BUENAS PRACTICAS EN GESTIÓN DE RIESGOS

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Gestión del Riesgo de Fraude:
Prevención, Detección e Investigación

The Institute of Internal Auditors

Instituto de Auditores Internos de España

BUENAS PRACTICAS EN GESTIÓN DE RIESGOS

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Gestión del Riesgo de Fraude:
Prevención, Detección e Investigación

Febrero 2015

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN: **Javier López Andreo, CFE, CISA.** PwC

Jorge Abad del Mazo. ENDESA

Luis Alonso Moreno. DELOITTE

Cristina Bausá Rosa, CIA, CRMA. SAREB

David Caña Domínguez, CIA. MAPFRE

Mariano Casado Carrillo de Albornoz, CFE. IBERDROLA

José Enrique Díaz Menaya, CIA, CRMA. BERGE Y CÍA

Enric Domenech Rey, CRMA. BDO

Reyes Fuentes Ortea, CIA, CISA, CFE, CCSA. NH HOTEL GROUP

Jaime García Ajuria, CIA. TRIODOS BANK

Sergio Gómez-Landero Pérez, CIA, CISA, CFE. ENDESA

Luis Mesa Palomino. CORTEFIEL

Vicente Obrero Castilla. CAJASUR

Fernando Paton Botella, CFE. INDITEX

Almudena Ruiz-Ruescas Pradera. PwC

Juan Jesús Valderas Martos. DELOITTE

Leyre Zayas Mariscal, CIA, CCSA. PwC

LA FÁBRICA DE PENSAMIENTO, el *think tank* del Instituto de Auditores Internos de España, aborda con acierto en este último documento –un resumen ejecutivo de una investigación más amplia que el Instituto editará próximamente– los diferentes procesos para una óptima gestión del riesgo de fraude, que pasa inexorablemente por un programa eficaz de prevención, detección e investigación de fraudes.

Además de establecer este programa y las características a tener en cuenta para su elaboración, este documento aporta un valor fundamental al definir un enfoque efectivo para la administración del fraude y un análisis profundo sobre las responsabilidades y concienciación en su prevención, detección e investigación.

Este enfoque se basa en un sistema de principios, valores, reglas y comportamientos que, tal y como sostienen los autores del documento, comienza en la alta dirección de la organización, que tiene la misión de definir, y asumir, un código de conducta como pilar básico de su programa de cumplimiento.

Si bien todos los miembros de la organización son responsables del establecimiento y mantenimiento de los controles adecuados contra el fraude, Auditoría Interna tiene un papel fundamental de aseguramiento ante el Consejo de Administración y la dirección de que los controles de fraude son suficientes.

Las nuevas tendencias, impulsadas por la realidad económica y por una creciente demanda social de mayor transparencia y control, exigen de los auditores internos respuestas pertinentes frente a casos de fraudes corporativos y, sin duda, éstas llegarán si tendemos hacia la excelencia en nuestro trabajo, que viene motivada por la formación y la capacitación, además de un correcto dimensionamiento de los equipos de Auditoría Interna.

Con este espíritu y con el impecable desarrollo de la investigación por parte de los integrantes de la Comisión Técnica se ha desarrollado esta guía, que contribuirá sin duda al óptimo desempeño de nuestras funciones como auditores internos, y por ende, al de las organizaciones en las que se desenvuelve nuestra profesión.

Ernesto Martínez

Presidente del Instituto de Auditores Internos de España

Índice

Introducción

El sistema de principios, valores y reglas de actuación en las organizaciones comienza en la alta dirección y, a través de diversos elementos (códigos de conducta, políticas y procedimientos, etc) se traslada al conjunto de la organización.

En el actual marco regulatorio global, las organizaciones están cada vez más sujetas a normativas internacionales relacionadas con la comisión de delitos, sobre todo de corrupción y soborno. Históricamente, el regulador más activo ha sido, dado su carácter extraterritorial, el Departamento de Justicia (DOJ) de los Estados Unidos, a través de la FCPA *(Foreign Corrupt Practices Act).*

En este campo, muchos gobiernos siguen las recomendaciones de la OCDE (Organización para la Cooperación y el Desarrollo Económico). Los de Reino Unido, Francia, Turquía, y España, entre otros, han reformado sus legislaciones, alineándolas a la lucha contra el fraude y la corrupción. Un ejemplo es la reforma del Código Penal de España, cuyo trámite se inició en octubre de 2013 y fue aprobado finalmente el 21 de enero de 2015 por el Congreso de los Diputados. En otros casos, como el del Reino Unido, se han introducido nuevas leyes como la *UK Bribery Act.*

De acuerdo con las recomendaciones de la OCDE, los programas de cumplimiento normativo definen los principios, valores, reglas de actuación y comportamientos de la actividad de la organizaciones; cuestiones que deben aceptarse, comunicarse, supervisarse, revaluarse y adaptarse con regularidad, para asegurar la eficacia continua de los controles internos, medidas y políticas de la compañía.

El objeto es doble: por un lado, facilitar al mercado información sobre los mecanismos específicos con los que la entidad mantiene un ambiente de control interno que propicia la generación de información financiera completa, fiable y oportuna; y por otro, prevenir y atenuar las posibles conductas irregulares así como propiciar las vías para detectarlas.

Este sistema de principios, valores y reglas empieza en la alta dirección. Y a partir de ahí, a través de un código de conducta, comportamientos adecuados y el diseño y la comunicación de las correspondientes políticas y procedimientos, se proyecta al resto de la organización.

En esta guía detallamos los principales elementos de un programa eficaz de prevención, detección e investigación de fraudes.

Prevención, detección e investigación del fraude

En cualquiera de sus categorías: apropiación de activos, corrupción, manipulación contable, uso de información privilegiada, etc., los delitos económicos han derivado en nuevas amenazas para las organizaciones de todo el mundo. La irrupción de las nuevas tecnologías y las dificultad de las organizaciones para adaptarse por sí solas a un entorno económico en cambio continuo, complican la situación. El aumento de los fraudes detectados y su impacto han obligado a invertir en nuevas medidas de prevención para minimizar los daños.

Es fundamental contar con un programa eficaz de prevención, detección e investigación de delitos; junto al que deben constar, al menos, los siguientes elementos:

1. Un órgano colegiado o unipersonal, dependiente del Consejo de Administración, que vele por la aplicación del Código de Conducta y sirva para procurar un comportamiento profesional, ético y responsable de toda la organización.
2. Un Código de Conducta o de Buenas Prácticas que defina los principios y valores que rigen las relaciones de la organización con sus grupos de interés (empleados, clientes, accionistas, socios de negocio, y proveedores) y que se implanta, se difunde y es aceptado por dichos grupos de interés.
3. El compromiso de la alta dirección.
4. Un plan de comunicación y formación para toda la organización.
5. Un programa eficaz de prevención, detección e investigación de fraude.
6. Un canal de denuncias, como vía de comunicación interna, que permita informar al órgano responsable, tanto de irregularidades de naturaleza financiera y contable, como de eventuales incumplimientos del Código de Conducta.

Para lograr reducir la probabilidad de fraude, las organizaciones deben realizar un gran esfuerzo en la gestión de dicho riesgo. A continuación mostramos cinco principios fundamentales para que una organización gestione proactivamente el riesgo de fraude. Esto es, los cinco elementos de un programa eficaz de prevención, detección e investigación de delitos:

1. **Establecer un programa de gestión del riesgo de fraude,** como parte de la estructura de gobierno. También conocido como programa anti-fraude, que incluye una política escrita y que recoge las expectativas del Consejo de Administración y los altos directivos en relación con la gestión de riesgo de fraude.
2. **Realizar una evaluación periódica de la exposición al riesgo de fraude,** con el fin

La irrupción de las nuevas tecnologías y un entorno económico en constante cambio, obligan a las organizaciones a invertir en nuevas medidas de prevención del fraude.

de identificar potenciales actuaciones y fraudes específicos que la organización necesita mitigar.

3. **Implantar técnicas de prevención** que eviten, en la medida de lo posible, posibles fraudes y mitiguen los impactos en la organización (tanto económicos como reputacionales).

4. De forma adicional, **implantar técnicas de detección,** para descubrir fraudes cuando las técnicas de prevención hayan fallado o no hayan mitigado el riesgo de comisión de fraude.

5. Y, por último, **implantar un proceso de reporting,** para solicitar *input* sobre potenciales fraudes. La investigación del fraude debe coordinarse con la acción correctiva, para que la gestión sea adecuada.

En los siguientes apartados, detallamos el rol del auditor interno en prevención, detección e investigación de fraude, en cada uno de estos cinco elementos.

Según la última encuesta realizada por el Instituto de Auditores Internos de España y contestada por 170 auditores internos, Auditoría Interna incluye cada vez más entre sus funciones la prevención, detección e investigación de fraude: un 81% de los encuestados manifiesta que Auditoría Interna colabora en la prevención de fraude interno; un 84%, en la detección; y un 82%, en la investigación. En el caso del fraude externo, los porcentajes son similares, aunque algo menores, tanto en la prevención como en la detección.

