El cambio del comportamiento humano y su rol en la prevención del fraude

Brenda Gabriela Ampuero Alfaro
Estudiante del décimo ciclo de Contabilidad de la Pontificia Universidad Católica del Perú. Coordinadora del área de NIIF de la Revista Lidera. Presidente de AECAFP en el 2013.

El fraude corporativo es un problema que podrían enfrentar todas las empresas en el mundo. Desde las más pequeñas hasta las más grandes, pueden tener algún estafador al interior de su organización, así como algún externo que solo busca obtener provecho. Pese a que esto es conocido, las empresas siguen negando que en su trabajo pudiera ocurrir un fraude. Para analizar este tema, se han desarrollado ideas sobre la base de la lectura Corporate Fraud: The Human Factor de Maryam Hussain (2014). En esta, se menciona que existen muchos motivos por los cuales las personas (ordinarias o extraordinarias) llegan a cometer dichos crímenes, como la avaricia o la necesidad. Además, como se ha mencionado, son las personas quienes lo realizan; y, por ello, el factor humano siempre va a ser una constante en los fraudes, tanto en el pasado como en el presente y en el futuro. En mi opinión, deben rescatarse las siguientes cinco ideas de la lectura, y ser tomadas en cuenta para cualquier empresa.

1. La efectividad de los controles no va a cubrir todos los riesgos; por ello, la cultura de la organización es vital.

Considero que es importante esta noción, debido a que, en muchas compañías, se tiene la creencia de que al tener manuales de control interno los riesgos de fraude son mitigados. Como sabemos, esto no es cierto, puesto que el fraude lo comete una persona que siempre va a buscar formas ingeniosas de burlar dichos controles. Además, como se mencionó previamente, no es remoto que el fraude suceda; y, más bien, es uno de los riesgos más comunes, que no solo podría involucrar pérdida de dinero. En algunos casos, podría perderse también propiedad intelectual. Por ello, las empresas deben buscar asesoramiento en fraudes para cubrir las amenazas y riesgos. En este marco, lo primero que realizan las empresas es reforzar sus controles internos. Estos serán efectivos si son alineados con los riesgos que puede enfrentar la empresa, y si cambian de acuerdo con las circunstancias.

A pesar de ello, los grandes riesgos vienen del comportamiento y las intenciones de los gerentes y ejecutivos que luchan con presiones externas e internas. Si ni la estructura del negocio ni el ambiente laboral son adecuados, no habrá impacto de los controles mencionados. Por este motivo, la cultura organizacional –que depende de las decisiones y comportamientos de los empleados, principalmente, de los dueños como modelos a seguir– debe brindar un mensaje uniforme. Esto significa que los valores de la empresa serán los

mismos valores que posean los empleados. Lamentablemente, en muchas empresas, sucede que la Alta Gerencia envía mensajes que confunden a los empleados, en la medida que incentiva malas prácticas.

En ese contexto, para brindar el factor humano dentro de la cultura organizacional, se debe difundir entre los empleados lo noción de que todos tienen un rol importante para combatir el fraude, desde la Junta de Directores hasta los empleados en general. La confianza es un elemento clave dentro de la cultura que la compañía debe inculcar; y, en paralelo, también debe establecer sanciones cuando abusan de ella. De este modo, el ambiente que se crea es de libre expresión, transparencia, cumplimiento y apoyo mutuo para detección de fraudes.

2. Estafadores extraordinarios han realizado fraudes extraordinarios.

Como se conoce, los líderes del caso Enron y Worldcom estuvieron involucrados en el colapso de dichas entidades. Esta idea es importante, porque para que en una empresa haya fraudes a tan gran escala requiere personas que tengan conocimiento de la mayor información de la compañía.

> **"El factor humano siempre va a ser una constante en los fraudes."**

Estas personas han planeado al detalle el fraude que cometerán, lo cual es posible en la medida que conocen los vacíos del control interno de la compañía y las formas para burlar los sistemas. Esto lo han obtenido gracias a los años que mantienen al interior de la empresa. Además, han racionalizado su causa. Es decir, ellos consideran que, debido a que todo lo realizan por la empresa, se merecen más y es por ello que llevan a cabo los fraudes. Por último, se debe considerar que estas personas ocupan altos rangos dentro de la compañía, lo cual les da mayor acceso a información más privilegiada y posibles malos manejos.

Por esta razón, considero que las empresas deberían adoptar políticas para que las personas que ocupan altos rangos roten en cortos períodos de tiempo. Asimismo, el conocimiento de la organización puede ser transmitido a nuevas mentes y personas. De esta manera, no se da el tiempo para crear tales planes tan organizados que puedan llevar al fin de la compañía.

3. Todo fraude va a dañar la reputación de la empresa, pero una detección temprana va a ahorrar dinero y no se tendrá daños irreparables.

Esta idea es relevante, pues –como se sabe– los fraudes que se encontraron en varias empresas son historias que se conocen alrededor del mundo. De este modo, la reputación de la compañía se verá afectada, lo cual aumentará mientras más grande sea el impacto. Este último es aun mayor, ahora que las personas tenemos la información en tiempo real a nuestra disposición.

