Revista de Contabilidad y Dirección
Vol. 23, año 2016, pp. 41-59

Diseño del sistema organizativo y de control interno para la prevención y detección del fraude

JORDI RIERA
PEDRO RUANO
Ernst & Young

Fecha de recepción: 25/01/2016
Fecha de aceptación: 26/04/2016

RESUMEN

El último informe sobre fraude y corrupción de EY señala que 7 de cada 10 directivos españoles alertan de que los sobornos y la corrupción son el *modus operandi* habitual en los negocios. Tomando como referencia esta nefasta percepción (o realidad según con qué prisma se mire) resulta imprescindible que las empresas, y sobre todo sus órganos de administración, implanten en el seno de su organización las medidas oportunas para minimizar los potenciales riesgos de fraude que deban afrontar. Como respuesta a este riesgo es fundamental que los órganos de administración de las compañías y los propios directivos estén involucrados en la implantación de los denominados programas antifraude. Dichos programas tienen como objetivo principal la prevención y la detección del fraude interno y constan de tres elementos clave: (i) establecer un tono adecuado en la organización, (ii) actuar proactivamente y (iii) tener implantado un plan de respuesta.

Clasificación JEL: D21; M40; M42

PALABRAS CLAVE

Perfil, motivaciones, defraudador.

ABSTRACT

The latest report on fraud and corruption EY notes that 7 out of 10 Spanish executives warn that bribery and corruption are the usual modus operandi in business. Referencing this negative perception (or reality, depending on how you look at it) is essential that companies, especially their management bodies, implement within the organization adecuquate measures to minimize the potential risks of fraud. In response to this risk is essential that the corporate gorvernance and managers themselves are involved in the implementation of so-called anti-fraud programs. These programs are aimed to prevention and detection of internal fraud and consist of three key elements; (I) establish an appropriate tone in the organization, (ii) act proactively and (iii) have implemented a response plan.

Classification JEL: D21; M40; M42

KEYWORDS

Internal oganizational system, prevention, fraud.

1. Introducción

Las recientes reformas legislativas, y particularmente la reforma de la Ley de Sociedades de Capital, imponen claramente a los administradores la responsabilidad de adoptar las medidas precisas para la buena dirección y el control de la sociedad que administran y, en el caso de empresas cotizadas, además especifican la obligación indelegable de determinar las políticas de control interno y gestión de riesgos.

Por tanto, ¿debemos considerar que los administradores son los únicos responsables de la lucha contra el fraude? Evidentemente no. La prevención y detección del fraude debe ser una cuestión que implique a toda la organización, desde el primer ejecutivo hasta el último empleado. Pero para conseguir este objetivo no basta con implantar medidas disuasorias, es necesario instituir una cultura que fluya de forma transversal por toda la organización, y que permeabilice las distintas capas que la conforman. Esta cultura debe ser perdurable en el tiempo y debe estar presente en el día a día de todos los miembros de la organización.

En este artículo expondremos cómo diseñar un sistema organizativo y de control interno para la prevención y detección del fraude considerando

que el mismo debe ser perdurable, transversal y revisable. Para ello, resulta imprescindible iniciar nuestra disquisición hablando sobre el Gobierno Corporativo y su rol en la prevención y detección del fraude.

2. El rol del Gobierno Corporativo en la lucha contra el fraude

El término Gobierno Corporativo hace referencia a los órganos de responsabilidad de una organización empresarial y describe las responsabilidades del conjunto de estamentos que la conforman. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) lo describe en sus "*Principios de Gobierno Corporativo*" como:

> "*Los procedimientos y procesos según los cuales una organización es dirigida y controlada. La estructura de gobierno corporativo especifica la distribución de derechos y responsabilidades entre las diferentes partes de la organización –el consejo de administración, la dirección ejecutiva, los accionistas u otras partes interesadas- y establece las normas y procedimientos para la toma de decisiones*".

El Gobierno Corporativo es el punto de partida a partir del cual debe establecerse la cultura antifraude que comentábamos previamente. Sin embargo, no todas las partes que integran el Gobierno Corporativo tienen las mismas funciones ni la misma responsabilidad. A continuación, enumeramos de forma sucinta las distintas funciones y responsabilidades de cada una de ellas:

- El órgano de administración

Tal y como hemos indicado previamente, los recientes cambios legislativos acaecidos en España no dejan lugar a duda de que los administradores son los responsables finales de la existencia de un adecuado marco de control interno de la organización, por tanto, su papel en este ámbito resulta fundamental.

Los administradores son responsables de velar por el buen uso de los recursos y activos de la empresa, y representan el nexo de unión entre la propiedad (los accionistas o socios), y quienes gestionan la organización (los directivos). Así, el órgano de administración es responsable de definir los objetivos y estrategias de la organización, y de supervisar su correcta ejecución por parte de los directivos.

La importancia de la participación activa y comprometida del órgano de administración en la gestión de los riesgos de fraude no debe ser subestimada. Su dedicación no solo sirve para establecer una cultura antifraude, sino también para generar confianza a los accionistas y realzar la reputación ética de la organización.