Los departamentos de sistemas de información, cumplimiento normativo, legal, financiero y recursos humanos colaboran junto a Auditoría Interna en la prevención, detección e investigación de fraudes tal y como describimos a lo largo de esta guía y resumimos en la sección relativa al rol del auditor interno.

PROGRAMA DE GESTIÓN DE RIESGO DE FRAUDE

El Libro Verde de Gobierno Corporativo de la Comisión Europea define éste como *"el sistema por el cual las empresas son dirigidas y controladas"*; aunque se puede definir de muchas otras maneras, como *"el proceso por el cual las empresas se hacen sensibles a los derechos y deseos de las partes interesadas"*. También puede describirse como el modo en

que la dirección cumple con sus obligaciones y responsabilidades.

Las partes interesadas de todas las organizaciones tienen sus expectativas puestas en los comportamientos éticos de las mismas. Por ello, las organizaciones deben responder ante estas expectativas.

El Consejo de Administración y la alta dirección deben asegurar que las prácticas de gobierno marcan las pautas para la adecuada gestión del riesgo de fraude. Además, deben implementar políticas que fomenten un comportamiento ético y que incluyan tanto procesos relativos a empleados, clientes, proveedores y otras terceras partes, como procesos que especifiquen a quién reportar en los casos en los que no se cumplan los estándares.

La mayoría de las organizaciones tienen políticas y procedimientos de gestión de riesgo de fraude, pero pocas han desarrollado un documento único que incluya todas estas actividades y que constituya una guía documental útil a la hora de comunicar y evaluar sus procesos, es decir, un agregado de políticas y procedimientos que denominamos *programa de gestión del riesgo de fraude.*

Según la encuesta del Instituto de Auditores Internos de España antes mencionada, el 49% de los encuestados afirma que su organización cuenta con un mapa de riesgos de fraude con el que valora y gestiona sus riesgos; si bien sólo un 27% de los trabajos de Auditoría Interna incluyen tareas encaminadas a la valoración de los citados riesgos.

A continuación exponemos los principales aspectos que deben abordarse en cualquier programa eficaz de gestión del riesgo de fraude:

- Roles y responsabilidades.
- Compromiso de la alta dirección.
- Conocimiento del fraude.
- Evaluación del riesgo de fraude.
- Procedimiento de reporte y protección de los denunciantes y denunciados.
- Procedimiento de investigación.
- Acciones correctivas.
- Vigilancia / seguimiento continuo.

Un programa eficaz sobre ética en los negocios es la base para prevenir y detectar actos fraudulentos y criminales.

Un programa eficaz sobre ética en los negocios es la base para prevenir y detectar actos fraudulentos y criminales. En la medida en que una organización fortalece los sistemas de prevención y detección de fraude, mayor es la probabilidad de evitarlo y, en su caso, identificar y detectar su existencia. Una organización que fomenta el tratamiento ético con sus empleados, clientes, proveedores y otras terceras partes, consigue ser tratada de la misma forma.

EVALUACIÓN DEL RIESGO DE FRAUDE

Para protegerse, tanto a sí misma como a otras partes interesadas, la organización debe entender y conocer cuál es su riesgo de fraude y cuáles son los riesgos específicos a los que está directa o indirectamente expuesta. Esta evaluación puede integrase en una evaluación del riesgo en conjunto, o desarrollarse de forma independiente; pero, como mínimo, debe incluir:

- La identificación del riesgo concreto.
- La probabilidad de ocurrencia e impacto.
- La respuesta al mismo.

Identificación del riesgo de fraude concreto

Para identificar un riesgo, la organización puede utilizar fuentes de datos externas o internas. Entre las externas están los organismos reguladores, el propio sector, las principales guías como COSO[1], y organizaciones profesionales como The Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA), Association of Certified Fraud Examiners (ACFE), etc.

Las fuentes internas incluyen entrevistas con el personal adecuado o representante de un amplio abanico de actividades dentro de la organización; la revisión de las denuncias interpuestas a través de los mecanismos implantados (canal de denuncias o línea ética) y otros procedimientos analíticos.

Para que un proceso de identificación y evaluación del riesgo de fraude sea efectivo, debe incluir la evaluación de los incentivos y las presiones y oportunidades de cometer fraude. Asimismo, la evaluación del riesgo de fraude debe considerar la potencial eliminación de controles por parte de la dirección, así como el análisis de aquellas áreas donde los controles son débiles o no existe una clara segregación de funciones.

La tecnología proporciona a la organización muchos beneficios, como la velocidad en las comunicaciones y la accesibilidad a la información, pero también incrementa la exposición al riesgo de fraude. Por tanto, una evaluación del riesgo debe considerar tanto los accesos a los sistemas como las amenazas internas y externas a la integridad de los datos, la seguridad de los sistemas y el robo de información confidencial y sensible.

Evaluar la probabilidad e impacto de los riesgos inherentes permite gestionar el riesgo de fraude e implementar y aplicar procedimientos de prevención y detección de manera razonable.

Probabilidad de ocurrencia e impacto

Evaluar la probabilidad e impacto de los potenciales riesgos de fraude es un proceso en el que hay que contar con factores monetarios o económicos, financieros, operacionales, reputacionales y legales. No todos los riesgos potenciales tienen la misma probabilidad y el mismo impacto en todos los casos.

La organización debe considerar en primer lugar aquellos riesgos inherentes[2] a su negocio. Evaluar la probabilidad y el impacto de estos riesgos le permite gestionar su riesgo de fraude e implementar y aplicar procedimientos preventivos y de detección de una forma racional.

Una vez mapeados los riesgos, con sus respectivos controles, es posible que exista un riesgo residual[3].

La dirección evalúa el potencial impacto de los riesgos y decide la naturaleza y alcance de los controles preventivos y de detección así como los procedimientos para su gestión.

- **Probabilidad de ocurrencia.** La evaluación de la probabilidad de ocurrencia de un determinado riesgo de fraude considera factores como la ocurrencia en la organización de ese riesgo en el pasado, su frecuencia en las organizaciones del mismo sector, la

1. Committee of Sponsoring Organizations of the Treadway Commission.

2. El riesgo inherente es aquel riesgo al que está expuesta toda organización ante la ausencia total de controles.

3. El riesgo residual es aquel riesgo que queda en la organización una vez aplicados todos los controles.

complejidad del riesgo y el número de personas involucradas en la revisión y aprobación del proceso, entre otros factores.

Evaluada la probabilidad de ocurrencia, ésta se categoriza de varias formas. La tres más utilizadas son *probabilidad remota, probabilidad posible* y *probabilidad probable.*

- **Impacto en la organización.** La evaluación del impacto de que un riesgo de fraude finalmente se materialice no solo tiene en cuenta factores monetarios en los estados financieros, sino también factores operacionales, el valor de la marca, la reputación, aspectos legales y regulatorios.

  Al igual que con la probabilidad de ocurrencia, una vez evaluado el impacto de que un riesgo de fraude se materialice, éste se categoriza. La forma más común es la que diferencia entre *impacto no significativo, impacto significativo* e *impacto material.*

De forma adicional, las organizaciones deben evaluar los incentivos y presiones de los individuos y departamentos: qué individuos y departamentos tienen mayores incentivos y, por tanto, mayor probabilidad de comisión de fraude. Toda esta información permite a la organización diseñar las respuestas adecuadas.

Respuesta al riesgo residual de fraude

La tolerancia al riesgo varía de una organización a otra. La alta dirección establece el nivel de tolerancia al riesgo teniendo en cuenta su responsabilidad frente a los socios o accionistas, las entidades financiadoras y demás partes interesadas.

Algunas organizaciones prefieren gestionar únicamente los riesgos de fraude con impacto material en los estados financieros; otras, implantan programas de respuesta al fraude más estrictos, con políticas de "tolerancia cero".

La tolerancia al riesgo varía de una organización a otra. Es la alta dirección quien establece el nivel de tolerancia considerando su responsabilidad ante los diferentes grupos de interés.

LA PREVENCIÓN DEL FRAUDE

Las técnicas de prevención de fraude no garantizan que el fraude no se cometa, pero son la primera línea de actuación para minimizar el riesgo.

Un elemento importante en un programa de prevención de fraude es la existencia de una política escrita que establezca quién es el responsable de gestionar el riesgo dentro de la organización en sus diferentes ámbitos y circunstancias (prevención, detección, e investigación). Un documento oficial que detalle claramente cuáles son los derechos y obligaciones de todos los directivos y empleados frente

a la potencial irregularidad y sus consecuencias, independientemente de su categoría o nivel profesional, o de su vinculación a la organización. De hecho, el 64% de los encuestados por el Instituto de Auditores Internos de España manifiesta que su organización cuenta con una política antifraude de este tipo.

La existencia de políticas claramente definidas, la contribución del área de Recursos Humanos, los límites de la autoridad o las revisiones efectuadas por terceras personas son algunos de los elementos principales de la prevención del fraude.

Entre otros de los muchos elementos trascendentales en la prevención del fraude, se encuentran los procedimientos de Recursos Humanos, los límites de la autoridad y los procedimientos transaccionales.

