Traducción al Español Auspiciada por:

FLAI
Fundación Latinoamericana
de **Auditores Internos**

PERSPECTIVAS Y PERCEPCIONES GLOBALES

FRAUDE

PARTE I: Fraude en la criptoesfera

PARTE 2: Auditores internos y examinadores de fraudes: Una asociación valiosa

PARTE 3: La resaca: El fraude en la era post-COVID

The Institute of
Internal Auditors

Contenido

Parte 1

Fraude en la Criptosfera

Sobre los Expertos

Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Dana Lawrence es la Directora de Cumplimiento Normativo de Fideseo. Es una experta reconocida y líder en cumplimiento complejo, gestión de riesgos empresariales (ERM), auditoría interna y creación, ampliación y corrección de programas de gobernanza. La carrera de Lawrence en tecnología y servicios financieros abarca hipotecas, banca comunitaria, grandes bancos estadounidenses y mundiales, socios de banca abierta, fintech y cripto. Ha desempeñado funciones de liderazgo senior, trabajando directamente con reguladores bancarios y auditores internos y externos. Lawrence es una popular oradora pública y anfitriona de eventos, hablando en eventos locales, nacionales y mundiales con hasta 40.000 participantes. Es una voluntaria comprometida y una líder de opinión, al servicio de diversos grupos como el IIA.

Lourdes Miranda, CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

Lourdes Miranda es la Directora de Cumplimiento de SendCrypto, una empresa de tecnología blockchain. Es una antigua agente de la CIA y analista del FBI con más de 20 años de experiencia gubernamental y corporativa, especializada en investigaciones de delitos financieros y recopilación y análisis de inteligencia a nivel mundial. Cuenta con una amplia experiencia sobre el terreno en la persecución de blanqueadores de dinero y financiadores del terrorismo. Desde 2017, Miranda ha estado trabajando para FinTechs como investigadora sénior de cripto, oficial sénior de cumplimiento y gerente de riesgos, creando equipos de cumplimiento, investigación, cripto e inteligencia y programas de capacitación. También es autora, instructora y colaboradora de múltiples cursos en línea como experta en la materia. Además, Miranda es miembro del Consejo Asesor de Toronto Compliance & AML Enterprise (TCAE), con sede en Canadá.

Introducción

Cripto y fraude en la conversación global

Sam Bankman-Fried, el carismático fundador de la bolsa de criptomonedas FTX, llegó a tener un valor estimado de 26.500 millones de dólares. Como líder de la que fue en su momento la tercera bolsa más grande del mercado de criptomonedas, Bankman-Fried y FTX eran los favoritos de una serie de inversores de alto perfil, como BlackRock y el jugador de la NFL Tom Brady. Sin embargo, perdió todo su patrimonio prácticamente de la noche a la mañana en una de las quiebras empresariales más dramáticas de la historia moderna.

Bankman-Fried fue detenido el 13 de diciembre de 2022 en las Bahamas. Según informes publicados, se enfrenta a varios cargos, entre ellos fraude electrónico, conspiración de fraude electrónico, fraude de valores, conspiración de fraude de valores y blanqueo de dinero.

Aunque el mero espectáculo de una caída tan increíble tiene un interés humano, el suceso también ha planteado cuestiones de mayor calado en relación con los activos digitales. Con paralelismos con escándalos como los de Tornado Cash y Bitzlato, el colapso de FTX y el posterior impacto en la industria que representaba ha llevado a muchos a cuestionar la viabilidad a largo plazo de los criptoactivos, al menos en su estado actual, que el presidente de la Comisión de Bolsa y Valores de Estados Unidos, Gary Gensler, calificó de "Salvaje Oeste".

A pesar de que se basan en la tecnología blockchain, que es una de las formas más seguras de mantener los criptoactivos y la información, si la cabeza muy visible de uno de los intercambios de criptodivisas más prominentes del mundo puede presuntamente cometer actos de fraude a gran escala, ¿qué otras vulnerabilidades pueden existir para las empresas que operan en la industria en alguna capacidad? ¿Cómo ha cambiado el panorama de riesgos con el meteórico ascenso de los criptoactivos, y cómo están respondiendo con éxito a estos cambios algunas organizaciones y sus funciones de auditoría interna?

La Parte 1 de esta serie de tres partes sobre el fraude abordará estas preguntas mediante el examen de los esquemas de fraude comunes que se ven en las primeras etapas de un mundo de criptoactivos. Para obtener más información sobre este tema, el IIA ofrecerá una repetición de su reciente seminario web "Perspectivas de fraude: Blockchain, Crypto, y KYC", junto con una sesión de preguntas y respuestas en directo con los expertos en la materia citados en este informe.

Incertidumbre en la Criptoesfera

Un futuro apasionante, pero arriesgado

Las organizaciones están prestando atención

Aunque sus implicaciones son enormes y nada menos que revolucionarias, la tecnología blockchain es relativamente fácil de entender conceptualmente, ya que no es más que un registro continuo y creciente de transacciones de activos digitales que puede compartirse y almacenarse en prácticamente cualquier estructura de red. Lo que la diferencia es que utiliza metodologías de verificación que cifran continuamente el bloque con cada nueva transacción, lo que la hace más segura.

"La tecnología en sí es extremadamente complicada y se necesitan años de formación y educación para analizarla, pero yo pienso en la propia blockchain como en un estado financiero", afirma Lourdes Miranda, directora de cumplimiento de SendCrypto, una empresa de tecnología blockchain. "La blockchain tiene información relativa a quién envió los activos, dónde se depositaron, si hubo alguna retirada y el saldo resultante".

Podría decirse que la criptomoneda es el activo más conocido que utiliza esta tecnología, que crea un sistema (o sistemas) monetario descentralizado y de código abierto inmune a la influencia de entidades, como los bancos centrales - pero otros ejemplos de criptoactivos basados en blockchain incluyen tokens no fungibles (NFT), tecnologías de libro mayor distribuido (DLT), tokens de juegos, entre otros.

