



CÓDIGO ANTIFRAUDE

Octubre de 2011

CONTENIDO

	Pág.
INTRODUCCIÓN	
1. OBJETIVO	4
2. MARCO DE REFERENCIA CORPORATIVO	5
3. MARCO CONCEPTUAL	6
4. MARCO DE ACTUACIÓN	8
5. ESTRUCTURA DE GOBIERNO	10
6. MECANISMOS DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y RESPUESTA	12
7. ÁMBITO DE APLICACIÓN Y SEGUIMIENTO	16

INTRODUCCIÓN

La inteligencia, la creatividad y la capacidad para el planeamiento estratégico y la gestión de riesgos son algunos atributos asociados con condiciones positivas del ser humano. Sin embargo, estas mismas variables pueden resultar tremendamente dañinas en manos de individuos que tengan como intención conseguir beneficios de forma inapropiada, individuos motivados por el interés de cometer un fraude.

Hoy en día, las crisis corporativas derivadas de la materialización de eventos de fraude son una realidad. El fraude se ha convertido en un hecho posible de la vida corporativa, sobrepasando el escenario clásico de hurto de efectivo y trascendiendo a nuevas modalidades como el engaño, el abuso de confianza, el dolo o simulación. Puede ser realizado de forma intencional, lo cual trae consigo implicaciones como la manipulación, la falsificación o alteración de registros o documentos, la malversación de activos, la eliminación u omisión de los efectos de ciertas transacciones en los registros o documentos, el registro de transacciones sin respaldo y la mala aplicación de políticas contables. Implicaciones que son potenciadas aprovechando las facilidades y vulnerabilidades de las nuevas herramientas tecnológicas.

Consecuente con esta realidad, la alta dirección debe capacitar a la Organización para anticiparse a este tipo de eventos y estar preparada para gestionarlos adecuadamente, salvaguardando ante sus distintos grupos de interés (accionistas, colaboradores, proveedores, clientes, sociedad y Estado) cualquier tipo de activo, con énfasis en los recursos financieros, de información e imagen corporativa.

Por lo tanto, desde su Marco de Referencia Corporativo, ISA y sus empresas:

- Establecen un relacionamiento fundado en valores, políticas y compromisos que fortalecen la identidad corporativa y la coherencia institucional;
- Promueven la gestión bajo un ambiente ético y de autocontrol;
- Establecen los límites que guían la acción empresarial y,
- Desarrollan procesos que aseguren la gestión de sus riesgos.

Adicionalmente, incorporan buenas prácticas empresariales específicas en temas de prevención y administración de acciones fraudulentas.



1. OBJETIVO

El Código Antifraude de ISA y sus empresas, es un marco de referencia que busca formalizar su voluntad estratégica respecto al fraude, declarando una cultura de no tolerancia y estableciendo lineamientos corporativos y responsabilidades para su prevención, detección, investigación y respuesta.



2. MARCO DE REFERENCIA CORPORATIVO

La interpretación y aplicación de este Código deberá ser coherente con lo definido en el Marco de Referencia Corporativo de ISA y sus empresas, guardando una especial atención en los siguientes elementos relacionados:

- **Valores Corporativos**

Identifican su querer ser y hacer, sustentan su confianza y credibilidad, su forma de conducta y la manera como se quiere ser reconocido.

Los valores definidos son: ética, responsabilidad social, excelencia e innovación.

- **Código de Buen Gobierno**

En este documento, ISA define una serie de prácticas respecto de su gobierno, su conducta y su información, para que las actuaciones de los accionistas, administradores, directivos y colaboradores estén orientadas a garantizar la integridad ética empresarial, el adecuado manejo de sus asuntos, el respeto de quienes invierten en ella, el cumplimiento de los compromisos con sus grupos de interés y el conocimiento público de su gestión.

- **Código de Ética**

Brinda un marco de referencia que busca materializar la filosofía y los valores corporativos de la Organización, a través de criterios orientadores para la actuación de todos sus trabajadores y miembros de sus Juntas Directivas en el que se rechaza, explícitamente cualquier tipo de fraude.