- **Procedimientos de Recursos Humanos.** La función de Recursos Humanos juega un papel muy importante en la prevención del fraude en los siguientes procedimientos:
  - Desarrollo de investigaciones de antecedentes, o conocimiento y verificación del perfil de un empleado.
  - Impartición de cursos anti-fraude.
  - Evaluación del desarrollo y establecimiento de programas de compensación.
  - Realización de entrevistas de salida del personal.
- **Límites de la autoridad.** La comisión de un fraude es menos probable cuando el nivel de autoridad de una persona en la organización es proporcional a su nivel de responsabilidad. En este sentido, la desalineación entre responsabilidad y autoridad, unido a la ausencia de controles y de segregación de funciones, tiene un impacto elevado en la comisión de fraude.
- **Procedimientos transaccionales.** Las revisiones de terceros, incluso de otras partes relacionadas, ayuda a prevenir el fraude.

  Las medidas preventivas son especialmente necesarias para transacciones con partes relacionadas controladas por miembros de la alta dirección o por empleados con autoridad y con interés especial en compañías externas relacionadas con la organización.

LA DETECCIÓN DEL FRAUDE

En muchas casos, los controles de detección dependen de los riesgos de fraude identificados en la organización. Por ejemplo, si una organización americana opera en países con un alto nivel de corrupción, implantará controles para identificar violaciones de FCPA[4], como la revisión de gastos u honorarios de consultoría.

Igual que ocurre con los controles preventivos, la organización necesita evaluar y supervisar de forma continua sus técnicas de detección. Si bien un 41% de las empresas encuestadas por el Instituto de Auditores Internos de España manifiesta no realizar trabajos de supervisión o pruebas automatizadas para la detección del fraude, un 32% manifiesta que incor-

4. Foreign Corrupt Practice Act.

pora siempre en los Planes de Auditoría Interna tareas encaminadas a la detección de fraude.

Los controles de detección deben ser flexibles, para adaptarse a los cambios de los riesgos.

Los controles preventivos son fácilmente identificados por los empleados y/o terceras partes. Pero los controles de detección son, por su naturaleza, clandestinos: dichos controles operan en un contexto que no es evidente en el entorno empresarial. Las técnicas de detección preventivas suelen:

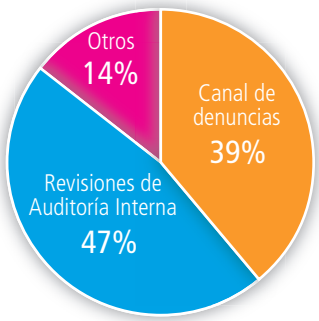
- Producirse en el curso normal de la actividad de la compañía.
- Basarse en información externa, que corrobora información generada internamente.
- Comunicar de manera formal y automática las deficiencias y excepciones identificadas.
- Mejorar y/o modificar otros controles.

Las técnicas de detección incluyen mecanismos de reporting anónimo (canal de denuncias), denuncia (anónima o no), procesos de control y procedimientos proactivos de detección de fraude, diseñados específicamente para identificar actividades fraudulentas.

La última encuesta referenciada al inicio de este documento muestra los medios de detección que las organizaciones ponen a disposición de sus empleados: los canales de denuncias internos y externos[5] y las revisiones de Auditoría Interna continúan siendo, con un 39% y un 47% respectivamente, los métodos de detección más eficaces.

Los canales de denuncia y las revisiones de Auditoría Interna continúan siendo los métodos más eficaces de detección de fraude.

EFICACIA DE MEDIOS DE DETECCIÓN



LA INVESTIGACIÓN DEL FRAUDE Y ACCIONES CORRECTIVAS

Cualquier violación, desviación o infracción de un código de conducta o de cualquier control, debe ser reportado y tratado de forma oportuna, independientemente de quién lo cometa. Es un hecho esencial para cualquier organización. El castigo impuesto debe ser apropiado a la infracción. Y el Consejo de Administración debe asegurar que se apliquen la mismas reglas a todos los niveles de la organización, incluyendo la alta dirección.

Es recomendable contar con un protocolo de actuación frente al fraude. Entre otros aspectos, el documento debe definir el procedimiento desde que se detecta la posible infracción hasta su resolución, y tratar todos los aspectos que surjan a lo largo de la investigación: legales, toma de evidencias, consultas a externos, áreas involucradas, modelo de reporting, medidas correctivas, medidas disciplinarias, etc.

5. Un 72,36% de los encuestados manifiesta contar en su empresa con un canal de denuncias o irregularidades, el cual en casi un 50% de los casos está abierto a colaboradores, agentes y clientes.

Una organización puede tener noticia de un potencial fraude a través de diversas vías: empleados, clientes, proveedores, auditores internos, auditores de cuentas, los procesos de control o, incluso, accidentalmente.

De la encuesta del Instituto de Auditores Internos de España se desprende que el 50% de las empresas cuentan con un protocolo de actuación frente al fraude; que en el 49% de los casos incluye quién es la persona o cuál es el departamento o comité encargado de resolver la investigación y de adoptar las correspondientes medidas.

Recepción y evaluación de las alegaciones

- **Recepción de alegaciones.** Una organización puede tener noticia de un potencial fraude a través de diversas vías: los propios empleados, clientes, proveedores, auditores internos, auditores de cuentas, los procesos de control, o, incluso, accidentalmente.

  Entonces, la organización debe asegurar que se ponga en marcha un sistema competente, eficaz y confidencial para la revisión de las alegaciones recibidas, la investigación del potencial fraude y su resolución.

  La investigación y respuesta incluyen los siguientes procesos:
  - Categorización de las alegaciones recibidas.
  - Confirmación de la validez de la alegación.
  - Definición de la gravedad de la alegación.
  - Propuesta para transmitir el asunto al nivel apropiado dentro de la organización.
  - Realización de la investigación y determinación de las responsabilidades.
  - Resolución y cierre de la investigación.
  - Determinar aquella información que debe permanecer confidencial.
  - Documentación de la investigación llevada a cabo.

  De forma adicional, implementar un sistema de gestión de denuncias o alegaciones donde puedan registrarse adecuadamente las mismas.

- **Evaluación de las alegaciones**. Recibida una alegación, se evalúa y califica. Para ello, se designa a un individuo o grupo de individuos con cierta autoridad dentro de la organización y con las habilidades o capacidades necesarias para esta primera evaluación y determinar el procedimiento a seguir.

  Si una alegación involucra a la alta dirección, o afecta a los estados financieros, es necesario atender a las leyes o regulaciones, que pueden exigir que otras partes sean debidamente informadas.

Realización de las investigaciones

Es esencial planificar la investigación para que sea competente y exhaustiva. Una investigación de fraude, generalmente, incluye las siguientes cuestiones: entrevistas, recolección de evidencias, tanto documentos internos como documentación de fuentes públicas, evidencias digitales a través de un análisis forense, y un análisis de las evidencias recopiladas, con pruebas analíticas de testeo o hipótesis.

Reporting de resultados

El equipo de investigación informa sobre los resultados obtenidos, tanto a la parte que supervisa la investigación, como a la dirección de la organización y al departamento de asesoría legal.

La naturaleza de la comunicación, así como la forma de distribuirla, debe tener en cuenta los objetivos de la investigación y evitar cualquier afirmación difamatoria. Por ello, antes de que el responsable de la supervisión de la investigación haga públicos los resultados, se necesita el asesoramiento de un abogado.

Acciones correctivas

Realizada la investigación, la organización determina qué acciones tomar en vista de los resultados. Entre las posibles acciones están:

- Despedir.
- Abrir un procedimiento penal.
- Abrir un procedimiento civil.
- Establecer medidas disciplinarias.
- Solicitar una reclamación al seguro contratado.
- Continuar con la investigación, implantando nuevos procedimientos.
- Implantar nuevos procesos de negocio y de control.

Responsabilidades y concienciación en la prevención, detección e investigación del fraude

INTRODUCCIÓN

Las organizaciones están cada vez más sujetas a exigencias de cumplimiento internacional relativas a la comisión de delitos, corrupción y soborno y, por tanto, implementando programas de cumplimiento normativo. Éstos, según la OCDE, deben definir el sistema de principios, valores, reglas de actuación y comportamientos que deben regular la actividad de la empresa. Este sistema debe ser aceptado, comunicado, supervisado, actualizado y adaptado con regularidad, según sea necesario, para asegurar la eficacia continua de los controles internos, medidas y políticas de la organización. Todo ello permite no sólo facilitar al mercado información acerca de los mecanismos específicos que la entidad ha habilitado para mantener un ambiente de control interno que propicie la generación de información financiera completa, fiable y oportuna, sino prevenir o atenuar la comisión de conductas irregulares y propiciar las vías para detectarlas.

Este sistema de principios, valores, reglas de actuación y comportamientos empieza en la alta dirección de la entidad, la cual influye a través de sus propias acciones en el resto de la organización, con el establecimiento de un

Las organizaciones deben definir el sistema de principios, valores, reglas de actuación y comportamientos que regulan su actividad y deben comunicarlo, supervisarlo y actualizarlo para mantener su eficacia.

código de conducta y unos adecuados comportamientos, y en el diseño y comunicación efectiva de las correspondientes políticas y procedimientos.

