidas en el *Programa Empresarial de Ética y Compliance*, son de obligatorio cumplimiento y tienen como propósito principal prevenir la ocurrencia de riesgos de Compliance, entre ellos el riesgo de fraude.

LÍNEA ÉTICA

La *Línea Ética* tiene un enfoque preventivo en la medida que actúa como mecanismo de consulta y reporte de situaciones de riesgo de fraude potenciales que pueden ser denunciadas por los *Terceros*. La información allí recibida se gestiona con base en la Guía Corporativa para la Gestión de Asuntos Éticos.

AUDITORÍAS

La realización de auditorías periódicas en ISA y sus *Empresas*, actúa como un mecanismo preventivo, y constituyen un elemento fundamental dentro del sistema de control interno y ayudan a generar un adecuado ambiente de control.

Las auditorías realizadas deben contribuir en la identificación preventiva de aspectos por mejorar en la gestión del riesgo de fraude.

SEGURIDAD DE LA INFORMACIÓN

En ISA y sus *Empresas*, se valora y se protege la información, el conocimiento y los productos, como activos relevantes.

Con base en lo anterior, se disponen de principios, modelos, guías institucionales y procedimientos tendientes a garantizar la seguridad de la información y de los sistemas.

En cuanto a seguridad de la información, se destacan no siendo las únicas, las Guías Corporativas para la Gestión y Uso de la Tecnología de la Información y las Telecomunicaciones, y de Divulgación de Información Pública, así como también las definiciones de cada empresa en lo relacionado con la protección de datos personales, la protección de la propiedad intelectual, derechos de autor y propiedad industrial.

Complementariamente con lo anterior, ISA y sus *Empresas* promueven la implementación permanente y sistemática de mejores prácticas de seguridad de la información y controles tecnológicos, incluyendo desde su estructuración, la gestión del riesgo de fraude.

B. DETECCIÓN

De acuerdo con lo establecido en el marco de actuación de esta guía, se deben implementar mecanismos efectivos que permitan detectar oportunamente posibles hechos fraudulentos, con el objetivo de minimizar su impacto. Estas medidas deberán ser complementarias con el enfoque preventivo que se define a nivel corporativo, y para cada proceso. Algunos mecanismos son:

MONITOREO PERMANENTE

Los esquemas de control interno establecidos en los procesos deben permitir la identificación de desviaciones en los mismos de tal forma que se advierta en forma temprana la posible ocurrencia de hechos que contraríen lo dispuesto en esta guía.

AUDITORÍA INTERNA

Los sistemas de auditoría y seguimiento diseñados en forma razonable para detectar fraudes y conductas irregulares son herramientas importantes utilizadas para determinar si los controles de ISA y sus *Empresas* están cumpliendo con su función.

LÍNEA ÉTICA

La *Línea Ética* de cada empresa tiene un enfoque detectivo en la medida que actúa como mecanismo de consulta y reporte de hechos sospechosos de fraude. La información allí recibida se gestiona con base en la Guía Corporativa para la Gestión de Asuntos Éticos.

UTILIZACIÓN DE TECNOLOGÍA

ISA y sus *Empresas* han dispuesto la tecnología para apoyar los procesos de negocio y facilitar el flujo de información natural entre procesos y entre sus *Empresas* en un ámbito de seguridad

tecnológica con criterios de confidencialidad, confiabilidad y disponibilidad.

Adicional a los controles de detección tradicionales, la empresa se reserva el derecho de monitorear su ambiente tecnológico con el objetivo de evitar y detectar posibles eventos de fraude en el ambiente tecnológico, respetando la confidencialidad de la información en el marco de la *Normatividad Aplicable*.

Adicionalmente, se propende por la implementación efectiva de alertas tempranas en los procesos y esquemas de monitoreo continuo.

En el Anexo – Señales de Alerta se enuncian posibles señales de alerta que pueden darse en algunos procesos organizacionales, no siendo las únicas que puedan presentarse.

C. INVESTIGACIÓN

Los mecanismos de investigación están destinados a adelantar las acciones necesarias para aclarar posibles hechos de fraude. Cuando se disponga de información sobre conductas fraudulentas, bien sea potenciales o reales, ISA y sus *Empresas*, adelantarán las verificaciones necesarias en forma objetiva y exhaustiva. El objetivo de tales verificaciones será recolectar información pertinente, de modo que la administración de la empresa pueda decidir la línea de actuación a seguir.