- **Políticas Empresariales**

Definen criterios y establecen marcos de actuación que orientan la gestión de todos los niveles de la organización en aspectos como el control interno, la comunicación, la información y el conocimiento, la adquisición de bienes y servicios, lo ambiental, el servicio, la gestión humana, la inversión, la salud ocupacional, lo social y la gestión integral de riesgos.



3. MARCO CONCEPTUAL

ISA y sus empresas definen el fraude, como cualquier acto o su tentativa, u omisión realizada intencionalmente para obtener un provecho indebido, en detrimento de los principios e intereses organizacionales. El fraude está conformado por cuatro categorías principales, así:

3.1. Apropriación o uso indebido de recursos financieros y otros bienes de la empresa

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

- Apropriación o uso indebido de bienes, equipos o inventarios, malversación de fondos, pagos a proveedores ficticios, pagos dobles, manipulación de excedentes de tesorería, apropiación de dineros, inadecuada utilización de fondos de caja menor, entre otros, cuya propiedad sea de la empresa o administrados por ella.
- Conceptos ficticios de compensación.
- Sobrepasso de los límites autorizados de gasto.

3.2. 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. 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 - y a los cuales la organización 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 distintos al digital 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.

3.3. Corrupción

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

- Ofrecer o solicitar, entregar o recibir, bienes en dinero o en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.



- Aceptar dádivas, para el empleado o sus familiares, cuyo tipo y monto hayan sido expresamente prohibidas en el Código de Ética u otro documento institucional.

3.4. Falsedad en informes

Creación, eliminación, modificación, alteración o divulgación de cualquier tipo de información tendiente a distorsionar la realidad del desempeño propio, de la empresa en general, o de terceros. Incluye la supresión de información material (que afecte la toma de decisiones). A continuación se incluyen algunos casos contemplados en esta categoría, los cuales no limitan la existencia de otros adicionales:

- 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: reconocimiento inapropiado de ingresos, sobreestimación o subestimación de activos, subestimación de pasivos, estimados significativos y no acordes con la realidad del negocio, entre otros.
- Ocultamiento y violación deliberada a normas cambiarias, impositivas, contables, de seguridad industrial, salud ocupacional, ambientales, del mercado energético, en general de la normatividad aplicable a ISA y sus empresas.
- Ocultamiento de errores contables.

El fraude puede involucrar hechos deshonestos de clientes, proveedores, representantes, competidores, colaboradores, ex colaboradores, administradores, directivos o terceros en general, por lo tanto, el fraude puede contextualizarse a partir de las fuentes que lo originan:

- **Fraude interno:** hechos fraudulentos realizados al interior de las empresas por parte de sus trabajadores, directivos, administradores o representantes.
- **Fraude externo:** hechos fraudulentos realizados por personas externas a ISA y sus empresas, como proveedores, contratistas, clientes y terceros en general.
- **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.



4. MARCO DE ACTUACIÓN

Para ISA y sus empresas, la ética, como valor de valores, es un elemento diferenciador y dinamizador de sus negocios, lo que implica que su gestión sea ejecutada dentro de los más altos estándares de transparencia y buenas prácticas empresariales, dentro de las cuales se incorpore una cultura de prevención y administración de acciones fraudulentas.

Consecuente con ello, 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 fraudulentos. Estos criterios, son de obligatorio cumplimiento y no son discrecionales en su interpretación o aplicación:

1. Se promueve una cultura de no tolerancia al fraude. Los administradores, directivos y colaboradores 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.
2. 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 programas de transformación cultural.
3. La exposición al riesgo de fraude es evaluada sistemática y periódicamente con el fin de implementar medidas de administración efectivas que permitan su adecuada y oportuna detección y gestión.
4. En el ámbito de las relaciones de confianza establecidas con los diferentes grupos de interés, ISA y sus empresas generan un ambiente de colaboración mutua 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.
5. Todos los administradores, directivos y colaboradores deben reportar a través de a su superior inmediato, a la línea ética, al área de auditoría o al Comité de Ética, cualquier tipo de información, duda o sospecha de actos fraudulentos. Este tipo de reportes serán manejados con absoluta reserva y garantizando su confidencialidad.
6. 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.
7. Las empresas, cuando sea procedente, pondrán en conocimiento de las autoridades competentes toda conducta que contraríe lo previsto en este Código e igualmente emprenderán y acompañarán las acciones judiciales que sean pertinentes.
8. En caso de presentarse un fraude, la información que requieran los públicos de interés será transparente, imparcial y objetiva, conforme a lo establecido en la Política de Información y del Conocimiento, en la Política de Comunicación y en