Por tanto, es esencial que las compañías establezcan un código de conducta como pilar básico de su programa de cumplimiento, que procure un comportamiento profesional ético y responsable de la organización y de todos sus empleados, en el desarrollo de sus actividades en cualquier parte del mundo. Dicho código de ética debe reflejar su cultura empresarial en la que se debe asentar la formación y el desarrollo personal y profesional de sus empleados, y definir los principios y valores que deben regir las relaciones de la organización con sus grupos de interés (empleados, clientes, accionistas, socios de negocio, y proveedores).

Es esencial que las organizaciones establezcan un código de ética como pilar básico de su programa de cumplimiento.

Una vez que la organización cuente con el compromiso de la alta dirección, se debe transmitir este sistema de principios, valores, reglas de actuación y comportamientos al resto de la organización.

Se recomienda la continua comunicación y formación a los empleados de la organización no sólo en cuanto al Código de Conducta –cultura empresarial de la organización– sino también en cuanto a los riesgos inherentes a la comisión de delitos, al establecimiento e implantación de medidas para detectar y prevenir conductas irregulares, a los cambios regulatorios, a la existencia de mecanismos para denunciar o consultar el modo de proceder ante conductas que pudieran entenderse como irregulares y respecto a todo aquello que fomente y asiente la cultura empresarial de la organización.

De forma adicional, dentro de los pilares básicos de un eficaz programa de cumplimiento, destaca aquel que permita minimizar la probabilidad de que se produzcan irregularidades y asegurar que, las que eventualmente puedan producirse, sean siempre identificadas, comunicadas y resueltas con prontitud. Por esto es recomendable, y así se está poniendo cada vez más en práctica, la implantación de canales de denuncia, como vía de comunicación interna que permita la comunicación al órgano responsable de irregularidades de naturaleza financiera y contable, así como de eventuales incumplimientos del código de conducta y actividades irregulares. Este canal permite demostrar a terceros interesados que la organización cuenta con procedimientos y medios adecuados y que los mismos son permanentemente revisados.

ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO DE FRAUDE

Para que un programa de cumplimiento corporativo sea eficaz, es fundamental que la alta dirección asuma sus principios y valores y que los apoye de forma explícita y evidente. Lo mismo ocurre con el compromiso del equipo directivo para prevenir y detectar conductas irregulares.

La alta dirección es responsable de la disuasión frente al fraude:

- A través del propio ejemplo en su gestión. El tono ético de toda una organización depende, significativamente, de cómo el resto de la organización percibe la conducta de

la alta dirección en su día a día y de cómo ésta maneja las situaciones de crisis.

- La alta dirección es responsable además del sistema de control interno, supervisión y documentación de las áreas de mayor riesgo, tales como el reconocimiento de ingresos, la gestión del efectivo, las compras y el inventario.

Para que la gestión del riesgo de fraude sea efectiva, es importante que estén muy bien definidos los roles y las responsabilidades del personal de la organización en todos los niveles. Las políticas internas de una organización, la descripción de los puestos de trabajo y las delegaciones de autoridad, deben definir esos roles y responsabilidades relacionados con la gestión del fraude.

Toda esta estructura debe establecer quién es el responsable de la supervisión de los controles, cuál es la responsabilidad de la dirección en relación con el diseño y la implementación de la estrategia y qué departamentos de la organización respaldan y apoyan la gestión del riesgo.

Los departamentos de gestión de riesgos, de cumplimiento normativo, asesoría jurídica, el comité de ética, seguridad y tecnologías de la información y Auditoría Interna, o sus equivalentes, suelen ser los que respaldan la gestión del riesgo de fraude. Sin embargo, son el Consejo de Administración, el Comité de Auditoría, la dirección, el propio personal y los auditores internos los que tienen dentro de la organización el rol y la responsabilidad de la gestión de dicho riesgo.

Por tanto, uno de los objetivos es establecer un enfoque efectivo para la administración del fraude, dirigido a:

- Prevenir, detectar y responder ante la comisión de cualquier irregularidad.
- Hacer converger las exigencias normativas y las tendencias –concentrando e integrando auto-evaluaciones y auditorías– con el riesgo real de fraude.
- Crear el área específica de Auditoría Interna y desarrollar una metodología o programa antifraude.
- Delimitar las responsabilidades de los integrantes de la evaluación del fraude.
- Implementar un proceso continuo dentro de la evaluación del control interno.

Las políticas internas de una organización, la descripción de los puestos de trabajo y las delegaciones de autoridad, deben definir los roles y responsabilidades relacionados con la gestión del fraude.

ENFOQUE EFECTIVO PARA LA ADMINISTRACIÓN DEL FRAUDE

Fuente: elaboración propia

Evaluar, supervisar, planificar, informar y colaborar son algunas de las actividades de Auditoría Interna en materia de fraude.

La organización debe:

- Identificar riesgos de fraude y mitigarlos con controles.
- Asegurar que estos controles son efectivos.
- Asegurar que los niveles más altos de la organización comparten la responsabilidad del enfoque de administración del riesgo.

Auditoría Interna, por su parte, asume la responsabilidad de:

- Validar que se estipulan políticas y normas que realizan una evaluación y cobertura aceptable del riesgo.
- Planificar y supervisar la eficiencia del modelo, en base a la matriz.
- Informar al Comité de Auditoría de los resultados de las actividades.
- Colaborar en la implementación de programas de análisis de riesgos de fraude.

En el cuadro adjunto mostramos las diferencias de enfoque entre un proyecto de Auditoría Interna convencional y un proyecto de Auditoría orientado a la detección del fraude.

Pese a que la existencia de un adecuado sistema de control interno es esencial en la prevención, detección e investigación del fraude, es necesario tener en consideración las siguientes cuestiones referentes al mismo:

- Un buen sistema no garantiza la eliminación del fraude. Siempre existen restricciones de recursos para realizar los controles y muchos de ellos pueden ser vulnerables.
- Los sistemas de control interno requieren programas de prevención, que disminuyen la probabilidad de ocurrencia, minimizan su impacto y permiten mayor rapidez de detección.
- Los riesgos no son únicos ni estáticos. Debemos estar atentos a los cambios tecnológicos que representan, a la vez que nuevas oportunidades, nuevas amenazas, tales como actividades en la nube *(cloud computing),* la ciber-seguridad, las redes sociales como medio de venta, los dispositivos inteligentes y su nueva tecnología, los proveedores de servicios,etc.

Por tanto, las **claves del éxito de un sistema de control interno** son:

- Apoyo de la alta dirección y la gerencia.
- Firme decisión de cambio cultural de control interno.

Diferencias entre la auditoría tradicional y la auditoría para la detección de fraude

AUDITORÍA INTERNA TRADICIONAL	DETECCIÓN DE FRAUDE
Procedimientos programados.	Aleatoria - no programada.
Orientada a: - Foco en fortalezas del control interno, errores y omisiones. - Énfasis en materialidad. - Evaluación del diseño y su cumplimiento. - Trabajo sobre muestras.	Orientada a: - Pensamiento defraudador. - Prácticas no habituales. - Uso abusivo de excepciones. - Cambios en la conducta emocional.
Basada en el análisis de procesos.	Focalizada en debilidades de control interno, excepciones y conductas. Trabaja sobre universos e indicadores.

Fuente: Elaboración propia.

- Participación activa de los diferentes actores.
- Adopción de herramientas tecnológicas.
- Coordinación y trabajo interdisciplinar.
- Flexibilidad del modelo.
- Focalizar el objetivo, con soluciones alcanzables.
- Diseño y ejecución de un plan de información.
- Implementación en etapas para evaluar el avance.

Por tanto, un programa efectivo de administración de fraude requiere que toda la organización dirija sus esfuerzos hacia "la gestión del riesgo de fraude".

El Consejo de Administración

El Consejo de Administración es el responsable de fijar el tono adecuado de gobierno de una organización en el nivel más alto posible y de asegurar que la dirección diseña un sistema eficaz de gestión del riesgo de fraude, que fomenta el comportamiento ético y anima a los empleados, clientes y proveedores a cumplir estos estándares en todo momento.

Por ello, el Consejo de Administración debe:

- Entender el riesgo de fraude.
- Supervisar la evaluación del riesgo y asegurar que forma parte del plan estratégico en relación con la evaluación de los riesgos generales. La responsabilidad se gestiona a través del orden del día del Consejo.
- Realizar el seguimiento de los informes de la dirección en relación con los riesgos de fraude, las políticas establecidas y las actividades de control.
- Supervisar los controles internos de la dirección.
- Establecer el tono adecuado desde lo más alto de la organización *(tone at the top),* con la descripción del puesto del máximo ejecutivo, su proceso de contratación, su evaluación y los planes de sucesión o permanencia en el cargo.
- Contratar expertos externos, cuando fuese necesario.
- Facilitar a los auditores de cuentas las evidencias necesarias que den constancia de la involucración del Consejo en el conocimiento y gestión del riesgo de fraude.