La investigación será adelantada por el *Encargado de Cumplimiento* o quien haga sus veces, en acompañamiento de las áreas organizacionales requeridas o con el apoyo de externos, con base en lo dispuesto en la Guía Corporativa para la Gestión de Asuntos Éticos y será realizada respetando siempre la *Normatividad Aplicable* en cada país.

D. RESPUESTA

Los mecanismos de respuesta están destinados a tomar las medidas correctivas y reparar, en lo posible, el daño ocasionado por el fraude. Consecuente con lo establecido en los criterios definidos de esta guía, los hechos fraudulentos, debidamente soportados y analizados, tendrán la respuesta administrativa y legal acorde con lo establecido en la normatividad interna y la *Normatividad Aplicable* en cada país.

En caso de tratarse de un contratista se iniciarán las acciones contractuales respectivas y será causal de terminación del contrato de acuerdo con lo establecido en el mismo. En todos los casos se propenderá por el resarcimiento del daño causado.

Como parte de la gestión que se realice, se deberán diseñar e implementar acciones correctivas orientadas a contener el impacto del evento, entre ellas y cuando aplique, la activación del protocolo para la gestión de crisis reputacional.

Otros elementos adicionales para considerar son:

MANEJO DE INCIDENTES

En caso de presentarse un fraude, se estudiarán sus causas, las debilidades de control detectadas y se presentará un plan de respuesta, garantizando que se ha administrado el riesgo y que se fortalecerán los controles. Se generará un aprendizaje del incidente para evitar su recurrencia, teniendo en cuenta aspectos como: rediseño de procesos, planes de mejoramiento, actualización de evaluación de riesgos determinando si es necesario modificar el perfil y posibles ajustes en controles.

TRANSFERENCIA DEL RIESGO

Con el objetivo de minimizar el impacto de las pérdidas y daños causados, ISA y sus *Empresas*, mantendrán vigentes los mecanismos de transferencia de riesgos que consideren pertinentes, acorde con la evaluación de riesgos realizada.

7. DIVULGACIÓN Y CAPACITACIÓN

Será responsabilidad del *Encargado de Cumplimiento* o quien haga sus veces, en conjunto con las áreas de comunicaciones en cada empresa, divulgar los cambios realizados a esta guía a través de los medios definidos para ello, entre ellos, a través de capacitaciones, cuando así se requiera.


No obstante, lo anterior, todos los destinatarios de este documento serán responsables de mantenerse actualizados respecto de su contenido.

8. DEFINICIONES

- **Administradores:** son los miembros de juntas directivas, directorios o consejos directivos, los representantes legales, los trabajadores del nivel directivo y quienes de acuerdo con las leyes del país correspondiente y los estatutos sociales de ISA o la respectiva Empresa, tengan el carácter de administrador o directivo.
- **Beneficio Económico:** es cualquier cosa de valor. Puede ser efectivo o equivalentes de efectivo, tales como: certificados o bonos de Regalo, el pago de gastos o deudas, Regalos, viajes, alojamiento. También beneficios intangibles, oportunidades de empleo para un *Tercero*, un Funcionario Público o sus familiares, oportunidades para hacer negocios con ISA o sus Empresas o invitaciones para asistir a Eventos exclusivos. No se incluyen en esta definición los regalos, atenciones e invitaciones a eventos que cumplan con los criterios definidos en este documento y en la Guía Corporativa de Gestión Anticorrupción y Antisoborno.
- **Comité de Ética:** es el comité conformado en ISA y en cada *Empresa* para obrar como órgano de consulta que oriente a los trabajadores y *Terceros* en general, en la aplicación de los principios declarados en el Código de Ética y Conducta de ISA y sus *Empresas*. Cuando esta guía se refiera a este comité debe entenderse que se hace referencia al Comité de Ética de ISA o de la Empresa empleadora del trabajador, o en la cual se tenga el carácter de Administrador, según corresponda.
- **Empresas:** son las sociedades controladas directa o indirectamente por ISA.