Sin embargo, como las industrias están aprendiendo rápidamente, el hecho de que los criptoactivos se basen en una tecnología segura prácticamente imposible de manipular por métodos tradicionales no significa que sus adoptantes sean inmunes al riesgo. El colapso de FTX ilustra esto en más de un sentido. Por ejemplo, ilustró lo perjudicial que puede ser la falta de un gobierno corporativo y unos controles internos adecuados, no sólo para la organización, sino para los inversores de todo el sector.

Este fue un punto que el presidente y CEO de IIA, Anthony Pugliese, hizo en una carta reciente al Congreso de los Estados Unidos en la que pedía que establecieran nuevos requisitos para reforzar el gobierno corporativo en los intercambios de criptomonedas, las empresas de tecnología blockchain, los mercados NFT y las plataformas Web3 que operan en los Estados Unidos. "Innumerables inversores están pagando ahora el precio de los fracasos de FTX", dijo Pugliese. "Está claro que no podemos confiar en que las bolsas de criptomonedas no reguladas hagan lo correcto por su cuenta: necesitamos ordenar normas de gobierno corporativo más estrictas y garantizar la rendición de cuentas cuando estas bolsas no estén protegiendo a sus clientes. Cuando los malos actores corporativos fracasan, no deberían ser los inversores los que se queden con la bolsa.

Pugliese subrayó que el colapso de FTX y sus consecuencias para el mercado podrían haberse mitigado con la actuación de una sólida función de auditoría interna. "El colapso de FTX es el último recordatorio de que las organizaciones que carecen de una sólida función de auditoría interna están, en el mejor de los casos, jugando con fuego y, en el peor, exponiéndose a sí mismas y a sus accionistas a una caída desastrosa y totalmente evitable", afirmó.

Estas preocupaciones de Pugliese y otros no cayeron en saco roto. El 3 de enero de 2023, la Reserva Federal, la Corporación Federal de Seguros de Depósitos (FDIC) y la Oficina del Contralor de la Moneda (OCC) publicaron su primera declaración conjunta sobre la criptomoneda. En ella, destacaron una variedad de riesgos que podrían estar en juego para las organizaciones bancarias que operan en criptodivisa de alguna forma, incluyendo:

- Riesgo de fraude y estafas entre los participantes en el sector de los criptoactivos.
- Incertidumbres jurídicas relacionadas con las prácticas de custodia, los reembolsos y los derechos de propiedad.
- Declaraciones y divulgaciones inexactas o engañosas por parte de las empresas de criptoactivos.
- Volatilidad significativa en los mercados de criptoactivos, cuyos efectos incluyen impactos potenciales en los flujos de depósitos asociados a las empresas de criptoactivos.
- Riesgo de contagio dentro del sector de cripto-activos resultante de las interconexiones entre ciertos participantes de cripto-activos, incluso a través de acuerdos opacos de préstamos, inversiones, financiación, servicios y operaciones.
- Prácticas de gestión de riesgos y gobernanza en el sector de los criptoactivos que muestran una falta de madurez y solidez.
- Mayores riesgos asociados con redes abiertas, públicas y/o descentralizadas, o sistemas similares.

Si bien todos estos riesgos son dignos de discusión (y en muchos casos aplicables a organizaciones más allá de los bancos que incursionan en cripto), este informe se limitará a los actos de fraude cometidos contra los criptoparticipantes y las formas prominentes que adoptan en el entorno actual.

Un panorama propicio al fraude

Un panorama de riesgos en constante expansión

Una nueva herramienta en la caja de herramientas del malhechor

Aunque los criptoactivos presentan una letanía de características ventajosas, como la transparencia y un cifrado extraordinariamente avanzado contra la manipulación, estas mismas características han convertido a estos activos (y a la tecnología blockchain que los sustenta) en una poderosa herramienta para quienes buscan cometer fraude.

De hecho, es este atractivo para los malos actores lo que ha llamado la atención de los reguladores y las fuerzas de seguridad. "La única razón por la que los habituales se preocupan por los criptoactivos es porque los malos actores los están utilizando para financiar operaciones y blanquear dinero", dijo Miranda, que investigó delitos financieros para la CIA y el FBI durante casi 30 años. "Blockchain es muy difícil de manipular, pero se puede utilizar de maneras que promuevan actividades nefastas".

Un método, por ejemplo, es el uso de identidades de identificación falsas dentro de la blockchain. "Esto es enorme en la criptoesfera", dijo Miranda. "Los malos actores usarán identidades legítimas y válidas compradas en el mercado negro para pasar el proceso de incorporación KYC [Know Your Customer] cuando abren billeteras. Estas identidades no tienen antecedentes penales ni figuran en ninguna lista negra: están completamente limpias. Entonces, bajo este nombre limpio, pueden mover dinero en gran medida sin ser detectados hasta que los investigadores puedan ver con sus propios ojos las tendencias de fraude reveladoras."

La industria de los criptoactivos también ha introducido una serie de herramientas que, si bien están diseñadas para la comodidad del consumidor, tienen una serie de lagunas que pueden ser explotadas. Un iniciador de fraude, por ejemplo, puede hacer uso de un centro de transacciones de criptomonedas, como un cajero automático de Bitcoin, junto con un teléfono desechable para evitar las llamadas de las fuerzas de seguridad.

"Digamos que estoy en Nueva York y quiero mover dinero en finanzas, y tengo que pagar a mis malos actores en Miami. Quieren cobrar y cobrar rápido. No voy a recibir un cheque, y no puedo usar un ordenador o portátil, porque la dirección IP hace ping, así que lo que hago es ir a un cajero automático Bitcoin en Nueva York y usar dinero en efectivo y un teléfono desechable. Así puedo pagar a la gente eludiendo los protocolos contra el blanqueo de capitales. Eso es fraude", afirma Miranda.