Por lo general, el Consejo de Administración delega la supervisión de algunas o de todas sus responsabilidades en el correspondiente Comité de Dirección. No obstante, el Consejo debe asegurarse de que la dirección cuenta con los recursos necesarios y aprueba en el presupuesto a largo plazo los recursos suficientes para realizar su gestión.

El Consejo de Administración, además, nombra entre sus miembros a los componentes del Comité de Auditoría que asesoran y prestan ayuda especializada al propio Consejo en cuestiones relacionadas con la auditoría de cuentas, los sistemas de control interno, la elaboración de las cuentas de la sociedad, su posterior comunicación externa, etc.

El Comité de Auditoría

El Comité de Auditoría debe gestionar proactivamente el riesgo de fraude, supervisar activamente la evaluación que la organización realiza del mismo y mantener un contacto frecuente con los auditores internos y el personal designado que realiza el seguimiento de dicho riesgo de fraude.

Asimismo, mantiene el contacto con los auditores de cuentas, comprometiéndose en la gestión del riesgo de fraude y discute con

El Consejo de Administración es el responsable de fijar el tono adecuado de gobierno en una organización para asegurar que la dirección diseña un sistema eficaz para la gestión del riesgo de fraude.

ellos el enfoque de los planes en materia de detección del mismo como parte de la auditoría de los estados financieros.

El Comité de Auditoría debe comprender, por tanto, las estrategias de Auditoría Interna y externa en la gestión del riesgo de fraude, y no centrarse sólo en las acciones concretas que llevan a cabo los auditores en detección del fraude.

Todos los miembros de una organización son responsables del establecimiento y mantenimiento de los controles adecuados contra el fraude.

Del mismo modo, el Comité de Auditoría debe ser consciente de que los auditores de cuentas tienen la responsabilidad, al planificar y realizar su auditoría, de obtener una seguridad razonable de que los estados financieros están exentos de errores significativos, sea por equivocación o fraude.

El compromiso de cooperación del Comité de Auditoría supone un diálogo abierto y franco entre los miembros del Comité, los auditores internos y los externos en relación a cualquier tipo de fraude o sospecha, que afecte a la organización; también respecto a la forma en que el Comité de Auditoría ejerce su función de supervisión de los programas y controles establecidos por la organización para mitigar dichos riesgos.

De forma adicional, el Comité de Auditoría debe buscar asesoramiento legal en caso de denuncias de fraude. Las acusaciones de fraude deben tomarse con la suficiente consideración, ya que puede existir una obligación legal de investigar y/o informar sobre ello.

La dirección

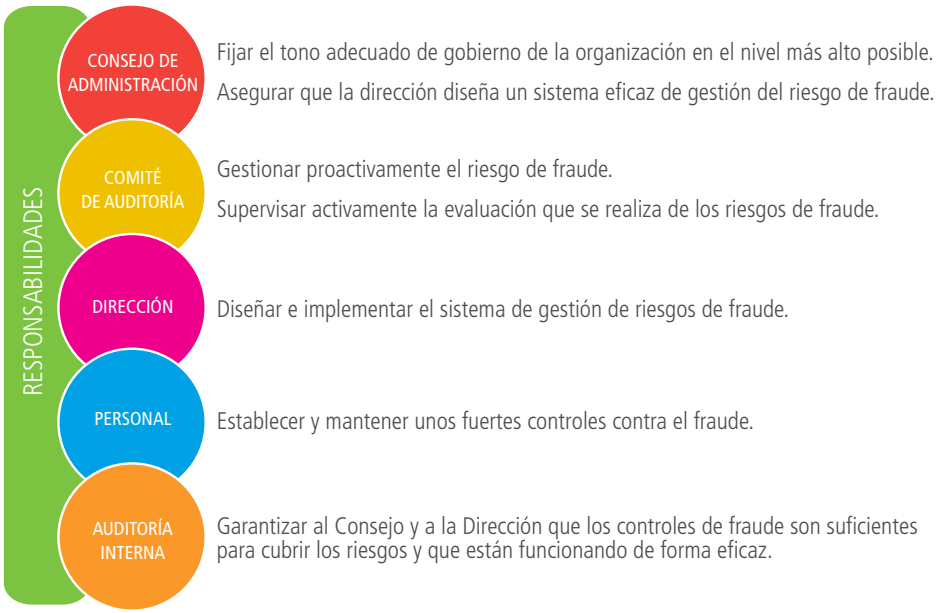
La dirección de la organización tiene la responsabilidad general del diseño e implementación del sistema de gestión del riesgo de fraude, incluyendo:

- Establecer el tono ético en la parte superior de la organización. La cultura de la organización juega un papel fundamental en la prevención, detección y disuasión del fraude. La dirección transmite al resto de la organización que el fraude no es un comportamiento tolerable, que este tipo de hechos serán tratados con rapidez y se asegura a los denunciantes que no sufrirán represalias.
- Implementar los controles internos adecuados, redacción y recopilación de las políticas y procedimientos necesarios de gestión del riesgo de fraude y evaluación de su eficacia.
- Informar al Consejo de Administración de que se han tomado medidas para gestionar los riesgos de fraude, así como presentar periódicamente informes sobre la evaluación de la eficacia del programa de gestión de dicho riesgo.

El personal

Todos los miembros de una organización son responsables del establecimiento y mantenimiento de los adecuados controles contra el fraude. La importancia de los controles internos para la gestión del riesgo de fraude no es un concepto nuevo. En 1992 –después de más de tres años de colaboración entre diferentes líderes empresariales, legisladores, reguladores, auditores, académicos y otros muchos– COSO presentó una definición común sobre los controles internos y proporcionó un marco con el que las organizaciones pueden evaluar y mejorar sus sistemas de control interno.

COSO identificó cinco componentes de lo que denominó *Marco Integrado de Control Interno:* entorno de control, evaluación de riesgos, actividades de control, información y comunicación, y supervisión. Estos elementos sirven para el diseño de los controles en cada orga-



nización. Están entrelazados entre sí, de tal forma que proporcionan un proceso interactivo natural que promueve el tipo de entorno que no tolera el fraude.

Todos los niveles de la organización, incluida la dirección, deben:

- Tener un conocimiento básico del fraude y estar atentos a las señales de alerta.
- Entender cuál es su papel en el marco de control interno. El personal debe comprender cómo sus procedimientos de trabajo están diseñados para gestionar el riesgo de fraude y que su incumplimiento puede dar oportunidad al fraude.
- Leer y entender las políticas y procedimientos (políticas de fraude, código de conducta y canal de denuncias, entre otros) así como las políticas operacionales (manual de compras, etc.).
- Participar, en su caso, en el proceso de creación de un fuerte ambiente de control y en el diseño e implementación de las actividades de control de fraude, así como en las actividades de seguimiento.
- Informar acerca de sospechas o indicios de fraude.
- Cooperar en las investigaciones de fraude.

Auditoría Interna

Según la definición de The Institute of Internal Auditors, *"Auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de gestión de riesgos, control y gobierno."*

Auditoría Interna debe asegurar al Consejo de Administración y a la dirección que los controles de fraude son suficientes para cubrir los riesgos identificados y garantizar que están funcionando de forma eficaz.

Auditoría Interna debe asegurar al Consejo y a la dirección que los controles en materia de fraude son suficientes para cubrir los riesgos identificados y garantizar que dichos controles funcionan de manera eficaz.

Los auditores internos deben evaluar, en sus planes anuales de Auditoría Interna, los riesgos de fraude de la organización y revisar periódicamente la capacidad de gestión de la dirección. Deben reunirse periódicamente con los encargados de identificar y evaluar el riesgo de fraude y con aquellos otros puestos clave de la organización para garantizar que han sido considerados adecuadamente todos los riesgos.

Al llevar a cabo su trabajo ordinario de control, los auditores internos deben actuar con un cierto grado de escepticismo profesional y mantenerse en guardia ante posibles signos de fraude. Los potenciales fraudes detectados durante una auditoría deben tratarse de acuerdo a un plan de respuesta bien definido y previamente establecido. De la misma forma, Auditoría Interna debe tener un papel proactivo en el apoyo a la cultura ética de la organización.

Auditoría Interna participa en la gestión de los cinco elementos que forman el sistema de control de COSO señalados anteriormente.

Los auditores internos, en el desempeño de su actividad, deben actuar con un cierto grado de escepticismo profesional y permanecer alerta ante posibles signos de fraude.