particular, en los principios definidos en el Manual de Comunicación para la Mitigación de Riesgos y Crisis de Reputación.



5. ESTRUCTURA DE GOBIERNO

A continuación se definen las responsabilidades específicas de los diferentes actores en la aplicación de este protocolo antifraude:

5.1. Junta Directiva

Dentro de las responsabilidades relacionadas con la adopción de medidas específicas con respecto al Gobierno de la Sociedad, la Junta Directiva es la encargada de:

- Aprobar el presente protocolo antifraude y sus actualizaciones.
- Dotar a los directivos de los elementos materiales y humanos 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 fraude.

5.2. Comité de Auditoría

Complementariamente con lo definido en los Acuerdos de Junta Directiva, el Comité de Auditoría tendrá las siguientes responsabilidades:

- Verificar que la evaluación de riesgos de fraude se haga de manera adecuada y acorde con las características del negocio y se implementen medidas efectivas de prevención, detección, investigación y respuesta.
- Supervisar los planes de acción tendientes a minimizar las vulnerabilidades de las empresas en términos de fraude.
- Dar lineamientos respecto de los controles a establecer para la gestión adecuada del riesgo de fraude.
- Supervisar el cumplimiento del presente protocolo.
- Informar a la Junta Directiva sobre los hechos defraude que considere relevantes.

5.3. Comité de Ética

Complementariamente con las responsabilidades generales definidas en los Comités de Ética de ISA y sus empresas, tendrá las siguientes responsabilidades:

- Incluir dentro de los planes y programas que desarrolle alrededor de la ética, actividades que fomenten la cultura de prevención del fraude.
- Dar trámite a la Auditoría o a quien haga sus veces, de las denuncias de sean puestas en su conocimiento relacionadas con posibles hechos fraudulentos.

5.4. Gerente General

Complementariamente con lo definido en la normatividad interna, el Gerente General, 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.



- Aplicar lo establecido en la Política de Información y del Conocimiento, en la Política de Comunicación y en particular, en los principios definidos en el Manual de Comunicación para la Mitigación de Riesgos y Crisis de Reputación especialmente en la comunicación que requieran los grupos de interés en asuntos relacionados con este Código.

5.5. Auditoría

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

- Adelantar 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.
- Ordenar la contratación de expertos en los casos que considere pertinentes.
- Planificar y llevar a cabo la evaluación del diseño y la efectividad de los controles anti fraude.
- 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 sobre las evaluaciones de control interno, auditorías, investigaciones y actividades relacionadas.

5.6. Colaboradores

Acorde con lo definido en la Política de Gestión Integral de Riesgos y en la Política de Control Interno:

- 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.
- Cada trabajador de las empresas del Grupo ISA, aplica los criterios definidos en la Política de Control Interno para construir, mantener y ejercer controles efectivos y eficientes en los procesos y actividades a su cargo

Complementariamente con lo anterior y conforme al presente Código, todos los colaboradores deberán informar o denunciar las dudas o sospechas de posibles hechos fraudulentos y colaborar con las investigaciones de fraudes.



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 y
- Establecer e implementar mecanismos efectivos para su prevención, detección, investigación, y respuesta.

Dicha evaluación debe realizarse tanto a nivel estratégico como operativo en forma sistemática y periódica.