La estafa de romance (Pig Butchering)

Otra táctica de fraude común que pueden utilizar los malos actores se conoce con el término gráfico de "pig butchering" o estafa de romance. "Se trata básicamente del concepto de que un estafador 'engorda' metafóricamente a su víctima invirtiendo mucho tiempo con ella para establecer la confianza", explica Dana Lawrence, directora de cumplimiento normativo de la consultora empresarial y tecnológica Fideseo. Según Lawrence, el tiempo invertido por los estafadores puede ocurrir en cualquier parte, pero lo más habitual es que se produzca en las redes sociales o mediante mensajes de texto a lo largo de semanas o meses. Lawrence citó específicamente LinkedIn como plataforma favorita, así como sitios sociales como Twitter.

En estos casos, el malhechor suele presentarse como una persona influyente o con información privilegiada que ha invertido con éxito en criptomoneda. Con el tiempo, promocionarán los beneficios de la criptomoneda en un esfuerzo por conseguir que la víctima les transfiera sus activos. En algunos casos, los estafadores incluso han proporcionado a la víctima estados financieros falsificados para que parezca que se están obteniendo beneficios sustanciales.

Aunque es fácil leer estas señales y resulta bastante obvio detectarlas, en este caso los estafadores se han vuelto muy sofisticados. Los equipos de estafadores radicados en países como Camboya y China, por ejemplo, han recibido una profunda formación por parte de psicólogos sobre cómo hacer que las personas más vulnerables tomen decisiones poco acertadas.

"Han sido entrenados por psicólogos para tratar de averiguar la mejor manera de manipular a la gente", dijo el fiscal de distrito del condado de Santa Clara, California, Jeff Rosen, en una entrevista con la CNN. "Estás tratando con personas que van a utilizar diferentes técnicas psicológicas para hacerte vulnerable y conseguir que te interese desprenderte de tu dinero".[1]

Infla y Vende (Pump and dump)

La otra gran forma de fraude que se observa en la criptoesfera es bien conocida por los observadores veteranos del mercado bursátil: el denominado esquema de " Infla y vende- Pump and dump".

"Este esquema suele comenzar con un grupo que se reúne para iniciar un nuevo proyecto de criptomoneda, como un token, y luego utiliza - por lo general con la ayuda de personas influyentes - recursos para darle bombo en plataformas como Twitter o Discord", dijo Lawrence. "Actualmente hay mucha fluctuación en el mercado de criptomonedas debido a la liquidez. Si mucha gente intenta comprar algo a la vez, el mercado sufre una especie de sacudida y sube el precio. Si esto ocurre, los malos actores en cuestión que poseen grandes cantidades del activo lo venden de repente para obtener un beneficio, haciendo caer el precio de repente y dejando a todos los demás inversores con algo que vale esencialmente cero".

La bandera roja en estas situaciones, dijo Lawrence, es una clara falta de información que indique a los inversores potenciales que perderlo todo es una posibilidad clara. Los estafadores también suelen utilizar mensajes copiados y pegados en redes sociales y foros de debate escritos por personas con nombres de usuario similares. Y, una vez finalizada la estafa, estos nombres de usuario suelen desaparecer, con su anonimato completamente intacto.

Otros ejemplos de fraude en el contexto de los criptoactivos

El fraude basado en criptomonedas no siempre tiene que ser tan sofisticado. En las organizaciones basadas en criptomonedas, a menudo todo lo que necesita un mal actor es la oportunidad adecuada. Por ejemplo, mientras que la propia cadena de bloques mantendrá seguros los activos digitales, todo lo que se necesita para eludir la seguridad y vaciar una cartera de criptomonedas es obtener una clave privada, una larga cadena de números que podría caber en una servilleta de restaurante y dejarse en cualquier lugar para que cualquiera la encuentre.

"Tu clave privada es tu identidad digital en el mercado de las criptomonedas, y cualquiera que se haga con ella puede realizar transacciones fraudulentas o robar tus criptomonedas", explica Lawrence. "Si alguien de alguna manera consigue acceder a eso, y se llevó todo mi Bitcoin, no hay nada que pueda hacer al respecto. No puedo recuperarlo, no puedo presentar una queja, no hay ninguna agencia de protección al consumidor o regulador con el que disputarlo - literalmente ha desaparecido."

A medida que el mercado de las criptomonedas madura, han surgido servicios de cripto seguridad especializados en proteger las claves individuales y de empresa contra el extravío, pero en algunos casos sus metodologías son sorprendentemente primitivas. Según Lawrence, la solución que emplean algunos de estos servicios es almacenar las claves en cámaras acorazadas en la ladera de montañas desoladas. El cripto-seguro también existe como red de seguridad para las empresas que pueden permitírselo, pero en este momento todo el sector está luchando con la rentabilidad, lo que obliga a las aseguradoras a ser increíblemente selectivas a la vez que ofrecen una cobertura que se ha ido reduciendo año tras año.

En un artículo publicado en el Insurance Times del Reino Unido, James Wickes, socio del grupo RPC Insurance, analizaba los retos del mercado de los cripto seguros. "El número relativamente pequeño de aseguradoras activas actualmente en el espacio de los seguros de criptoactivos probablemente esté dispuesto a revisar la letra pequeña de las pólizas para limitar la exposición potencial a la

1. Josh Campbell, "Beware the 'Pig Butchering' Crypto Scam Sweeping Across America," December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.

volatilidad de los mercados de criptoactivos, como ha demostrado la reciente caída", dijo. "El mercado de seguros para estos activos está en su infancia y queda por ver si un cuerpo suficiente de aseguradoras estará preparado para proporcionar suficiente capacidad para satisfacer la demanda y cuán valiente será el mercado para ampliar la cobertura más allá del riesgo de robo tradicional."[2]

Sin embargo, a pesar de estas precauciones, sigue habiendo ciertas herramientas que los malos actores pueden utilizar para seguir utilizando los criptoactivos y la cadena de bloques sin saltarse directamente una cuenta establecida: los mezcladores, también conocidos como tumblers. Una de las características principales de una cadena de bloques es su transparencia; en cualquier explorador de cadena de bloques, cualquiera puede ver el registro de todas las transacciones de la cadena de bloques desde el lanzamiento de la criptomoneda en 2009. Los mezcladores permiten al usuario mezclar esencialmente la cantidad de criptoactivos en cuestión antes de entregarlos a los destinatarios previstos, dándoles un grado de anonimato ya que es muy difícil descifrar exactamente quién envió cuántos activos a quién. Usando un mezclador, todo lo que un explorador mostrará es que una persona, así como docenas de otras personas, enviaron activos a un mezclador, y luego enviaron los activos en cantidades variadas a una variedad de otras personas. El resultado, en esencia, se asemeja a una forma perfeccionada de blanqueo de capitales.