RESPONSABILIDADES DE AUDITORÍA INTERNA SEGÚN LOS COMPONENTES QUE FORMAN COSO

AMBIENTE DE CONTROL	· Validar la existencia de políticas y procedimientos antifraude. · Verificar su alineación con el código de ética/conducta y políticas de contratación. · Complementar y analizar las funciones de Auditoría Interna en el nuevo contexto. · Incorporar un esquema de aprendizaje que desemboque en nuevos diseños y formación. · Implantar políticas y metodologías de investigación. · Revisar eventos, alertas y comportamientos sospechosos de fraude. · Delimitar responsabilidades y comunicar los resultados.
EVALUACIÓN DE RIESGOS DE FRAUDE	· Validar evaluaciones de procesos que contemplen el riesgo de fraude. · Incorporar el riesgo de fraude en las matrices de riesgos y controles existentes. · Converger en la documentación, actualización y certificación de los procesos.
ACTIVIDADES DE CONTROL DE FRAUDE	· Colaborar en la definición de controles mitigantes de riesgos identificados. · Contribuir a la mejora de controles preventivos y de detección. · Ayudar a generar planes antifraude con rotación de áreas aprobados por la dirección. · Incorporar al Plan Anual de Auditoría actividades de control antifraude.
INFORMACIÓN Y COMUNICACIÓN	· Consensuar con RR.HH programas corporativos de comunicación. · Asistir en la implementación de capacitaciones. · Fomentar el uso de programas de denuncia anónima.
SUPERVISIÓN	· Realizar evaluaciones periódicas de controles antifraude. · Aprovechar las herramientas de análisis de datos. · Implementar un modelo de seguimiento continuo.

Fuente: Elaboración propia.

La importancia que una organización concede a su unidad de Auditoría Interna indica su compromiso con el control interno. El Estatuto de Auditoría Interna debe incluir las funciones y responsabilidades relacionadas con la gestión del fraude. Y dentro de estas funciones puede incluirse el análisis de las causas, el establecimiento de recomendaciones de mejora de los controles establecidos, la realización de seguimientos del canal de denuncias o la promoción de sesiones de formación en relación con la cultura ética de la organización.

En el apartado siguiente profundizamos en el rol que puede adoptar el auditor interno frente al fraude.

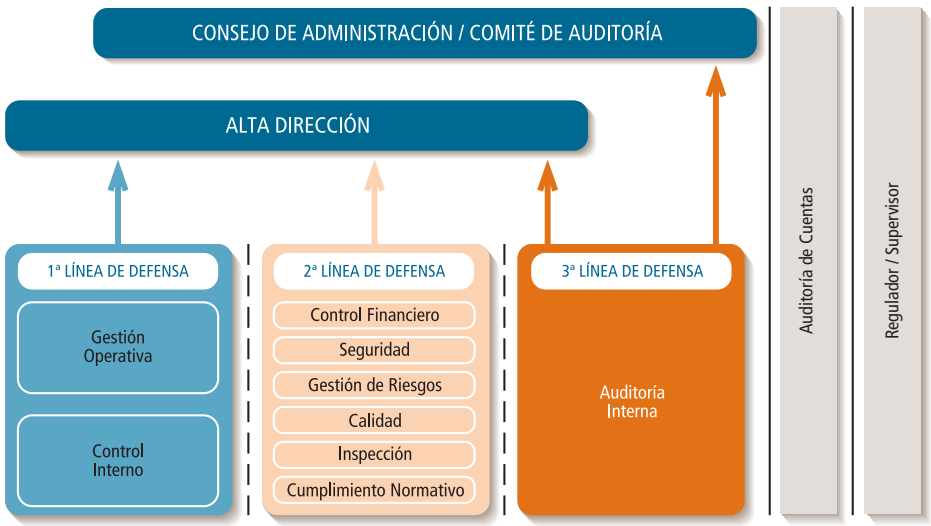
La importancia que una organización concede a su unidad de Auditoría Interna, es un indicador de su grado de compromiso con el control interno.

El rol del auditor interno

Actualmente, es habitual encontrar dentro de las organizaciones equipos compuestos por auditores internos, especialistas en riesgos, especialistas en cumplimiento normativo, investigadores de fraude etc., trabajando conjuntamente en la gestión del riesgo de la organización. Cada uno de estos especialistas tiene una única perspectiva y unas capacidades especificas que aportar a la organización.

Pero, dado que las tareas asociadas a la gestión del riesgo y su control crecen rápidamente y afectan a diversos departamentos y divisiones, deben coordinarse cuidadosamente para asegurar que gestionan adecuadamente el riesgo.

El modelo de las Tres Líneas de Defensa ayuda a delegar y coordinar las tareas de gestión del riesgo de forma sistemática. Este modelo



ofrece una manera simple y efectiva de potenciar las comunicaciones entre los implicados en la gestión y el control del riesgo, a partir de la simplificación de las tareas y responsabilidades de cada área.

Distingue entre tres grupos o líneas de defensa: en la primera línea, se sitúan aquellos que gestionan sus propios riesgos (son los dueños o titulares de los mismos, son las áreas de negocios de las organizaciones); en la segunda línea están los que vigilan los riesgos (departamentos de gestión de riesgo, cumplimento normativo, calidad, etc.) y en la tercera, los terceros independientes que proveen de su asesoramiento (los auditores internos).

La realidad económica y las tendencias en los nuevos roles de Auditoría Interna demandan incluir en los equipos permanentes de Auditoría Interna a miembros con las competencias necesarias en materia de fraude.

NORMATIVA A CONSIDERAR

Auditoría Interna es un ente de la organización a cargo de la ejecución de una actividad independiente y objetiva de aseguramiento y consulta, con responsabilidades en la evaluación de los procesos de gestión de riesgos, control y gobierno. Pero no debe olvidarse incluir entre sus compromisos la responsabilidad en temas de fraude que afectan o puedan afectar a la organización.

El **Código Ético** de Auditoría Interna recoge una serie de principios que cobran especial relevancia en temáticas críticas como las de fraude:

- ***Integridad,*** como capacidad para proporcionar base de confianza en los juicios emitidos.
- ***Objetividad,*** como característica del proceso de obtención, evaluación y comunicación de los hechos examinados, sin dejarse influir por intereses propios o de terceros.
- ***Confidencialidad,*** como deber de respeto del valor y propiedad de la información.
- ***Competencia,*** como medida de idoneidad profesional.

Las **Normas sobre Atributos** establecen que *"los trabajos deben cumplirse con aptitud y cuidado profesional adecuados"* y específicamente cita (1210.A2) que *"los auditores internos deben tener conocimientos suficientes para evaluar el riesgo de fraude y la forma en que se gestiona por parte de la organización, pero no es de esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude"*. Posteriormente indica (1220.A1) que *"el auditor interno debe ejercer el debido cuidado profesional al considerar (…) la probabilidad de errores materiales, fraude o incumplimientos"*.

La realidad económica (aumento de casos de fraude, disminución de recursos para la contratación de expertos, etc.) y las tendencias en los nuevos roles de Auditoría Interna, demandan por parte de la alta dirección que los equipos de Auditoría Interna sean capaces de ofrecer respuestas adecuadas frente a casos de fraudes corporativos. Esta realidad ha motivado que muchas organizaciones estén facilitando a los auditores internos formación en técnicas y habilidades relacionadas con la investigación, e incluyendo en los equipos permanentes de Auditoría Interna a miembros con las competencias necesarias.

El *Marco Internacional para la Práctica Profesional de la Auditoría Interna* (The Institute of

Internal Auditors) define varias normas y consejos relacionados con el fraude, que no reproducimos íntegramente a continuación, pero que ayudan a comprender el rol del auditor interno en toda su extensión.

- 2110 Gobierno
- 2120 Gestión de Riesgos
  Consejo para la práctica 2120-1
- 2130 Control
  Consejo para la práctica 2130.1:
  Control 2130.A1

El marco normativo confiere al Director de Auditoría Interna el deber de *"informar periódicamente a la alta dirección y al Consejo sobre la actividad de auditoría"* y que *"el informe también debe incluir exposiciones al riesgo (…) incluido riesgo de fraude"* (2060). Seguidamente indica que la actividad de Auditoría Interna debe evaluar la posibilidad de ocurrencia de fraude y cómo la organización maneja y gestiona el riesgo de fraude (2120.A2) y que el auditor interno debe considerar la probabilidad de errores, fraude, incumplimientos y otras exposiciones significativas al elaborar los objetivos del trabajo (2210.A2).

Por lo expuesto, la primera responsabilidad de Auditoría Interna en materia de fraude implica la identificación de los riesgos, la revisión de la calidad y operatividad de los controles que mitigan –de forma principal o secundaria– el riesgo de fraude, el deber de informar sobre los riesgos existentes y, paralelamente, formarse y cumplir internamente los requisitos para el desempeño de la función de manera idónea y con total cumplimiento de las normativas vigentes.

Tal como señala la Norma sobre Atributos (1010-Reconocimiento de la definición de Auditoría Interna, el Código de Ética y las Normas, en el Estatuto de Auditoría Interna) la función debe estar definida en propósito, autoridad y responsabilidades dentro del Estatuto que delimita la actividad del área.

El rol del auditor en materia de fraude queda definido en diversas normas del Marco Internacional para la Práctica Profesional de la Auditoría Interna.

Dentro de este Estatuto debe estar claramente definido el rol de Auditoría Interna en relación al tratamiento de los supuestos de comisión de delitos o irregularidades (identificados o denunciados) que se investiguen dentro de la organización, sin perjuicio de las responsabilidades que colateralmente tengan determinados departamentos de la organización en aspectos derivados de la investigación como por ejemplo, el departamento de Asesoría Jurídica, el de Recursos Humanos, etc.