• Comités y comisiones delegadas

Con el objetivo de supervisar ciertos temas específicos, el órgano de administración puede delegar en los miembros del propio órgano, o en otras personas especializadas, aspectos de control concretos.

En relación con el contenido de este artículo nos gustaría destacar los comités que, a nuestro entender, tienen un papel más relevante en la prevención y detección del fraude: el comité de auditoría y el comité de prevención penal.

i. **Comité de auditoría:** En el año 2002 se estableció por primera vez la obligatoriedad de que las compañías cotizadas tuvieran un comité de auditoría. Contar con un comité de auditoría proporciona a los accionistas un confort adicional en relación con la integridad de los estados financieros. Las funciones de este comité pueden variar de una organización a otra dependiendo de su tamaño, sector o áreas geográficas de influencia, pero en términos generales son las de supervisar la integridad de la información contenida en los estados financieros y velar por la efectividad del sistema de control interno contable.

ii. **Comité de prevención penal:** Desde el pasado 1 de julio de 2015, fecha de entrada en vigor de la Ley Orgánica 1/2015 según la cual se modifica el Código Penal, las compañías que no estén autorizadas a presentar cuentas de pérdidas y ganancias abreviadas están obligadas a implantar estos comités si quieren cumplir con una de las condiciones establecidas para la exención de responsabilidad penal de la persona jurídica.

   Según se establece en la propia Ley, el órgano de administración de la sociedad debe confiar a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control, la supervisión del funcionamiento y del cumplimiento del modelo de prevención de delitos adoptado.

   A pesar de que estos modelos de prevención de delitos analizan los riesgos (delitos) que puedan cometerse desde la empresa y en su propio beneficio, es indudable que estos comités irán adquiriendo más relevancia en los próximos años. Esta importancia será, si cabe, muy superior en las empresas no cotizadas, donde dicho comité podrá realizar, además de las funciones descritas en el Código Penal,

otras funciones que en compañías cotizadas realizan habitualmente los comités de auditoría, es decir, convertirse en los denominados comités éticos o de *compliance*.

• Dirección ejecutiva

El equipo que conforma la dirección ejecutiva dirige la organización y a sus empleados y es responsable de las decisiones que afectan al día a día y, en última instancia, a los accionistas.

La dirección ejecutiva está liderada por el CEO (*Chief Executive Officer*) y normalmente la componen los jefes o directores de finanzas, legal, recursos humanos, operaciones e informática. Los principales roles y funciones de la dirección ejecutiva actuando en conjunto y en relación al gobierno corporativo, son los de establecer los objetivos estratégicos y operacionales bajo la supervisión del consejo de administración, dirigir a los empleados en el desarrollo de sus actividades diarias, vigilar los resultados de sus tareas y establecer el tono ético real de la organización.

• Accionistas

Los accionistas son los propietarios de las organizaciones y, como tales, están preocupados en primer lugar por maximizar el retorno de su inversión. Con este objetivo, los accionistas tienen la responsabilidad de estar activamente involucrados en los procesos de Gobierno Corporativo. Esta involucración incluye, entre otros aspectos, el permanecer informados acerca de las operaciones y resultados de la compañía, leer y analizar los reportes y otras comunicaciones preparadas por la dirección de la corporación y, en el caso de tener dudas o cuestiones, plantearlas al consejo de administración.

En definitiva, una lucha eficaz contra el fraude requiere dedicación y un análisis focalizado, incluyendo un proceso formal de supervisión por parte del órgano de administración, y una participación activa por parte de los accionistas. El órgano de administración debe supervisar las políticas y controles establecidos y la efectividad de los mismos desde un punto de vista global, y los accionistas, por su parte, deben asegurarse de que las personas que eligen para formar el órgano de administración estén capacitadas para llevar a cabo dicha supervisión. Esta interdependencia establece las condiciones necesarias para una gestión del riesgo de fraude eficaz.

Una vez analizadas las funciones y responsabilidades de las distintas partes que conforman el Gobierno Corporativo en relación con la prevención y detección del fraude, continuaremos nuestra exposición focalizándonos en cómo debe ser el marco de control interno a implantar para luchar contra el fraude de forma efectiva y eficaz. Este marco de control interno y cumplimiento normativo recibe la denominación de Programa Antifraude.

3. Qué es un Programa Antifraude

Tal y como hemos comentado previamente, las funciones de control interno que ayudan a la prevención y detección del fraude deben extenderse a todos los estamentos e individuos de la organización. Basándonos en este axioma principal y en las mejores prácticas internacionales de control interno definidas por el *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), se ha definido el Programa Antifraude de EY.

En mayo de 2013, COSO publicó su marco actualizado para el diseño, implementación, desarrollo y evaluación de los sistemas de control interno. El nuevo marco tomó gran parte de la estructura del marco original emitido en 1992, poniendo de relieve las nuevas áreas de interés y preocupación, entre ellas, los riesgos de fraude que, a partir de ese momento, pasan a ser considerados de forma independiente del resto de riesgos de la organización.