- **Encargado de Cumplimiento:** es la persona o área designada por ISA o sus Empresas para gestionar el cumplimiento del *Programa Empresarial de Ética y Compliance* en cada una de ellas.
- **Línea Ética:** es el canal dispuesto por ISA y en cada *Empresa* para que los *Terceros* puedan consultar o reportar posibles incumplimientos al *Programa Empresarial de Ética y Compliance*.
- **Normatividad Aplicable:** cualquier ley, ordenanza, regulación, directiva, orden, decreto, decisión judicial o administrativa, que sea vinculante para ISA y sus *Empresas* en cualquier jurisdicción.
- **Programa Empresarial de Ética y Compliance:** es el conjunto de principios, directrices, guías y procedimientos definidos por ISA y sus *Empresas* para identificar, detectar, prevenir, gestionar y mitigar los riesgos de soborno, corrupción, fraude, lavado de activos y financiación del terrorismo y de la proliferación de armas de destrucción masiva, que puedan afectar a ISA o sus *Empresas*, y promover el comportamiento ético de sus *Administradores*, trabajadores y *Terceros*.
- **Tercero:** contratista, proveedor, distribuidor, consultor, intermediario, subcontratista, accionista, inversionista, cliente, Funcionario Público, y en general todo aquel con quien se establezca una relación comercial, contractual o de cooperación, así como los familiares de los *Administradores* y trabajadores de ISA y sus *Empresas*.

La presente Guía Corporativa rige a partir de su expedición y publicación en la Intranet Corporativa.

DocuSigned by:

4E52CFF42B664E8...

Carlos Ignacio Mesa Medina
Vicepresidente Auditoría Corporativa

ANEXO – SEÑALES DE ALERTA

A continuación, se enuncian algunas señales de referencia para algunas temáticas:

Temática	Señales
Gestión Financiera	<p>Gestión de Recaudo</p> <ul style="list-style-type: none"> - Ajustes recurrentes a saldos de cuentas por cobrar indicados como devoluciones, descuentos y rebajas - Registro Manual de recaudos no relacionados con una factura <p>Gestión de Tesorería Alto número de rechazos en las transacciones de banca electrónica</p> <ul style="list-style-type: none"> - Cheques girados a favor de un tercero sin restricción, que pueden ser endosados falsamente y/o consignarse en cuentas de particulares - Cuentas bancarias inactivas o no saldadas que aprovechado su invariabilidad pueden ser utilizadas indebidamente - Cheques consignados en cuenta de la empresa sin identificar - Expedir cheques al portador que facilitan la falsificación del endoso - No efectuar arqueos de caja, recibos de caja anulados, sin soporte o faltantes en el consecutivo. - Diferencias sin explicación en arqueos de caja <p>Gestión Cuentas por Pagar</p> <ul style="list-style-type: none"> - Cuentas por pagar que superan el plazo establecido en la política de pagos - Pagos: realizados antes de lo convenido; o recurrentes a proveedores por el mismo valor - Incremento injustificado en el valor a pagar a un proveedor <p>Gestión Contable</p> <ul style="list-style-type: none"> - Saldos contrarios por montos significativos a la naturaleza de las cuentas contables - Conciliaciones bancarias incompletas o con poca claridad - Partidas conciliatorias con antigüedad considerable y/o que no estén justificadas - Falta de conciliación entre módulos y los registros del libro mayor - Comprobantes manuales sin soportes - Omisión de información en transacciones y/u operaciones relacionadas con partes relacionadas <p>Gestión de Activos</p> <ul style="list-style-type: none"> - Cambios en los valores de depreciación / amortización sin movimientos importantes de activos que los soporten - Cambios de estado de los activos sin justificación - Registro incompleto de datos de identificación del activo - Registro de transacciones en horarios no laborales <p>Gestión de datos maestros</p> <ul style="list-style-type: none"> - Cambio sin justificación en el cupo de crédito de los clientes (en los negocios que aplique) - Clientes desconocidos y/o con información no veraz - Cambio sin justificación en los datos maestros de terceros
Gestión de los activos	<ul style="list-style-type: none"> - Alto número de transferencias de materiales entre diversos proyectos - Materiales y suministros mantenidos físicamente, pero que no están asignados a ningún almacén - Diferencias en tomas físicas de inventarios y materiales que no se encuentre debidamente justificadas - Demoras injustificadas en la formalización de los cierres de proyectos y su debida capitalización - Desviaciones importantes no justificadas en la culminación de proyectos o en los costos incurridos en relación con las estimaciones iniciales del costo del proyecto - Pagos por alquiler de equipos y materiales que exceden su costo real o del mercado - No se realizan tomas físicas sobre el inventario de activos fijos - Baja frecuencia de tomas físicas de inventarios de materiales y activos de mantenimiento - Ajustes frecuentes en los registros de inventarios. - Cambios importantes en la rotación del inventario, especialmente para aquellos ítems que son de lento movimiento - Reversar entradas de material de la cuenta de inventario después del cierre del período contable - Inventarios que se conservan fuera de los almacenes de las locaciones operativas - Recepción de materiales que no han sido solicitados - Ingreso o retiro de inventario por cantidades diferentes a las solicitadas en la orden de pedido de forma recurrente para un tercero o algún tipo de material - Limitaciones a la inspección física y detallada de los activos fijos y materiales - Debilidades en la segregación funcional entre el responsable del activo y la persona que lo registra en el sistema - Activos fijos sin identificación o asignación de código en el sistema