Frente a estas realidades, las organizaciones que optan por existir en la criptoesfera deben aceptar que están en gran medida por su cuenta cuando se trata de la mitigación de riesgos en esta etapa. Esto no significa que deba evitarse el cripto, pero sí que el cumplimiento, el control interno sólido, los esfuerzos de detección y disuasión del fraude y la auditoría interna deben desempeñar un papel destacado en las conversaciones sobre cripto desde el nivel de la junta directiva hacia abajo.

2. Isobel Rafferty, “Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments,” Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

Por donde puede empezar la auditoría interna

La normativa está aquí y vendrán más

Recursos de orientación publicados

Como se ha mencionado anteriormente, los marcos normativos a los que pueden recurrir las empresas para gestionar la seguridad y la gobernanza en relación con los criptoactivos y los riesgos de fraude asociados son escasos. Sin embargo, ciertas industrias como los servicios financieros no están totalmente desprovistas de recursos que aborden los principios de gobernanza adecuados en relación con la protección de los activos digitales, muchos de los cuales son aplicables a la criptomoneda.

En octubre de 2022, la Unión Europea presentó el texto acordado del Reglamento sobre Mercados de Criptoactivos (MiCA), que constituye uno de los primeros intentos a escala mundial de regulación exhaustiva de la comercialización de criptodivisas, aunque la legislación se ha presentado hasta abril de 2023 para traducirla a 24 idiomas diferentes. En caso de que se adopte formalmente, el reglamento:

- Define oficialmente el criptoactivo como "una representación digital de valor o derechos que pueden transferirse y almacenarse electrónicamente, utilizando tecnología de libro mayor distribuido o tecnología similar". Además, ofrece cuatro categorías diferentes de criptoactivos: tokens referenciados a activos, tokens de dinero electrónico, tokens de utilidad, y una cuarta categoría para criptoactivos que no entran en las otras tres categorías.
- Hacer oficialmente responsables a los proveedores de criptoactivos si pierden los criptoactivos de los inversores.
- Exigir a los actores de los mercados de criptoactivos que declaren información sobre su huella medioambiental y climática.
- Se solapará con la legislación actualizada en materia de lucha contra el blanqueo de capitales, y encargará a la Autoridad Bancaria Europea (ABE) el mantenimiento de un registro público de proveedores de servicios de criptoactivos que incumplan la normativa.
- Exigirá a los proveedores de criptoactivos autorización para operar en la UE.
- Proporcionará un marco sólido aplicable a las "stablecoins" (criptomoneda vinculada a un activo de referencia externo), que exigirá que el emisor ofrezca gratuitamente a todo titular de una stablecoin la posibilidad de reclamarla en cualquier momento.[3]

En EE.UU., una declaración conjunta de la Reserva Federal, la Corporación Federal de Seguros de Depósitos (FDIC) y la Oficina del Contralor de la Moneda (OCC) ofrece algunos recursos para las empresas estadounidenses que proporcionan orientación diseñada para ayudar a "las organizaciones bancarias a participar en discusiones de supervisión sólidas sobre las actividades propuestas y existentes relacionadas con los criptoactivos".[4]

- OCC Interpretive Letter 1179 "Chief Counsel's Interpretation Clarifying: (1) Autoridad de un Banco para Participar en Ciertas Actividades de Criptodivisas; y (2) Autoridad de la OCC para Constituir un Banco Fiduciario Nacional."
- Federal Reserve SR 22-6/ CA 22-6: "Participación en actividades relacionadas con criptoactivos por parte de organizaciones bancarias supervisadas por la Reserva Federal".

3. General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

4. "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

- FDIC FIL-16-2022 “Notificación y procedimientos de retroalimentación de supervisión para las instituciones supervisadas por la FDIC que participan en actividades relacionadas con criptomonedas.”

Estos no son los únicos recursos disponibles. Tras el colapso de FTX, la SEC también publicó unas directrices que aconsejaban a las empresas revelar su participación en empresas de materias primas digitales.

El valor de la educación

Suponiendo que se adopte, la legislación propuesta por la UE entraría en vigor en 2024, pero es casi seguro que no será la última. A medida que el panorama normativo se llena de parches mes a mes, la medida más valiosa que puede tomar un auditor interno es hacer todo lo posible por mantenerse al corriente de los cambios y articular claramente esos cambios al consejo de administración y a las partes interesadas aplicables.

En el entorno actual, los auditores internos también deben explicar a las partes interesadas qué otras regulaciones existen que puedan ser aplicables a sus esfuerzos criptográficos. Por ejemplo, dijo Lawrence, una empresa que ofrece su propia criptodivisa puede requerir el registro en la Red de Aplicación de Delitos Financieros de EE.UU., un detalle crítico que podría pasarse por alto fácilmente porque la criptodivisa no se cita específicamente en la legislación. "Ahora hay mucha incertidumbre", dijo. "Corresponde a los auditores internos informar a los líderes sobre lo que es aplicable y lo que no".

Centrarse en las nuevas tecnologías tampoco debe distraer a las empresas de las mejores prácticas básicas en materia de protección de activos digitales, incluido el uso de una red privada virtual (VPN) y la seguridad, recopilación y, cuando sea necesario, eliminación adecuadas de la información de los perfiles de usuario, especialmente de los consumidores. "Los perfiles de usuario son un control organizativo fundamental", afirma Miranda. "Si yo estuviera auditando una empresa, comprobaría que los perfiles de usuario coinciden con la actividad transaccional. Por ejemplo, la información geográfica es increíblemente importante para el cumplimiento de la normativa y las investigaciones. Las organizaciones necesitan mantener esta información segura, así como saber dónde reside." Sobre este punto, Miranda señaló que las organizaciones a menudo pasan por alto los acuerdos de confidencialidad (NDA), que contienen información crítica sobre los perfiles, como direcciones físicas que pueden ser fundamentales para una investigación de fraude.