Con el objetivo de cumplir con los objetivos operacionales, de reporte y de cumplimiento normativo, COSO identificó cinco componentes interrelacionados de control interno: el ambiente de control, la evaluación de riesgos, las actividades de control, la información y comunicación, y la supervisión y seguimiento.

Siguiendo estas premisas, el Programa Antifraude de EY se ha planteado como una estrategia integral de lucha contra el fraude que ayude a la dirección y al órgano de administración proporcionando una herramienta de supervisión y seguimiento del riesgo de fraude en la organización y que identifique oportunidades de mejora. En la figura 1 mostramos un resumen representativo de los elementos esenciales que debe incluir este Programa Antifraude.

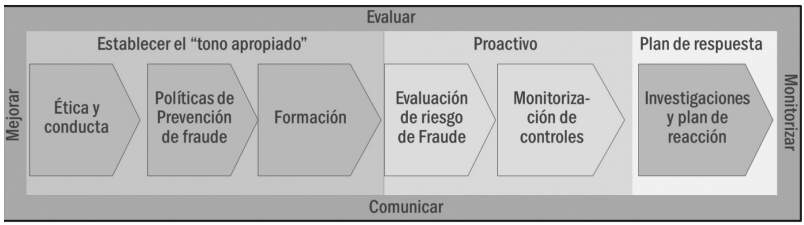

Figura 1. Elementos esenciales del Programa Antifraude.

Tal y como podemos observar en el gráfico, tres son los elementos clave que debe incluir la correcta implantación de un Programa Antifraude.

En los siguientes puntos de este artículo trataremos en profundidad los tres aspectos anteriores.

4. Establecimiento del tono adecuado para la prevención del fraude

Cuando hablamos del "tono adecuado" de una organización, nos estamos refiriendo a los principios de actuación definidos por la alta dirección que deben guiar el modo en que todos los miembros de la entidad deben comportarse y deben desarrollar su actividad profesional (*tone at the top*). Los principales marcos internacionales en materia de Compliance coinciden en considerar como elemento clave para que un programa de cumplimiento sea efectivo, que los líderes de la organización se comprometan de forma clara e inequívoca a promocionar y respetar principios de actuación basados en los más altos estándares éticos.

En las organizaciones donde la alta dirección alienta y respalda estándares de actuación éticos, la propensión de sus empleados a actuar de forma íntegra será más elevada que en aquellas organizaciones en las que la alta dirección no esté, o no parezca estar, interesada y concienciada de la necesidad de seguir y promover conductas de actuación éticas para lograr los objetivos marcados. Aquellas organizaciones que se focalizan exclusivamente en la consecución de objetivos económicos tienen un mayor riesgo de experimentar incidentes de fraude causados por sus empleados, pues éstos pueden entender que la prioridad de la organización es lograr a toda costa los objetivos económicos marcados, sin importar qué medios deban utilizarse para ello.

De acuerdo con el último estudio sobre fraude publicado por ACFE (*Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Survey*), una de las principales causas que explican por qué se produjo fraude en los casos analizados es que la organización no había establecido un tono adecuado.

Así, para crear una cultura de integridad, es preciso que los principios y actuaciones éticas estén presentes en la operativa diaria de la organización; por ello, en primer lugar consideramos imprescindible comunicar de forma clara e inequívoca a los empleados qué se espera de ellos. Y el punto de partida para lograr este objetivo es disponer de un código ético o de conducta en el que se establezcan claramente los valores éticos y los objetivos corporativos que deben ser respetados, proporcionando un marco general de actuación que permita guiar el desarrollo profesional de todos los miembros de la organización.

Dada la importancia del código ético, que es sin lugar a dudas la piedra angular a partir de la cual se debe establecer el tono de la organización, y del cual deben emanar el resto de políticas y procedimientos internos, resulta altamente recomendable que sea aprobado por el órgano de administración. Asimismo, se debe garantizar que el código ético no sea un elemento meramente cosmético "hacia el exterior", motivo por el cual, su aprobación debe ir acompañada por acciones dirigidas a su adecuada promoción y difusión entre todos sus destinatarios (administradores, directivos, empleados y terceras partes que se relacionan con la organización, como por ejemplo agentes o intermediarios), y debe ser objeto de revisión y actualización a lo largo del tiempo.

Pero como hemos señalado, el código ético proporciona un marco general de actuación, y, por lo tanto, es preciso desarrollar políticas y procedimientos internos específicos que permitan una adecuada gestión del riesgo de fraude. Así pues, es recomendable que las organizaciones implementen políticas de prevención de fraude que expongan de forma clara y sin ambigüedades la posición de la organización respecto al fraude, y donde se asignen las autoridades y responsabilidades en relación con la gestión de este tipo de riesgo. Resulta igualmente relevante detallar las acciones que constituyen fraude y que por lo tanto serán objeto de investigación y sanción por parte de la organización, así como los medios puestos a disposición de los empleados y de terceros para poder reportar irregularidades.