FUNCIONES DEL ÁREA DE AUDITORÍA INTERNA EN MATERIA DE PREVENCIÓN, DETECCIÓN E INVESTIGACIÓN DEL FRAUDE

De acuerdo con la encuesta realizada por el Instituto de Auditores Internos de España, cada vez son más los departamentos de Auditoría Interna que incluyen entre sus funciones la prevención, detección e investigación de fraude. Un 81% de los encuestados manifiesta que entre las funciones de la Auditoría Interna, se encuentra la colaboración en la prevención de fraude interno; un 84% la detección, y un 82%, la investigación. Los porcentajes

El mapa de riesgos de fraude es una parte integrante del mapa de riesgos generales de la organización.

de fraude externo son similares, aunque algo menores, tanto en la prevención como en la detección.

Además, junto a los departamentos de Auditoría Interna, colaboran en la detección e investigación de fraudes los departamentos de sistemas de la información, de cumplimiento normativo, legal, financiero, y recursos humanos.

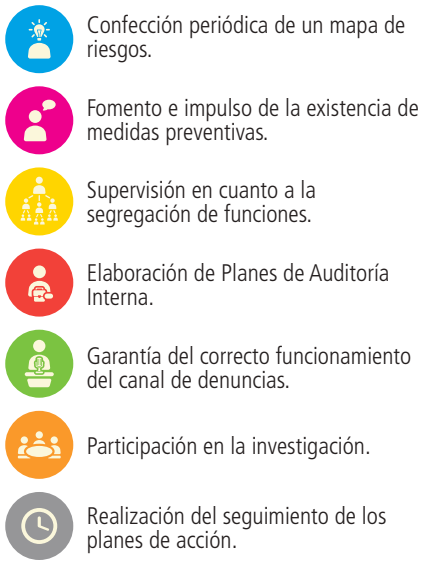
Entendemos que, en temas de riesgos de fraude, pueden ser también responsabilidad de Auditoría Interna:

La confección periódica de un mapa de riesgos. Analizar, con el apoyo de las áreas de negocio, las particularidades en materia de riesgos de fraude de cada proceso: su nivel de exposición, el tipo de procesamiento (manual o sistematizado), las particularidades de la gestión de la empresa (rotación de personal, antigüedad de gestores, posibles situaciones de conflicto de intereses, etc.), los posibles esquemas de fraude, los controles existentes y el grado de cobertura que ofrecen a los riesgos identificados.

Este mapa de riesgos de fraude es una parte del mapa de riesgos generales de la organización, desarrollado dentro del esquema de identificación que establece la organización (para ahondar en materia de *Risk Assessment* nos remitimos a lo ya señalado por el *Enterprise Risk Management* de COSO).

Fomentar e impulsar la existencia de medidas preventivas dentro de la organización en general y los procesos en particular. Algunas de las medidas preventivas se clasifican en:

- La existencia de un marco normativo apropiado y difundido dentro de la empresa, que incluye, entre otros, el código ético, códigos de conducta, código disciplinario y cualquier otro instrumento que dé a conocer el comportamiento ético esperado por parte de las personas (empleados, proveedores, clientes, socios de negocio, etc.) de la organización.
- La difusión y comunicación de los compromisos éticos como normas de comportamiento en todos los niveles.
- Una clara y transparente estructura de roles y funciones.
- La existencia de una metodología adecuada de evaluación de riesgos, conocida, difundida y aplicada.
- Asesorar en la necesidad de controles en los procesos, orientados a minimizar la exposición en riesgos de fraude.
- Prácticas efectivas de supervisión de actividades en cada área de negocio.



- Incorporar objetivos de control en materia de fraude o irregularidades dentro de las revisiones planificadas de auditoría.
- Fomentar la existencia de modelos de detección o alerta temprana gestionados por las áreas de negocio, o como indicadores *(hooks)* por parte de la propia auditoría, en forma de alertas ante anomalías o como *inputs* (en función de su grado de criticidad) para incorporar a posteriores revisiones planificadas.

La supervisión en cuanto a la segregación de funciones. Auditoría Interna mantiene una posición de independencia respecto al resto de áreas de la organización; independencia que ejerce con la debida supervisión en cuanto a la segregación de funciones.

En muchas organizaciones, la responsabilidad de pruebas en segregación de funciones –para bien o para mal– se relega al auditor de sistemas. El razonamiento que subyace tras esta asignación es que la revisión de la segregación de funciones se limita a los controles de acceso a los Sistemas de Información. No es que sea incorrecta, pero pasa por alto la importancia de revisar poderes y permisos para autorizar las funciones y también toda la comprensión de los riesgos de negocio que pueden ir asociados a funciones conflictivas.

Por ello, el auditor informático se eleva por encima de las matrices de configuración de acceso lógico, entiende el negocio de forma que identifica los riesgos y facilita los mecanismos de control más eficientes; es decir, trabaja en el marco de la Auditoría Interna de una forma organizada.

En este sentido se enmarca el rol del auditor interno al comunicar un riesgo asociado a la segregación de funciones: que los controles que deben implantarse vayan alineados con la estrategia y objetivos fijados para la organización. El auditor interno, por lo tanto, debe evaluar tanto que los controles de los poderes de las tecnologías de la información están alineados con la organización del negocio y debidamente implementados, como que los sistemas de control manuales de los poderes o autorizaciones responden realmente a los roles estratégicos asignados.

El auditor interno, con el soporte de auditores de sistemas, puede reforzar tres pilares fundamentales para una correcta segregación de funciones:
- El buen gobierno.
- La gestión de riesgos.
- La adecuación de los controles.

La elaboración de Planes de Auditoría Interna. Debe entenderse por planificación de Auditoría Interna el conjunto de planes, programas y actividades propios de auditoría encaminados a organizar en el tiempo la actividad de la función de Auditoría Interna, con la finalidad de que ésta garantice de forma eficaz y eficiente la máxima cobertura de los riesgos de la organización con los recursos de los que dispone.

La planificación es una actividad continua, lo que significa que debe existir una retroalimentación que permita, a su vez, que sea influida por los resultados de los trabajos programados.

Esto supone que los auditores internos deben obtener de su trabajo información para la elaboración de los planes correspondientes y fijar el alcance de futuras auditorías, recursos necesarios, tiempos de ejecución, rotación de riesgos, etc.

La planificación de Auditoría Interna es una actividad continua que debe contar con la necesaria retroalimentación y actualización periódica.

Un proceso de identificación y evaluación de riesgos es un elemento básico de un sistema de control y una de las bases del Plan de Auditoría Interna.

Auditoría Interna se encarga de la elaboración de los Planes de Auditoría, y considera en todo momento las opiniones e inquietudes de la dirección.

Estos planes deben ser consecuentes con el Estatuto de Auditoría Interna, con los objetivos de la organización y de Auditoría Interna y con los requisitos de los reguladores en materia de Auditoría Interna y control interno.

La eficacia en la elaboración de los mencionados planes radica en un conocimiento global del universo auditable (diferente al contable), así como de aplicar un enfoque basado en riesgos, para que la planificación de la auditoría vaya alineada con el crecimiento de las líneas de negocio y de los cambios que sufren las organizaciones.

La evaluación de riesgos permite analizar el impacto de los potenciales eventos en el logro de los objetivos. Por tanto, un proceso para identificar y evaluar los riesgos es un pilar básico de un sistema de control adecuado y una de las bases para establecer un Plan de Auditoría Interna.

Los cambios a los que se enfrentan las organizaciones hacen que los planes deban ser actualizados de forma periódica, al menos anualmente.

Garantizar el correcto funcionamiento del canal de denuncias. Auditoría Interna puede tener también la obligación de vigilar el cumplimiento de todo lo relacionado con el canal de denuncias, a fin de asegurar que está siendo debidamente administrado, que las denuncias recibidas son tratadas convenientemente y que, en el caso de producirse irregularidades, estás son adecuadamente identificadas.

De forma complementaria, Auditoría Interna debe coordinarse con los servicios jurídicos en aquellos aspectos que puedan tener implicaciones legales.

Además, es necesario establecer protocolos de actuación para aquellas denuncias que se reciben en temas de acoso o discriminación, derivando su tratamiento, por ejemplo, al área de relaciones laborales.

Por último, la metodología para la correcta evaluación de denuncias debe ser aplicable para el análisis de riesgos, previo a la realización de los trabajos de auditoría.

La participación en la investigación. La participación del auditor interno en las investigaciones de fraude puede ser diversa y abarcar diferentes niveles de responsabilidad en función de la organizacion:

- Realización de la investigación en una fase inicial, hasta confirmar las sospechas/indicios o desestimar la existencia de fraude.
- Realización de la investigación únicamente en casos de hasta un cierto límite de daño, o en casos que no requieran determinadas competencias o medios técnicos especiales, con los que no cuenta el área de Auditoría Interna.
- Realización completa de la investigación y coordinación con un equipo multidisciplinar.
- Colaboración/asistencia técnica a equipos externos, que lideran el proceso.
- Seguimiento de la implantación de recomendaciones o acciones de mejora propuestas por el equipo responsable de la investigación.