Temática	Señales
Ingresos	<ul style="list-style-type: none"> - Aumentos inusuales en las ventas en los meses cercanos al cierre del período - Inconsistencias recurrentes entre la documentación de trámites aduaneros (importación/exportación) y la información de la transacción - Mercancías facturadas por ventas a clientes son descargadas de inventarios en el siguiente período o viceversa - Porcentajes de descuentos otorgados que se encuentran por encima de los autorizados en la política de la Compañía - Alto nivel de ventas a intermediarios sin conocer el destino final de la venta
Gestión de Abastecimiento	<ul style="list-style-type: none"> - Alto número de procesos de compra a través de adjudicación "directa" - Proveedores asociados a un único gestor de abastecimiento, incrementa la posibilidad de manejos indebidos - Clausulas adicionales recurrentes a los términos de referencia en contrataciones - Órdenes de compra que no tengan entradas de almacén, recepción de servicios - Cambios continuos en las estrategias de liberación que no están soportados en cambios de la estructura organizacional o las áreas. - Aumento de consumos y/o requisiciones de compras en un periodo, sin estar considerados o alineados al Plan de Compras y Contratación - Inadecuada correlación entre los resultados de incumplimientos o incidentes operacionales bajo la responsabilidad del tercero y los resultados de las evaluaciones de desempeño - Aumento en las excepciones administrativas del proceso de compras y contratación
Gestión del Talento Humano	<ul style="list-style-type: none"> - Variaciones significativas (frente al promedio) en los costos de nómina y beneficios, concentra dos en ciertas locaciones operativas de la Empresa o áreas geográficas, sin que existan cambios importantes en la estructura organizacional o de beneficios - Alto nivel de rotación de personal gerencial o clave para el sistema de control de la compañía - Que la información del archivo maestro de empleados/beneficiarios no esté completa o que no esté actualizada - Diferentes empleados/beneficiarios con la misma dirección o número de teléfono - Solicitudes de reembolsos por gastos de viaje u otros asumidos por el empleado, que no cuenten con los soportes respectivos - Partidas conciliatorias de nómina, superiores a 30 días, sin contar con regularización - Aumento en los casos por falsedad en documentos presentados por aspirantes
Gestión de Tecnología de la Información	<ul style="list-style-type: none"> - Alto nivel de informalidad en el proceso de control de cambios a las aplicaciones y bases de datos - Personal de tecnología informática con accesos a registrar transacciones en los sistemas de información de la empresa - Ejecución de tareas críticas de administración y/o desarrollo de los sistemas de información por parte de terceros - Alto número de usuarios con privilegios en el sistema sin responsabilidad funcional relacionada - Sistemas de información transaccionales que pueden ser accedidos de forma remota sin los debidos controles de seguridad - Alto volumen de incidentes de seguridad informática - Ausencia de un esquema adecuado de segmentación de la red interna de datos de la compañía - Existencia de un alto volumen de procesos fallidos de cargue, salida o procesamiento de datos - Los logs de auditoría de los sistemas de información y sus bases de datos no están activas y/o no se realiza un seguimiento periódico al contenido de estas
Gestión de Proyectos	<ul style="list-style-type: none"> - Indicadores contradictorios de ejecución física del proyecto frente a la ejecución presupuesta - La estructura organizacional de las áreas que gestionan proyectos es limitada para mantener una adecuada segregación funcional entre las responsabilidades de Gestoría e interventoría - Alto número (Por encima del promedio) de reclamos o fallas técnicas, relacionadas con un proyecto o proveedor - Alto número (Por encima del promedio) de reclamos de proveedores o contratistas, relacionados con un proyecto o proveedor - Alto porcentaje de controles manuales para monitorear los proyectos - Cambios o ajustes continuos al alcance del proyecto - Acuerdos de confidencialidad no usados o sin formalizar - Alto número de adiciones (OtroSI) a los contratos originales
Negociación de Tierras	<ul style="list-style-type: none"> - Valores dispares (no congruentes) en la negociación de tierras en una misma zona geográfica o en tierras de características similares - Alto nivel de reclamos en zonas geográficas específicas, relacionadas con el tema de tierras - Requerimientos recurrentes de veedurías u órganos reguladores, relacionados con el tema de tierras - Costos de intermediación o comisiones para la negociación de tierras, registrados como mayor valor de un proyecto.