En este sentido, es importante tener en cuenta que no es posible reflejar en un documento escrito todas y cada una de las posibles situaciones éticamente comprometidas a las que un empleado puede tener que hacer frente a lo largo de su carrera profesional. Por tanto, aquellas entidades que pretendan establecer un *checklist* de actividades prohibidas, corren el riego de transmitir un mensaje equivocado a sus empleados, en el sentido de que éstos puedan creer que "si no está específicamente prohibido, está permitido".

Las organizaciones deben promover la creación de una cultura orientada hacia el comportamiento íntegro, de modo que cuando sus empleados estén ante una situación éticamente comprometida, sean capaces de reflexionar sobre cuál debe ser el modo de actuar siguiendo los principios y valores definidos por la organización.

Y el modo en que la alta dirección puede fomentar dicha cultura es liderando mediante el ejemplo. La actitud frente al fraude de los mandos directivos resulta capital en el establecimiento del tono general de la organización. De acuerdo con la ACFE una de las medidas más efectivas que una organización puede adoptar para reforzar su marco ético de actuación es incorporar empleados con un historial profesional éticamente intachable, especialmente en los cuadros de mando más elevados.

Una vez instituida una cultura de integridad en la organización, el siguiente paso necesario para establecer un tono adecuado para la prevención del fraude, es proporcionar a todos los miembros de la organización, incluidas terceras partes relacionadas con ellas, mecanismos de comunicación seguros a través de los cuales poder denunciar irregularidades y comportamientos contrarios a los principios éticos definidos en las políticas internas de la organización. Los denominados canales de denuncia (o *hotlines*) han demostrado ser mecanismos efectivos para descubrir fraudes en las organizaciones.

De acuerdo con los últimos datos publicados por ACFE, las denuncias son el método de detección de fraude más común, con mucha diferencia respecto al siguiente. En más del 40% de los casos analizados en dicho estudio, se tuvo conocimiento de la existencia del fraude como consecuencia de una denuncia. Asimismo, dicho estudio también concluye que aquellas organizaciones que cuentan con canales de denuncia son capaces de detectar la ocurrencia del fraude en la mitad de tiempo y sufrir pérdidas un 40% inferior a aquellas organizaciones que no cuentan con estos mecanismos de control.

Promocionar la existencia de un canal de denuncias en la organización, que permita a los empleados (e incluso a terceros) reportar irregularidades de forma confidencial y sin temor a represalias, traslada el mensaje de que la organización promueve y favorece un ambiente de trabajo ético, que por sí solo puede actuar como elemento de disuasión ante la comisión de fraude.

Por otro lado, el tercer elemento clave para establecer de forma exitosa una cultura antifraude en la organización es la comunicación y formación. Como ya hemos señalado, la publicación del código ético debe ir acompañada de acciones destinadas a promocionarlo y difundirlo entre todos los miembros de la organización, incluyendo, si fuera necesario, terceras partes relevantes en el desarrollo de la operativa de negocio. Pero no solo se trata de promocionar el código ético, todo el resto de políticas y procedimientos internos específicos, así como aquellas herramientas implementadas para una adecuada gestión del fraude, como es el caso de los canales de denuncia, deben ser bien conocidos a lo largo y ancho de la organización.

Aquellas organizaciones que no se preocupan por dar a conocer entre sus empleados las iniciativas puestas en marcha, o no se aseguran de que se conozca, comprenda y comparta el marco normativo interno, corren un mayor riesgo de sufrir fraude y, como ya hemos visto, de que estos incidentes tarden más en ser descubiertos y que las pérdidas ocasionadas sean mayores.

Así pues, las comunicaciones internas y externas, bien sean formales, como por ejemplo mediante mensajes de la alta dirección a toda la organi-

zación, bien sean informales, por ejemplo reforzando mensajes claves en reuniones de departamento, ayudan a reforzar el tono de la organización en materia antifraude.

Finalmente es importante subrayar que, para que el mensaje cale debidamente entre todos los estamentos de la organización, es preciso acompañar estas acciones de comunicación de un plan de formación ambicioso y efectivo que cubra todos aquellos aspectos relevantes que permitan dotar a sus empleados de los conocimientos suficientes y del espíritu crítico necesario para identificar situaciones irregulares y ponerlas en conocimiento de aquellas personas o áreas que correspondan.

Todos los miembros de la organización, incluidos los de la alta dirección, deben recibir formación periódicamente sobre prevención y detección de incidentes de fraude. Por ello, un plan de formación efectivo debe incluir el estudio y análisis de las normas, políticas y herramientas que la organización ha implementado para prevenir o detectar fraude, así como los roles y responsabilidades de cada empleado en la identificación y denuncia de irregularidades o comportamientos contrarios a los principios éticos de la organización. Es igualmente relevante informar sobre qué actuaciones (u omisión de las mismas) están prohibidas de acuerdo con las normas internas y/o con las leyes aplicables, a fin de evitar que los empleados incurran en situaciones comprometidas por desconocimiento.