Para más información, la guía complementaria del IIA “Internal Audit and Fraud: Assessing Fraud Risk Governance” (Auditoría interna y fraude: evaluación de la gobernanza del riesgo de fraude) ofrece orientaciones claras sobre las funciones y responsabilidades organizativas para una gobernanza y una gestión sólidas del riesgo de fraude, así como recomendaciones sobre orientaciones adicionales, como la Guía de gestión del riesgo de fraude de COSO.

Conclusión

La auditoría está preparada

La criptomoneda y la tecnología en la que se basa son demasiado revolucionarias como para que la auditoría interna las ignore, con intereses que merecen sobradamente la atención de la junta directiva. Las evaluaciones de riesgos que la ignoran tienen un punto ciego crítico. La criptomoneda puede ser un concepto relativamente nuevo para muchos, pero no disminuye el valor de un marco sólido de gestión del riesgo de fraude que pueda ser medido y probado por la auditoría interna.

Aunque es fácil lamentarse de que haya que añadir otra área de riesgo al radar cada vez mayor de la auditoría interna, la buena noticia es que ningún otro departamento de la organización está mejor posicionado para abordarla. Al igual que hizo la La Ley Sarbanes-Oxley (SOX)Ley Sarbanes-Oxley (SOX) en 2002, la evolución de la regulación de la criptomoneda prácticamente asegura a la auditoría interna una valiosa posición en la mesa en los próximos años. Aunque la función todavía no conozca las criptomonedas, sí conoce el fraude y conoce el riesgo; eso por sí solo es suficiente para que la auditoría interna adopte una posición de liderazgo a la hora de abordar los retos que se avecinan.

Parte 2

Auditores internos y examinadores de fraudes: Una asociación valiosa

Sobre los Expertos

Mason Wilder, CFE

Mason Wilder es Examinador de Fraudes Certificado y director de investigación de la ACFE. En este puesto, supervisa la creación y actualización de los materiales de la ACFE para la formación profesional continua, colabora en la planificación y producción de todos los actos de formación de la ACFE, trabaja en iniciativas de investigación como el Informe a las Naciones e informes de evaluación comparativa, imparte formación, escribe para las publicaciones de la ACFE y responde a las peticiones de los miembros y los medios de comunicación. Antes de incorporarse a la ACFE, Wilder trabajó durante más de una década en investigaciones e inteligencia de seguridad corporativa, especializándose en investigaciones de antecedentes y diligencia debida y análisis de inteligencia para seguridad física internacional y respuesta a crisis. Mason ha forjado su carrera recopilando información relevante de todas las fuentes para analizarla y destilarla en apoyo de la toma de decisiones críticas, y le apasiona ayudar a los profesionales de la lucha contra el fraude a mejorar continuamente sus capacidades para combatir el fraude con eficacia.

Shawna Flanders, CRISC, CISA, CISM, SSGB, SSBB

Shawna Flanders, directora de desarrollo de productos del Instituto de Auditores Internos (IIA), es una apasionada tecnóloga y profesional del sector de la formación técnica a la que le apasiona adaptar las conversaciones técnicas al lenguaje empresarial común. Shawna aporta una combinación complementaria única de habilidades a cada compromiso, incluyendo: Desarrollo/contribución de contenidos para SME, oratoria/formación, riesgos relacionados con IT, auditoría de IT, información y ciberseguridad, cumplimiento de IT, gobernanza de IT, gestión de proveedores, generalista de IT en telecomunicaciones, programación, diseño/revisión de arquitectura relacionada con voz y datos, ingeniería, gestión de análisis e integración, gestión de procesos empresariales, análisis empresarial, gestión de proyectos, gestión de programas y mejora de procesos/Six Sigma.

Introducción

Los auditores internos aportan perspectivas constructivas sobre la gobernanza, los riesgos y los controles internos que ayudan a las organizaciones a gestionar los riesgos, incluida la identificación y mitigación del fraude. Sin embargo, aunque la auditoría interna es una parte eficaz de la detección y disuasión del fraude, encontrar el fraude no es el trabajo del auditor interno. En cambio, un Examinador de Fraudes Certificado (CFE) se encarga específicamente de identificar e investigar el fraude. El CFE aporta conocimientos especializados a la lucha contra el fraude. En consecuencia, tiene sentido que ambos tipos de profesionales colaboren en una asociación que sirva a los intereses de la organización.

Este Informe Global de Conocimiento (Global Knowledge Brief), el segundo de una serie de tres partes sobre el fraude, examina las ventajas de establecer una relación simbiótica entre los auditores internos y los CFE.

El alcance del fraude

Pérdida media de casi 1,8 millones de dólares

El fraude sigue siendo un riesgo omnipresente

El fraude es cualquier acto ilegal que implique engaño, ocultación o abuso de confianza y que se lleve a cabo para obtener un beneficio económico o personal. Las personas u organizaciones que cometen fraude pueden estar buscando robar dinero, propiedades o servicios; evitar pagar o perder algo; o conseguir una ventaja personal o empresarial. Además de los estafadores externos, los fraudes también pueden ser perpetrados por empleados de la empresa que sufren presiones financieras o que sienten que se les debe el dinero o los servicios que toman porque perciben que la organización les ha tratado injustamente o debido a algún otro agravio. Cualquier tipo de organización puede ser víctima de un fraude, independientemente de su tamaño o de si es pública o privada, sin ánimo de lucro, un organismo gubernamental o una empresa de servicios públicos o privados, u otra entidad.