Ante este escenario, las empresas deben buscar que el Exposure Gap (espacio de tiempo desde el inicio del fraude hasta su detección) sea mínimo. Una de las alternativas que se menciona en la lectura –y que llamó mi atención– es la creación de líneas anónimas para denunciar fraudes. Esta debe ser flexible y asegurar el anonimato del denunciante y su protección (no despedir arbitrariamente por su buena fe); de igual modo, debe permitir que se brinde información no tan general y detallada (nombre del sospechoso, lugar, fecha, acciones). Lamentablemente, existen reportes maliciosos, los cuales no ayudan a la empresa sino más bien retrasan investigaciones que sí serían reales.

Otro elemento para una detección temprana sería la realización de auditorías internas sorpresa, a partir de las cuales se restringe el espacio para que el estafador pueda esconder sus planes, puesto que en cualquier momento se puede cuestionar informaciones no tan grandes pero importantes. Por último, se puede tener sistemas de análisis de inteligencia, que buscan datos más avanzados y buscan huellas de información que se pudo dejar en el camino. En este marco, las computadoras sirven como detectives ante las nuevas tecnologías, que pueden surgir como herramientas de los nuevos fraudes. A partir de ello, la información es analizada y se detectará algún movimiento sospechoso.

Todos estos esfuerzos se realizan de modo que la empresa pueda detectar el fraude y definir qué acciones realizar a nivel interno, sin necesidad de que personas externas puedan conocer este hecho y se tengan mayores pérdidas. Para ello, la empresa también debería mostrar una política de tolerancia cero ante cualquier fraude.

4. Recuperar lo robado es lo que buscan todas las compañías.

Este punto es importante, porque lo que le interesa a la mayoría de empresas es poder recuperar el dinero perdido,

la propiedad intelectual extraída, entre otros, pero no siempre se conocen las medidas adecuadas. Como se menciona en el texto, pueden recuperarse los activos; y, además, se podría lograr una posible sentencia. No obstante, el mundo es tan grande para esconder lo robado que, probablemente, una sentencia a los culpables es lo que casi nadie debería esperar. Se debe considerar que las autoridades no siempre van a tener los recursos para buscar lo robado. Además, el proceso es caro y no siempre se asegura que se logre encontrar los activos extraídos. En el mejor de los casos, se logra encontrar al sospechoso, pero no se obtiene el dinero perdido.

"No se puede dar por sentado el ingenio de las personas."

En ese sentido, considero que los remedios civiles son la mejor opción que una empresa podría tener. A partir de ello, se recupera lo financiero, que –como se menciona dentro de la idea– es lo que principalmente buscan las compañías. Esta opción no exige gran cantidad de evidencia; y un juez podría dictaminar la congelación de activos para, luego de una investigación, conocer el verdadero dueño de los activos.

La investigación sí podría ser infructuosa, pero actualmente siempre existe un modo de encontrar información, desde anécdotas de los empleados –como evidencia– hasta información en redes sociales. Ello es posible siempre y cuando se tenga un equipo de investigación y un equipo legal (puesto que podría estar en cualquier parte del mundo) para definir la mejor estrategia de búsqueda. Al final, el estafador no tiene una sentencia que implique más que devolver lo robado. Se debe agregar que, si se quiere jugar doble y al conocer al estafador querer apresarlo, se podría poner en riesgo la posible recuperación de lo que ya se había perdido.

5. El cyberfraud conlleva a robo y engaño.

Actualmente, todos hemos experimentado la revolución de las nuevas tecnologías. Por ello, no es de extrañar que los estafadores se valgan de estas herramientas para realizar nuevos fraudes. A esto se le suma la ingeniería social, mediante la cual se convence a las personas de divulgar información que normalmente no se difundiría. Esto es importante, porque considero que la mayoría de las empresas no está preparada para combatir los crímenes cibernéticos.

Las amenazas pueden ser internas como externas. Esta última representa una mayor amenaza, pues con un solo clic por parte de alguien de la compañía se pueden robar millones, y ocultarlos a través de miles de pequeñas transacciones. Además, con el uso de los spyware o malaware, los estafadores tendrían un acceso más fácil a información privilegiada, y simplemente destruir toda información.

Considero que esta es actualmente la mayor amenaza, porque no existen reportes de cyberfraud y tampoco se puede medir su impacto. Además, no existen parámetros jurisdiccionales, porque el estafador podría estar en cualquier parte. Esto representa un reto para las empresas, que deben estar preparadas para las nuevas tecnologías y crear mecanismos para evitar este tipo de fraudes.

Para finalizar, se debe señalar que Corporate Fraud: The Human Factor es una lectura muy enriquecedora, y brinda nuevas perspectivas de lo que representa el fraude. Este tema va más allá de los escándalos que conocemos de las grandes empresas. En esa medida, todos tenemos que estar alertas ante cualquier fraude y asegurarnos de que las compañías tengan en cuenta que podrían tener un estafador interno o tal vez alguien que quisiera robar información. Por último, no se puede dar por sentado el ingenio de las personas, pues la mente humana siempre busca formas de lograr sus objetivos; así, solo otras personas con ayuda de herramientas son capaces de combatir el fraude.

Bibliografía

Hussain, Maryam (2014). Corporate Fraud: The Human Factor. Londres: Bloomsbury Information Ltd.