En resumen, el establecimiento del tono adecuado por parte de la alta dirección ayudará a prevenir y reducir las pérdidas por fraude y favorecerá la creación de un entorno laboral ético que redundará en una mejora de la moral de los empleados y de su lealtad hacia la organización. Prevenir el fraude es un buen negocio, pero debe empezar en la cúspide de la organización.

5. Controles proactivos para la prevención y detección de fraude

Una gestión proactiva de los riesgos de fraude requiere contar con un programa antifraude efectivo. En esta sección estudiaremos dos componentes fundamentales de cualquier sistema de gestión efectivo:

- La realización de evaluaciones de riesgos periódicas
- Contar con un sistema de monitorización de los controles

5.1. Evaluación de riesgos de fraude

Para que un sistema de prevención y detección del fraude sea efectivo y permita asegurar razonablemente que contiene todos aquellos elementos necesarios para mitigar la probabilidad de ocurrencia del mismo, es necesario adoptar un enfoque basado en riesgos.

Para poder valorar si las medidas de control implantadas son adecuadas y suficientes para prevenir o detectar la ocurrencia de fraude en el seno de la organización, es preciso, en primer lugar, conocer los riesgos de fraude a los que la organización está expuesta por razón de su tamaño, de su estructura y complejidad organizativa, de su actividad, del entorno económico y regulatorio en el que opera, etc. Por consiguiente, resulta fundamental llevar a cabo una evaluación de riesgos de fraude.

Dado que las organizaciones son diferentes unas de otras, y están, además, en constante cambio y evolución, la evaluación de riesgos de fraude debe estar específicamente diseñada para cubrir las concretas necesidades de cada organización, y debe ser objeto de revisión y actualización de forma recurrente a lo largo del tiempo.

Veamos a continuación qué pasos debemos seguir para poder llevar a cabo una adecuada evaluación de los riesgos de fraude en nuestra organización:

a) *Planificar la evaluación de los riesgos de fraude*

En primer lugar es preciso planificar el modo en que se va a llevar a cabo la evaluación de los riesgos de fraude, teniendo en cuenta las particularidades de la organización (cultura empresarial, estructuras jerárquicas, etc.).

Los principales objetivos de esta fase deben ser:

- Configurar un equipo de trabajo que cuente con los conocimientos y las capacidades adecuadas. Este equipo puede estar formado tanto por recursos internos como externos, o por una mezcla de ambos.
- Determinar la metodología de trabajo a emplear en la evaluación de los riesgos de fraude. Los métodos y técnicas que se pueden utilizar al evaluar riesgos son múltiples (entrevistas individualizadas, *focus groups*, cuestionarios, encuestas, etc.), por lo que resulta preciso identificar el método, o métodos, que mejor se adapten a la cultura y circunstancias concretas de cada organización.
- Consensuar los objetivos, alcance, fases y calendario de ejecución del trabajo a realizar, acordando las directrices y estamentos para la adecuada gestión, control y seguimiento del proyecto.

- Identificar y entender el universo de riesgos de fraude que resulta aplicable a la organización, dada su actividad y el entorno en el que opera.
- Comunicar los objetivos del proyecto a todos los actores relevantes de la organización que vayan a participar en la evaluación de riesgos. Los empleados serán más propensos a participar activamente en el proceso si entienden por qué se hace y qué se espera de ellos.

b) *Ejecutar la evaluación de los riesgos de fraude*

Una vez definido el enfoque metodológico, es el momento de realizar el diagnóstico sobre la situación actual de la organización con respecto a los riesgos de fraude.

Los principales objetivos de esta fase son:

- *Identificar los potenciales riesgos de fraude en cada uno de los procesos y actividades incluidos en el alcance*. Una de las técnicas más efectivas para recopilar información que permita una exhaustiva identificación de los riesgos de fraude es mediante entrevistas tanto con las áreas claves en la gestión del riesgo de fraude (función legal, compliance o auditoría interna), como con aquellas áreas donde presumiblemente haya una mayor probabilidad de ocurrencia de fraude. También son instrumentos útiles para identificar los riesgos de fraude el envío de cuestionarios y la realización de encuestas entre el personal de las áreas claves.
- *Valorar los riesgos de fraude identificados*. Una vez identificados los riesgos es preciso valorarlos, sin tener en cuenta los controles existentes (*valoración del riesgo inherente*), ponderándolos en términos de probabilidad e impacto, al objeto de priorizarlos.
- *Identificar y evaluar la suficiencia de los controles existentes*. Definido el mapa de riesgos aplicable, es el momento de identificar, analizar y evaluar el grado de suficiencia de los controles existentes en la organización que deben mitigar la probabilidad de ocurrencia de los riesgos identificados. Con carácter general, los controles existentes en las organizaciones se pueden agrupar en tres categorías principales:
  - Políticas corporativas globales. Son aquellas que establecen los valores y principios éticos que marcan las pautas de actuación de todos los miembros de la organización en el desempeño de sus funciones profesionales. En esta categoría se engloban políticas de alto nivel como son el código ético, el procedimiento de denuncias o la política anticorrupción.