Los distintos roles que pueda adoptar Auditoría Interna en la investigación deben estar

previstos en las políticas corporativas y en los propios estatutos de Auditoría Interna. Estas directrices posicionan la labor del auditor interno y establecen su responsabilidad en la investigación, reconociendo su autoridad a todos los niveles dentro de la empresa.

En cualquier caso, consideramos que el auditor interno, al menos:

- Debe ser informado de la existencia de cualquier potencial fraude en los momentos previos a la investigación, dado que se encuentra en la mejor posición, por su presencia en la compañía y su conocimiento del negocio, para prestar un apoyo experto sobre la potencial irregularidad y los posibles pasos a llevar a cabo. Todo ello con independencia del rol que desempeñe en la futura investigación.
- Debe ser informado de los avances que se produzcan.
- Debe ser informado de los resultados finales de la investigación y de las posibles acciones, dado que los resultados pueden afectar al plan de trabajo del área de Auditoría Interna y a la evaluación y seguimiento de controles que realiza el área.

La investigación puede realizarse con personal propio o terceros especialistas contratados. Pero la gestión y supervisión debe recaer necesariamente en las áreas de Auditoría Interna y Asesoría Jurídica de la empresa.

Si la investigación de las denuncias recibidas o de las alertas identificadas recae en el departamento de Auditoría Interna, el mismo debe:

- Cumplir las normas y principios en su labor de investigación, soportando fehacientemente los hallazgos y realizando la labor con la idoneidad, transparencia y competencia debida.

  Algunas organizaciones realizan grandes esfuerzos para que los miembros de Auditoría Interna cuenten con la competencia y la capacidad para llevar a cabo las correspondientes investigaciones. Un 45% de los encuestados por el IAI manifiesta que sus equipos de Auditoría Interna no cuentan con formación especializada en investigación de fraudes y un 50% no cuenta con los recursos técnicos e informáticos adecuados.

- Documentar con el debido celo profesional todos los pasos ejecutados, prestando especial atención a la validez legal en la captura de evidencias y el debido soporte de los hallazgos, no sólo de cara a sustentar y soportar el contenido del informe final, sino además como soporte y herramienta de defensa de la empresa cuando, en caso de producirse una irregularidad, la organización decida iniciar acciones legales contra el infractor y sea necesario utilizar estas evidencias como prueba. Es necesario que Auditoría Interna cuente con el asesoramiento del área de Asesoría Jurídica de la empresa cuando sea necesario.

- Asesorarse/capacitarse sobre las particularidades legales que debe cumplir en la captura, tratamiento y custodia de datos de empleados, o terceros y en la forma en que puede acceder a los mismos durante la investigación, para no invalidar la prueba. El área de Asesoría Jurídica debe asesorar en materia de derechos del empleado y obligaciones legales de la empresa, para no

Cuando Auditoría Interna investigue denuncias o alertas de fraude debe documentar adecuadamente sus hallazgos y realizar su labor con la idoneidad, transparencia y competencia debidas.

violar principios constitucionales, ni leyes, ni cualquier otro tipo de normativa vigente[6].

- Informar a los órganos de gobierno de la empresa sobre las características de los hechos denunciados o identificados e investigados.

Realizar el seguimiento de los planes de acción para instaurar medidas correctivas de las debilidades de control o puntos de mejora en el desarrollo de los procesos, con el fin de garantizar la mejora continua del sistema de control interno (en el caso de la efectiva implantación de las medidas) o de alertar ante la permanencia de situaciones que exponen a la organización (en el caso de demoras o inacción en la implantación de medidas correctivas).

A continuación exponemos una matriz, a modo ilustrativo, que resume y visualiza las responsabilidades en materia de prevención, detección e investigación de fraude de los diferentes departamentos que forman una organización, entre ellos, el departamento de Auditoría Interna.

6. Es posible que sea necesaria la aplicación de procedimientos específicos para la recopilación de evidencia digital para los que el área de Auditoría Interna no dispone ni de los medios técnicos ni de las habilidades necesarias, para lo que, de acuerdo con la Norma 1210. A1, sea necesaria la intervención de expertos externos:

   "el Director de Auditoría Interna debe obtener asesoramiento y asistencia competentes en caso de que los auditores internos carezcan de los conocimientos, las aptitudes u otras competencias necesarias para llevar a cabo el trabajo"

   En estos casos, Auditoría Interna debe ponerse a disposición del equipo externo ofreciendo su cooperación y estando dispuesto a participar en el proceso en aquello para lo que se le requiera. Así, puede prestar una colaboración útil en identificar la información relevante y dónde se encuentra alojada (bases de datos, ficheros, etc.) ya que normalmente Auditoría Interna conoce estos aspectos por el curso de su actividad cotidiana, lo que puede suponer ahorros de tiempo. En cualquier caso, participe activamente Auditoría Interna o no, es importante mantener un clima de buen entendimiento entre ambos equipos ya que ambos trabajan por un mismo fin.

   PRECAUCIONES

   La Norma 1220. A2 referente al Cuidado Profesional en el ejercicio de su actividad dice: *"al ejercer el debido cuidado profesional el auditor interno debe considerar la utilización de auditoría basada en tecnología y otras técnicas de análisis de datos"*.

   y la Norma 1220.A3: *"el auditor interno debe estar alerta a los riesgos materiales que pudieran afectar los objetivos, las operaciones o los recursos"*.

   Por ello, el auditor interno debe actuar con la prudencia debida en tareas especialmente sensibles, para lo que debe evaluar cuáles son los riesgos a los que se enfrenta cuando aplica procedimientos que pueden tener un impacto elevado en el proceso, como son todos los relacionados con la evidencia digital. En particular, el auditor interno debe ser extremadamente prudente en no recopilar evidencias sin las debidas garantías simplemente porque conoce cómo llegar a ellas, no manipular evidencias para darles otra apariencia o no respetar la cadena de custodia.

EJEMPLO DE MATRIZ DE DECISIÓN EN LA POLÍTICA DE PREVENCIÓN, DETECCIÓN E INVESTIGACIÓN DE FRAUDE

ACCIÓN REQUERIDA	UNIDAD DE INVESTIGACIÓN	AUDITORÍA INTERNA	FINANZAS / CONTABILIDAD	DIRECCIÓN EJECUTIVA	DIRECCIÓN OPERACIONES	DIRECCIÓN RIESGOS	ÁREA COMUNICACIÓN	RR.HH	LEGAL
Controles para la prevención del fraude	S	S	S	P	C	C	S	S	S
Reportes de incidentes detectados	P	S	S	S	S	C	S	S	S
Investigación de fraude	P	S						S	S
Comunicación con las Autoridades	P								S
Recuperación de las cantidades defraudadas	P								
Recomendaciones para la prevención del fraude	C	C	S	S	S	C	S	S	S
Revisión de los controles internos		P							
Atender los casos/ situaciones de naturaleza sensible	P	S		S		C		S	S
Comunicados de prensa / Publicidad	S	S					P		
Litigios civiles	S	S							P
Acciones correctivas / Recomendaciones para prevenir acciones recurrentes	C	C		S	C	S			S
Supervisión de las recuperaciones	S		P						
Auditorías proactivas de fraude	S	P							
Formación y entrenamiento sobre el fraude	P	S			S		S		
Análisis de riesgos en las áreas de vulnerabilidad	S	S				P			
Análisis de los casos	P	S							
Canal de denuncias (1)	P	S							
Línea ética	S	S							P

P Responsabilidad Primaria S Responsabilidad Secundaria C Responsabilidad Compartida

Fuente: *Managing the Business Risk of Fraud: A Practical Guide* (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiners).

(1) Respecto al Canal de Denuncias, si seguimos las recomendaciones de la CNMV en materia de control interno sobre la información financiera en sociedades cotizadas, el Comité de Auditoría debe tener conocimiento y acceso directo a la denuncia de potenciales irregularidades. Por tanto, entendemos que es deseable que Auditoría Interna gestione el canal de denuncias, pudiendo ser el mismo administrado por la propia Auditoría Interna, por un departamento específico o bien por un tercero.

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

Depósito Legal: M-4003-2015

ISBN: 978-84-943299-0-6

Diseño y maquetación: desdecero, estudio gráfico

Impresión: IAG, SL

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Este nuevo documento de LA FÁBRICA DE PENSAMIENTO, el *think tank* del Instituto de Auditores Internos de España, aborda los diferentes procesos para una óptima gestión del riesgo de fraude, que pasa por el establecimiento de un programa eficaz de prevención, detección e investigación de fraudes.

Esta publicación, resumen ejecutivo del amplio estudio elaborado por la Comisión Técnica que será editado próximamente, define además un enfoque efectivo para la gestión del riesgo de fraude y un análisis profundo sobre las responsabilidades en su prevención, detección e investigación.

Se trata de una guía, en definitiva, que ayudará a la alta dirección –en la que debe comenzar el sistema de principios, valores y comportamientos adecuados para la organización– y a los auditores internos, que encontrarán las respuestas adecuadas frente a casos de fraudes corporativos.

Instituto de Auditores Internos de España

The Institute of Internal Auditors