El fraude es un riesgo grave y generalizado para las organizaciones. Las consecuencias del fraude pueden ser desde perturbadoras hasta nefastas. Pueden incluir no sólo retos y pérdidas financieras, sino también ineficiencias que dañan las operaciones, los ingresos o los beneficios; la cancelación de proyectos y, dependiendo de su alcance, potencialmente la quiebra de la organización.[5]

Una encuesta realizada por la Association of Certified Fraud Examiners (ACFE) entre CFE de todo el mundo abarcó 2.110 casos de fraude de 133 países. Dentro de ese grupo, las pérdidas globales debidas al fraude ascendieron a más de 3.600 millones de dólares, con una pérdida media por caso de casi 1,8 millones de dólares. De hecho, los CFE estiman que las organizaciones pierden cada año el 5% de sus ingresos a causa del fraude. Las empresas más pequeñas eran claramente las más expuestas al riesgo de fraude: Las que tenían menos trabajadores sufrieron la mayor pérdida media, de 150.000 dólares.

Aunque las pérdidas de esa cuantía pueden ser fáciles de detectar, el fraude suele producirse en incrementos más pequeños a lo largo del tiempo. Según la encuesta, un fraude típico puede suponer una pérdida de 8.300 dólares al mes y puede tardar 12 meses en detectarse. También es importante ser consciente de que la criptomoneda está implicada en algunos fraudes. La ACFE descubrió que estaban implicadas en el 8% de los casos. Los escenarios habituales implicaban la realización de pagos de sobornos y comisiones ilegales y la conversión de activos malversados.[6]

Categorías de fraude profesional

Existen tres categorías principales de fraude laboral, según el Informe a las Naciones 2022 de la ACFE.

Las tramas de fraude en los estados financieros, es decir, causar una inexactitud u omisión material en los estados financieros de la organización, fueron las menos comunes (9%) pero las más caras, con 593.000 dólares de pérdidas por caso.

La apropiación indebida de activos, en la que un empleado roba o utiliza indebidamente recursos de la empresa, se produjo en el 86% de los casos. Sin embargo, fue responsable de las pérdidas medias más bajas: 100.000 dólares por caso.

La corrupción, que abarca sobornos, conflictos de intereses y extorsión, estuvo implicada en el 50% de los casos y provocó pérdidas de 150.000 dólares por caso.

Fuente: *Occupational Fraud 2022: A Report to the Nations*, Association of Certified Fraud Examiners.

[5] [5] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[6] *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

El papel del auditor interno

Aseguramiento/asesoramiento en prevención del fraude

La detección y disuasión del fraude, pilar de la auditoría interna

Según el Instituto de Auditores Internos (IIA), "la auditoría interna es una actividad independiente y objetiva de aseguramiento y consultoría diseñada para añadir valor y mejorar las operaciones de una organización. Su función incluye la detección, prevención y control de los riesgos de fraude y su tratamiento en auditorías e investigaciones."[7]

Las organizaciones no deben esperar que el conjunto de habilidades de la auditoría interna incluya la investigación del fraude. Si las circunstancias requieren que la auditoría interna asuma un papel de investigación, los auditores internos deben ejercer la debida diligencia profesional y no deben proceder si no tienen la experiencia y los conocimientos necesarios.

Si bien la prevención del fraude es función de la dirección, la auditoría interna apoya los esfuerzos de gestión antifraude prestando los servicios de garantía necesarios sobre los controles internos diseñados para detectar e impedir el fraude. A menudo el fraude se produce debido a controles mal diseñados y a una gobernanza débil que socava los procesos de la organización. Casi la mitad de los casos de la encuesta de la ACFE se atribuyeron a la falta de controles internos (29%) o a la anulación de los controles existentes (20%). Los auditores tienen en cuenta el riesgo potencial de fraude y la adecuación de los controles internos en las áreas que examinan. Según la encuesta, cuando existen controles antifraude, tienden a producirse menos pérdidas por fraude y una detección más rápida del mismo.

La contribución de la auditoría interna a la lucha contra el fraude no debe subestimarse. Cuando el IIA pidió a los directores ejecutivos de auditoría (CAE) que citaran los ámbitos en los que las funciones de auditoría interna tenían una participación significativa, el 57% citó el fraude y el 56% señaló la evaluación general de riesgos.[8] Mientras tanto, la encuesta de la ACFE descubrió que la pérdida media

Consideraciones integradas en las auditorías

Fuente: 2023 North American Pulse of Internal Audit report

Encuesta del IIA sobre el pulso norteamericano de la auditoría interna, del 20 de octubre al 2 de diciembre de 2022. P25: Cuando realiza encargos de auditoría en general, ¿cuáles de las siguientes áreas suele incluir en sus consideraciones? (Elija todas las que correspondan.) n = 555.

[7] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.
[8] 2022 Premier Global Research, *Internal Audit: A Global View*, Internal Audit Foundation, 2022.

por fraude era un 50% mayor (150.000 dólares frente a 100.000 dólares) cuando no había auditoría interna.

De hecho, los datos del próximo informe 2023 North American Pulse of Internal Audit revelan que el fraude es la consideración más frecuentemente citada en las auditorías internas. En la encuesta anual a directores de auditoría norteamericanos se pidió a más de 500 encuestados que indicaran qué áreas incluían como parte de sus auditorías en general. "Las respuestas indican que los auditores suelen adoptar un enfoque holístico y tienen en cuenta una amplia gama de cuestiones, como la ciberseguridad, los terceros y la gobernanza", según el informe, que se presentará por primera vez en marzo en la Conferencia GAM 2023. En general, el 89% de los CAE dijeron que incluyen consideraciones de fraude en cada auditoría, que fue la categoría de riesgo más frecuentemente citada, con las consideraciones de TI en segundo lugar, con un 80%.

Según el Documento de Posición del IIA sobre Fraude y Auditoría Interna: Assurance over Fraud Controls Fundamental to Success (Aseguramiento sobre Controles de Fraude Fundamento para el Éxito), [9] la auditoría interna debe tener los conocimientos necesarios sobre el fraude para poder:

- Identificar las señales de alarma que pueden indicar que se ha cometido un fraude.
- Comprender las características del fraude y las técnicas utilizadas para cometerlo, así como los tipos de tramas y escenarios de fraude.
- Ser capaz de decidir si es necesario adoptar nuevas medidas o si debe recomendarse una investigación.
- Evaluar la eficacia de los controles para prevenir o detectar el fraude e identificar oportunidades de mejora.