- Normas internas que regulan la operativa. Son aquellas normas o procedimientos que, siguiendo las directrices generales contenidas en las políticas corporativas de carácter global, describen el marco de actuación concreto que debe ser observado en la ejecución de tareas específicas. Un ejemplo de normas que forman parte de esta categoría son los procedimientos de compras, contrataciones e inversiones.
- Controles y procedimientos operacionales. En esta categoría se englobarían aquellos controles y procedimientos, tanto manuales como automáticos, cuyo objetivo es anticiparse a la ocurrencia de eventos, errores o irregularidades que puedan suponer la comisión de fraude. Ejemplos de estos controles son disponer de una adecuada segregación de funciones en la organización, contar con procedimientos de control de pagos, de evaluación de terceras partes, etc.

Mención especial merece la necesidad de considerar en nuestro análisis los riesgos relacionados con las tecnologías de la información y comunicación (TIC). Hoy en día no hay proceso, actividad o negocio que no tenga una fuerte dependencia de las TIC, consecuentemente aquellas organizaciones con un entorno de control insuficiente o inadecuado para prevenir ciberataques, estarán más expuesta a amenazas externas que pongan en peligro la correcta preservación de la información sensible (financiera o no), lo que puede resultar en significativas pérdidas financieras y reputacionales.

c) *Identificar las fortalezas y las debilidades*

Establecido el mapa de riesgos de fraude de la organización e identificados los controles que mitigan la probabilidad de ocurrencia e impacto de dichos riesgos, es preciso identificar las fortalezas y las debilidades de su entorno de control.

Los principales objetivos de esta fase son:

- *Evaluar la efectividad de los controles*. Tras valorar el riesgo inherente de los eventos de fraude identificados, el análisis debe ahora focalizarse en determinar cuál es el grado de efectividad de los controles existentes, y consecuentemente, cuál es el riesgo de fraude residual al que la organización está expuesta, es decir, cuál es el riesgo no cubierto por los controles implantados. Para ello, además de analizar los controles desde el punto de vista de su diseño, es preciso analizar su efectividad operativa mediante la realización de testeos sobre una muestra representativa de dichos controles.
- *Realizar un diagnóstico de la situación actual de la organización y elaborar un plan de acción con las recomendaciones de mejora*.

Una vez evaluada la exposición al riesgo neta, es decir, tras evaluar la efectividad de su marco de control, podemos conocer qué riesgos de fraude están insuficientemente cubiertos, y por lo tanto, es el momento de definir las recomendaciones de mejora necesarias para subsanar las deficiencias detectadas.

- *Presentar los resultados obtenidos*. Una vez completada la evaluación de riesgos es preciso presentar los resultados del trabajo realizado a la dirección de la organización, que deberá definir su estrategia de respuesta en relación con los riesgos no cubiertos o insuficientemente cubiertos.

En definitiva, llevar a cabo una evaluación de riesgos de fraude puede aportar numerosos beneficios a una organización:

- Ayuda a mejorar la concienciación respecto al fraude en la organización. En el transcurso de la evaluación de los riesgos de fraude deben participar muchos y muy diversos actores de la entidad, lo que permite reforzar el mensaje de que la organización se preocupa por el fraude. Asimismo, discutir abiertamente sobre fraude puede, además, disuadir a potenciales defraudadores de cometer irregularidades al sentir que la organización tiene una actitud vigilante, así como hacer más difícil la racionalización de la actitud deshonesta por parte del individuo.
- Permite identificar las actividades y las áreas en las que la organización es más vulnerable al fraude. Como consecuencia de esta identificación se podrán establecer planes para proactivamente monitorizar los riesgos en dichas áreas, ayudando a aumentar la sensación de control y, de este modo, disuadir a los potenciales defraudadores de que cometan, o continúen cometiendo, irregularidades.
- Permite identificar debilidades en el entorno de control de la organización y diseñar planes de actuación para mitigar los riesgos que no están cubiertos o que lo estén, pero de manera insuficiente.

5.2. Monitorización de controles

Un programa de prevención de fraude eficaz es aquel que previene la comisión de irregularidades, o que, cuando no pueda prevenirlas, sea capaz de detectarlas rápidamente, de subsanar las deficiencias y de reportarlas a los estamentos de la entidad que correspondan, a través de los canales formalmente establecidos a tal efecto.

Los últimos datos dados a conocer por ACFE indican que aquellas organizaciones que disponen de controles proactivos que permiten la monito-

rización y análisis de datos son capaces de reducir la pérdida media causada por el fraude en casi un 60%, y de disminuir el tiempo medio para desenmascarar el fraude en un 50%.