Temática	Señales
Servicios Jurídicos	<ul style="list-style-type: none"> - Alto número de procesos judiciales (a favor o en contra de la Empresa) concentrados en uno o pocos abogados externos - Alto número de procesos judiciales (de diverso tipo) en contra de la Empresa, concentrados en algunas locaciones geográficas - Alto nivel de rotación (Superior al promedio) de abogados encargados en un proceso judicial crítico. - Alto número de fallos judiciales en contra de la compañía
HSE	<ul style="list-style-type: none"> - Volumen importante de quejas y/o reclamos por incumplimiento de normas ambientales, de seguridad o de salud ocupacional - Requerimientos reiterados de la autoridad y/o regulador ambiental a operaciones específicas - Requerimientos reiterados de la autoridad y/o regulador en Salud Ocupacional a operaciones específicas - Cambios o alteraciones en los documentos soporte de medicina laboral (ejemplo habilitación para trabajo en alturas).

Certificado de finalización

Identificador del sobre: 2D85A90C5A944C2BB5B3F3D07D8B5EC3
 Asunto: Aplicar DocuSign a: GuiaAntifraude_ISA_Empresas_25072022_Aprobada.docx
 Sobre de origen:
 Páginas del documento: 16 Firmas: 1
 Páginas del certificado: 3 Iniciales: 0
 Firma guiada: Activado
 Sello del identificador del sobre: Activado
 Zona horaria: (UTC-05:00) Bogotá, Lima, Quito, Rio Branco

Estado: Completado

Autor del sobre:
 NANCY CATALINA OTÁLVARO GÓMEZ
 Calle 12 sur N° 18 - 168 Bloque 1
 Medellín, 050022
 notalvaro@ISA.com.co
 Dirección IP: 200.24.1.3

Seguimiento de registro

Estado: Original
 28/07/2022 17:58:47

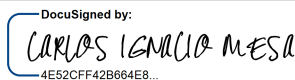
Titular: NANCY CATALINA OTÁLVARO GÓMEZ
 notalvaro@ISA.com.co

Ubicación: DocuSign

Eventos de firmante

CARLOS IGNACIO MESA
 cmesa@ISA.com.co
 Vicepresidente Auditoría Corporativa
 ISA
 Nivel de seguridad: Correo electrónico,
 Autenticación de cuenta (ninguna)

Firma

DocuSigned by:

 4E52CFF42B664E8...

Adopción de firma: Estilo preseleccionado
 Utilizando dirección IP: 200.24.1.3

Fecha y hora

Enviado: 28/07/2022 17:59:59
 Reenviado: 29/07/2022 9:19:16
 Visto: 29/07/2022 11:50:31
 Firmado: 29/07/2022 11:50:54

Información sobre confidencialidad de registros y firmas electrónicas:

No ofrecido a través de DocuSign

Eventos de firmante en persona**Firma****Fecha y hora****Eventos de entrega al editor****Estado****Fecha y hora****Eventos de entrega al agente****Estado****Fecha y hora****Eventos de entrega al intermediario****Estado****Fecha y hora****Eventos de entrega certificada****Estado****Fecha y hora****Eventos de copia de carbón****Estado****Fecha y hora**

ARCHIVO
 archivo@INTERCOLOMBIA.com
 Nivel de seguridad: Correo electrónico,
 Autenticación de cuenta (ninguna)

Copiado

Enviado: 29/07/2022 11:50:56
 Visto: 29/07/2022 12:10:51

Información sobre confidencialidad de registros y firmas electrónicas:

Aceptado: 27/07/2022 9:10:32
 ID: 3218659f-3498-4fee-ab69-5b5424027e58

Eventos del testigo**Firma****Fecha y hora****Eventos de notario****Firma****Fecha y hora****Eventos de resumen de sobre****Estado****Marcas de tiempo**

Sobre enviado Con hash/cifrado
 Certificado entregado Seguridad comprobada
 Firma completada Seguridad comprobada
 Completado Seguridad comprobada

28/07/2022 17:59:59
 29/07/2022 11:50:31
 29/07/2022 11:50:54
 29/07/2022 11:50:56

Eventos del pago**Estado****Marcas de tiempo**

CONFIDENCIALIDAD DE REGISTROS Y FIRMAS ELECTRÓNICAS

Para el uso de esta herramienta necesitamos su autorización para el uso de datos personales y manejo de la firma electrónica. En caso de estar de acuerdo, favor hacer click en el botón "Acepto Usar registros y firmas electrónicas" y click en "CONTINUAR".