[9] IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

El papel del examinador de fraudes

Investigar el engaño

La investigación competente del fraude es fundamental

El examinador de fraudes participa y apoya los programas generales de examen de fraudes de la organización. Lo hace, en parte, llevando a cabo investigaciones de fraude que "tratan de obtener hechos y pruebas que ayuden a establecer lo sucedido, identificar a la parte responsable y ofrecer recomendaciones cuando proceda."[10] Una de las cuestiones que un examinador tiene en cuenta al iniciar una investigación es la predicción, lo que significa que el conjunto de circunstancias debe hacer que a un profesional bien formado le parezca razonable que se ha producido un fraude.

Los pasos que da un examinador de fraudes en una investigación pueden incluir la obtención de pruebas, la elaboración de informes sobre lo que se encuentra, testificar sobre esos hallazgos según sea necesario y ayudar en la detección y prevención del fraude. Dos objetivos comunes de un examen de fraude son la investigación de un posible fraude o de una acusación de fraude y la revisión de las políticas y controles antifraude de una organización. ” Otros objetivos más específicos de un examen de fraude pueden ser:

- Determinar las pérdidas o responsabilidades reales o potenciales derivadas del fraude.
- Demostrar el compromiso de la organización para identificar y mitigar el fraude.
- Ayudar a facilitar la recuperación de pérdidas.
- Prevenir futuros fraudes y las pérdidas o responsabilidades relacionadas.
- Abordar las consecuencias más allá de las pérdidas financieras.
- Detectar y reforzar los puntos débiles de los controles internos.
- Cuando sea necesario en algunos casos, cumplir con las leyes, reglamentos, contratos o deberes del derecho consuetudinario.[11]

[10] “Planning and Conducting a Fraud Examination,” *Fraud Examiners Manual: 2022 Edition*, ACFE.
[11] ibid

Comparación de enfoques

Esta tabla ofrece una visión general de algunas diferencias importantes entre las funciones, enfoques y objetivos de los auditores internos y los Certified Fraud Examiners -CFEs.

Características	**Auditoría interna**	**Examen de fraude**
Intention	Los procedimientos de auditoría interna pueden descubrir fraudes, pero no garantizan que se detecten. Por ejemplo, los auditores pueden encontrar una transacción o situación sospechosa en una revisión y puede que finalmente se identifique como fraude. Sin embargo, encontrar un fraude sólo será un aspecto de un examen más amplio de los controles y procedimientos dentro del área auditada.	Un examen de fraude se centra directamente en descubrir el fraude y considerar acciones o actividades antifraude.
Ocurrencia	Las auditorías suelen ser periódicas, aunque pueden utilizarse auditorías emergentes para abordar una situación única o cuestiones en un área.	Por lo general, los exámenes de fraude sólo se llevan a cabo con suficiente antelación, aunque pueden producirse sin ningún desencadenante específico como parte de un programa de gestión de riesgos o de evaluación del riesgo de fraude. Sin embargo, la mayoría se realizan en respuesta a un chivatazo o una denuncia. La encuesta de la ACFE descubrió que el 43% de los fraudes se detectaban gracias a soplos, una cifra casi tres veces superior a la del siguiente método más común para encontrar fraudes. Más de la mitad de los avisos de fraude procedían de empleados.
¿Adversario o no?	Las auditorías internas no tienen carácter contencioso. El objetivo de los auditores es ofrecer ideas e información que los jefes y miembros de los equipos puedan utilizar para mejorar los controles u otros procesos, por ejemplo.	Los exámenes de fraude son intrínsecamente contenciosos. Parte del objetivo es culpar a quien comete el fraude.
Normas	Los auditores internos siguen las *Normas Internaciones para la Práctica Profesional* de la Auditoría Interna, establecidas por el Instituto de Auditores Internos (IIA).	Los CFEs siguen el *Codigo de Normas Profesionales* de la ACFE. Los CFE pueden utilizar una herramienta de evaluación del riesgo de fraude de la ACFE en sus exámenes.

Poner en práctica la colaboración

Respeto mutuo y responsabilidades

Trabajar la batalla contra el fraude

Existen numerosas oportunidades de colaboración beneficiosa entre auditores y examinadores del fraude. Pueden consultarse mutuamente sobre:

- Puesta en marcha de una investigación de fraude
- Planificación anual de auditorías y exámenes de fraude
- Evaluaciones de riesgos
- Evaluación y valoración de controles y programas antifraude
- Transmisión de los resultados de auditoría con implicaciones de fraude
- Subsanación de deficiencias de control

Muchas organizaciones tienen normas que rigen los protocolos cuando la auditoría interna entrega un hallazgo de fraude a un equipo de examen de fraude externo o interno. El equipo de auditoría interna toma nota del hallazgo de fraude y luego realiza un informe conjunto con el examinador de fraude al final de la revisión.

Además, la auditoría interna puede auditar al departamento antifraude de una organización para asegurarse de que sus propios controles son adecuados. Un equipo antifraude puede informar a los equipos jurídicos o de gestión del riesgo empresarial, entre otras áreas, incluida la auditoría interna. En caso de que un equipo antifraude dependa de auditoría interna, cualquier auditoría de ese departamento debe subcontratarse para garantizar la objetividad.

Un caso de estudio ilustra la colaboración en el trabajo

El siguiente caso práctico demuestra cómo pueden trabajar juntos los dos equipos. Se basa en un debate de Shawna Flanders CRISC, CISA, CISM, SSGB, SSBB, directora de desarrollo de productos del IIA, en un reciente seminario web del IIA y la ACFE, *Fostering Collaboration: El Auditor y examinador de fraudes*.