Es por tanto necesario que la organización cuente con un mecanismo formalmente establecido para asegurar la correcta monitorización de su programa antifraude de forma continua y a lo largo del tiempo. Este sistema de monitorización continua debe contemplar tanto los roles y responsabilidades de los distintos estamentos de la entidad en relación con este ámbito, como los procedimientos y controles específicos que permitan validar el efectivo funcionamiento de los controles mitigantes del riesgo de forma continua, sin olvidar que un sistema de monitorización eficaz también debe contemplar la necesidad de llevar a cabo auditorías periódicas realizadas por profesionales independientes.

La monitorización continua de controles permite a las organizaciones constatar el grado de efectividad de las medidas implantadas para prevenir y/o detectar la ocurrencia de fraude en su seno, lo que les permitirá comprender hacia dónde deben dirigirse las futuras actuaciones de mejora de su entorno de control.

Por su parte, la realización de auditorías antifraude de manera periódica por parte de expertos independientes, ayuda no solo a contrastar la efectividad de los controles implantados, sino que puede ayudar a identificar nuevos riesgos de fraude que, o bien no habían sido considerados inicialmente, o bien se habían descartado por considerarlos como remotos. Estas auditorías no deben centrarse únicamente en verificar si la organización dispone de procedimientos y controles para cubrir riesgos específicos, y si éstos están correctamente diseñados, sino que también debe focalizarse en testear transacciones concretas donde se presuma riesgo de fraude.

La automatización de los procesos, junto con la creciente disponibilidad de datos en soporte digital, permite a las organizaciones incorporar herramientas de análisis masivo de datos (*data analytics*) al proceso de monitorización de riesgos de fraude, tanto en el ámbito de la monitorización continua, como en el de las auditorías periódicas.

Las nuevas técnicas de *data analytics* permiten combinar la utilización de grandes volúmenes de datos y un extensivo análisis estadístico y cualitativo, con modelos explicativos y predictivos que facilitan la detección de errores y fraudes, así como la identificación de patrones de comportamiento anómalos. Ya no se trata de analizar muestras de datos, sino de analizar la población completa.

En definitiva, dotar el programa antifraude de las herramientas adecuadas que permitan su efectiva monitorización ayuda no solo a prevenir y detectar la ocurrencia de incidentes de fraude en la organización, evitando

o disminuyendo las pérdidas en las que pudiera incurrir, sino que también actúa como un potente mecanismo de disuasión, y ayuda a difundir el mensaje de que la prevención del fraude está en lo más alto de las agendas de los líderes de la organización.

6. Plan de respuesta ante hechos fraudulentos

El último elemento que debe incluir un programa antifraude es el elemento reactivo, el cual debe contener el proceso de evaluación y respuesta ante las sospechas de fraude, así como la investigación del caso y las acciones disciplinarias a adoptar.

Cuando se presenta una sospecha de fraude la respuesta inicial es crucial y los responsables deben responder de forma adecuada y oportuna. Para ello es básico que la organización haya desarrollado un protocolo de reacción que detalle cómo responder a este tipo de situaciones. Dado que cada fraude es distinto, este protocolo no debe definir todos los procedimientos a realizar, sino que simplemente debe utilizarse como guía para minimizar los riesgos y maximizar las posibilidades de éxito. Entre los elementos que deben detallarse en el protocolo de reacción se encuentran los siguientes:

a) **Protocolos de respuesta:** Una vez se tenga la sospecha de que se ha producido un fraude o una actividad irregular, estos protocolos aseguran que los individuos que deben conocer dicha situación la conozcan.
b) **Equipo de respuesta:** El plan de respuesta debe identificar el personal clave que deberá responder a un fraude en particular. Dicho personal variará en función del tipo de irregularidad y del tipo de organización funcional de la compañía.
c) **Factores que determinarán los próximos pasos:** En términos generales las sospechas de fraude deben conducir al inicio de una investigación, pero existen circunstancias que deben tenerse en cuenta con anterioridad. Por ejemplo la credibilidad, el impacto reputacional, la probabilidad de que el incidente haya ocurrido, preservar la prueba, privacidad de la información, si han existido casos similares en el pasado, etc.
d) **Protocolos de protección de la documentación relevante:** Estos protocolos son necesarios para evitar la potencial destrucción de documentos relevantes una vez se ha dado a conocer una sospecha de fraude. En este aspecto son muy relevantes los protocolos de mantenimiento y análisis de la información electrónica de la empresa (correo electrónico, chats, carpetas de red, copias de seguridad…).

e) **Principios de documentación del plan de respuesta:** La compañía deberá establecer unos principios para documentar o dejar constancia de toda la información analizada y que servirá para tomar una decisión en relación al caso concreto.
f) **Informe:** Con el objetivo de registrar los esfuerzos de la compañía, ésta deberá desarrollar informes para todas las sospechas de fraude identificadas, hayan sido o no investigadas.