La evaluación del riesgo de fraude deberá estar enmarcada en la Política de Gestión Integral de Riesgos e incluir como mínimo: la evaluación de escenarios o esquemas de fraude relevantes para la empresa, su probabilidad y severidad, determinando los mecanismos de prevención, detección y protección existentes. Esta evaluación, deberá establecer planes de tratamiento adicionales necesarios para minimizar la vulnerabilidad en cada empresa. Dicha evaluación será realizada por los responsables de los procesos con el soporte y acompañamiento del equipos de riesgos y auditoría o quien haga sus veces.

A continuación, se exponen los mecanismos mínimos de prevención, detección, investigación y respuesta que cada empresa debe implementar, acorde con los criterios expuestos en este Código:

6.1. 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 ellos.

En este sentido es importante adoptar un enfoque coherente e integrado que tenga en consideración todos los elementos definidos en el Marco de Referencia Corporativo, así como en guías institucionales, procedimientos y normatividad interna en general, de tal forma que todos operen efectivamente.

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.

6.1.1. Prácticas de gestión del talento humano

Dada la importancia del factor humano en la prevención de los riesgos, en particular del 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.

6.1.2. 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.

6.1.3. Prácticas de contratación

De acuerdo con lo establecido en la Política para la Adquisición de Bienes y Servicios, la transparencia es un criterio fundamental de aplicación y la define así: “Los procesos de adquisición deben realizarse con base en procedimientos claros, imparciales y objetivos que garanticen la igualdad de condiciones y oportunidades de los proponentes”

Con respecto a la gestión específica del riesgo de fraude, es necesario que cada empresa 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 este Código sea de obligatorio cumplimiento, tanto cuando se actúa como contratante y contratista.

6.1.4. Línea Ética

En su enfoque preventivo, ISA y sus empresas disponen de una Línea Ética a la cual todos los colaboradores y demás grupos de interés pueden comunicar dudas o necesidades de asesoría en relación con el cumplimiento del Código Ética, así como también en lo relacionado con información que contraría lo prescrito en este Código Antifraude. La consulta será recibida garantizando la confidencialidad de la información y de la persona que la presenta.

6.1.5. Auditorías

La existencia de auditorías periódicas en ISA y sus empresas, como un mecanismo preventivo, 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.

6.1.6. Seguridad de la información

En ISA y sus empresas, se valora y se protege la información, el conocimiento y los productos, como activos estratégicos.

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 las guías corporativas para el Uso y Gestión de TI, la guía de Protección de la Propiedad Intelectual, Derechos de



Autor y Propiedad Industrial, la guía de Divulgación de Información Pública Producida por ISA y sus empresas y la guía de Estructura Documental.

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.

6.2. Detección

De acuerdo con lo establecido en el marco de actuación de este Código, 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:

6.2.1. 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 este Código.

6.2.2. 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.

6.2.3. Línea Ética

La línea ética, también es concebida, como principal elemento de comunicación de hechos sospechosos de fraude. El reporte será recibido garantizando la confidencialidad de la información y de la persona que la presenta.

6.2.4. 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 ley aplicable.

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

6.3. 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 área de Auditoría, o quien haga sus veces, para lo cual adoptará un protocolo y será realizada respetando siempre la normatividad aplicable en el país correspondiente.

6.4. 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 del marco de actuación de este Código, los hechos fraudulentos, debidamente soportados y analizados por el Gerente General y con quien éste considere pertinente, tendrán la respuesta administrativa y legal acorde con lo establecido en la normatividad interna y externa aplicable en cada país.

Otros elementos adicionales a considerar, son:

6.4.1. 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.

6.4.2. Transferencia

Con el objetivo de minimizar el impacto de las pérdidas y daños causados, ISA y sus empresas, mantendrán vigente los mecanismos de transferencia de riesgos que consideren pertinentes, acorde con la evaluación realizada para los riesgos que lo permitan.



7. ÁMBITO DE APLICACIÓN Y SEGUIMIENTO

La aplicación del presente Código, incluye a los miembros de las juntas directivas y/o directorios, así como a todos los colaboradores independientemente de su nivel jerárquico en las empresas.

El cumplimiento del presente manual será supervisado por el Comité de Auditoría o quien haga sus veces en cada una de las empresas