Una vez definidos los elementos que debe contener un protocolo de reacción, a continuación describiremos otro de los aspectos esenciales de todo plan de respuesta, la investigación:

1) Conocimiento inicial del hecho fraudulento:
Las fuentes de información acerca de un fraude o una irregularidad pueden ser múltiples y variadas. A grandes rasgos dichas fuentes pueden diferenciarse entre internas (canal de denuncias, análisis de auditoría interna, revisiones de la dirección…) y externas (chivatazos, auditor externo, denuncias…).

2) Filtro y análisis de la información inicial recibida:
El primer aspecto que debemos considerar al tratar la información inicial recibida es su credibilidad. Para ello, la compañía deber recopilar toda la información posible relacionada con el caso y valorar su consistencia. Como norma general se puede aseverar que cuanto más detallada es dicha información más creíble será la alegación, sin embargo, es conveniente que quien tenga encargada la función de recibir esta información se asegure de que la misma es verosímil y, en el caso que no lo sea, documente los pasos seguidos para llegar a dicha conclusión.

3) Respuesta:
La respuesta es la fase más compleja y difícil de todas las que conforman los elementos reactivos de un programa antifraude. Una vez la información inicial ha sido contrastada deben iniciarse los pasos que permitan a la Dirección de la compañía tener toda la información necesaria para poder tomar la mejor decisión. A pesar de que cada investigación es única y singular, existen ciertos procedimientos comunes que debe comprender:
i. **Lanzamiento de la investigación:** Este procedimiento inicial consiste en la planificación de la investigación, que básicamente debe incluir la confección del equipo, el alcance y el plan de trabajo.

ii. **Preservación de la documentación:** El primer objetivo del equipo de investigación debe focalizarse en la identificación y recopilación de la información que podrá ser relevante para el caso. Esta información puede referirse a documentación física, digital, visual o sonora. En este punto es muy importante documentar la cadena de custodia de toda esta información y tener en cuenta las leyes sobre privacidad que sean de aplicación a la misma.

iii. **Revisión contable-forense:** Tal y como hemos comentado previamente, las compañías almacenan una gran cantidad de información que puede ser utilizada, no solo como un elemento preventivo o detectivo, sino también para desenmarañar la trama fraudulenta que ha sido identificada.

iv. **Entrevistas:** En el transcurso de una investigación las entrevistas son una parte crítica en el proceso de obtención de información. A nivel general es importante tener en cuenta los siguientes aspectos:
   - El orden de las entrevistas es importante. Es recomendable iniciar las entrevistas por personas que no estén directamente implicadas en el caso y acabar con los principales sospechosos y testigos.
   - Al afrontar una entrevista, el entrevistador debe haber revisado la documentación soporte del caso y tenerla preparada por si debe ser utilizada durante la entrevista.
   - Es importante prestar atención al lenguaje no verbal del entrevistado.
   - Es recomendable que una persona se encargue de tomar notas exhaustivas de toda la entrevista.

v. **Informe:** Al finalizar los procedimientos anteriores se emitirá un informe en el que se detallará el trabajo realizado, así como las conclusiones alcanzadas. Dichas conclusiones se basarán en hechos claramente identificables y todas las afirmaciones deberán incluir la documentación soporte correspondiente.

4) Remediación:

Cuando ocurre un caso de fraude es fundamental tomar las medidas necesarias para intentar que éste no vuelva suceder. Por tanto, en primer lugar es importante que en el transcurso de la investigación se identifiquen las áreas de control interno que han sido vulneradas con el objeto de mejorarlas y, en segundo lugar, se forme a los empleados con el objetivo de evitar que dichas acciones fraudulentas se repitan de nuevo. Dependiendo del caso será conveniente tomar medidas disciplinarias o legales contra el autor del fraude lo que comportará muy probablemente la participación de profesionales especializados (abogados externos, peritos, etc.).

De este modo, el plan de respuesta debe protocolarizar ciertos aspectos para asegurar que las denuncias y sospechas de fraude son atendidas por las personas adecuadas y de forma correcta y, además, constituye un aspecto imprescindible para mejorar los controles de la compañía y reducir el riesgo de que el fraude se vuelva a repetir en el futuro.

Referencias Bibliográficas

ACFE (2014) "Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Survey".

BIEGELMAN, M. y BARTROW, J. (2012) "Executive roadmap to fraud. Prevention and Internal Control", Wiley, Nueva York.

EURORAI (2012) "Buenas prácticas antifraude. Impulsar el papel de los auditores en la lucha contra el fraude". http://www.eurorai.org/eurorai/eurorai_es.nsf/documento/otros_informes/$file/Eurorai_Counter%20Fraud%20Good%20Practice%20-%20FINAL%20April%202012_ES.pdf.

KEVIN, L.J. (2003) "The Effects of Internal Audit Structure on Perceived Financial Statement Fraud Prevention", Accounting Horizons, vol. 17, núm. 4, pp. 315-327.

MARK, S. B. (1996) "An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud", The Accounting Review, *v*ol. 71, núm. 4, pp. 443-46.