Normalmente, la auditoría interna descubre un patrón que imita el fraude y alerta a los examinadores de fraudes. En el caso presentado por Flanders, una auditoría interna incluía una revisión de los préstamos para automóviles. Uno de los pasos que dio su equipo fue evaluar las cuentas morosas. En un grupo de 40 cuentas de este tipo, destacaban cinco. El sistema estaba configurado para marcar los préstamos morosos que debían ser objeto de seguimiento, pero por alguna razón estos cinco no estaban marcados. Además, todas tenían características poco habituales: un tipo de interés del 0%, plazos de 72 meses y ningún pago mínimo.

Cuando Flanders investigó, descubrió que el ID de usuario asociado a los préstamos pertenecía a un representante de atención al cliente, lo que no tenía sentido. Una persona con esta función no solía aprobar préstamos. A continuación, revisó los archivos de registro relacionados con los préstamos y descubrió que, aproximadamente una hora antes de que se presentara y aprobara cada uno de ellos, el titular del identificador de usuario disponía de acceso adicional al sistema. Ese acceso se eliminó aproximadamente una hora después de que se aprobaran y activaran los préstamos. Dadas las inusuales condiciones de los préstamos, la participación del

representante del servicio de atención al cliente y los cambios en el acceso al sistema, el equipo de auditoría supo que había llegado el momento de remitir el caso al departamento de fraudes de la empresa.

Dependiendo de las políticas y procedimientos de la organización, los pasos que el departamento de fraude podría dar en este caso cuando se le alerta de la actividad sospechosa incluyen:

- Corroborar la información recibida de los auditores.
- Examinar todas las actividades relacionadas con estas cuentas.
- Determinar si la creación de estas cinco cuentas fue una acción única o parte de un posible esquema en curso.
- Identificar a los cómplices.
- Considerar si hay otras sucursales u oficinas implicadas y el alcance global del fraude.

En este punto, los examinadores del fraude también pueden considerar si el fraude debe detenerse y cómo. Si se necesitan más pruebas o información, puede decidirse que debe permitirse que el fraude continúe al menos temporalmente. Según Mason Wilder, CFE, director de investigación de la ACFE, que también participó en el seminario web, se trata de una determinación complicada que dependerá de cuánto haya perdido ya la empresa, cuánto podría perder potencialmente si el fraude continúa y el apetito de riesgo de la organización. En este caso, los pasos a dar antes de cerrar el fraude pueden incluir entrevistar al representante de atención al cliente para obtener más información e identificar el alcance del fraude, y descubrir potencialmente fraudes adicionales o planes para cometer más.

Una vez reunidas y analizadas las pruebas, los examinadores de fraudes comunicarán sus conclusiones -oralmente o por escrito- a las personas adecuadas de la organización. Puede tratarse de la dirección, el consejo de administración o el comité de auditoría. Según el Manual de Examinadores de Fraude de la ACFE, "un informe de examen de fraude es una narración de las actividades específicas del examinador de fraude, sus hallazgos y, si procede, sus recomendaciones". La dirección de la organización puede utilizar el informe para determinar los pasos a seguir.

Si los examinadores del fraude revisan la situación y no encuentran fraude real, pueden devolver el caso si determinan que la alerta roja original surgió debido a una deficiencia en los controles de gestión del riesgo de fraude. La auditoría interna podría entonces incluir esta deficiencia en su informe.

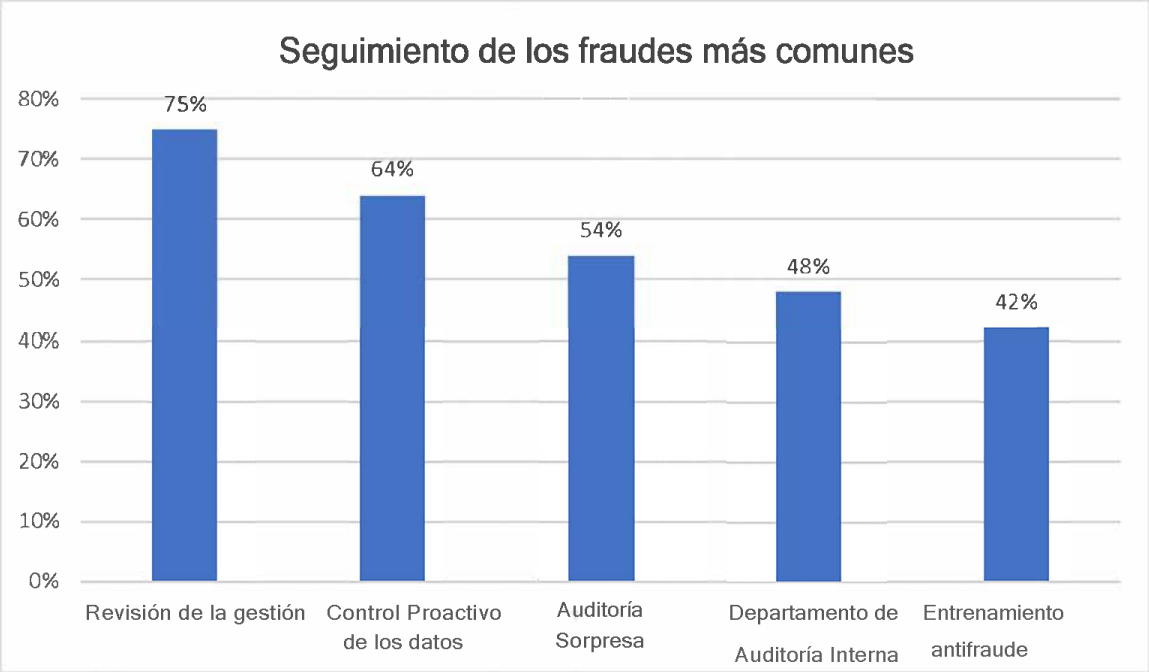
Combinar Fuerzas

Quienes se preocupan por el fraude deben recordar que la mitigación es importante. El informe de la encuesta de la ACFE señalaba que las medidas proactivas para descubrir el fraude pueden conducir a una detección más temprana y a menores pérdidas, mientras que los esfuerzos reactivos permiten que las tramas se desarrollen durante más tiempo y aumentan el impacto financiero para la víctima.

Sin embargo, las organizaciones no pueden identificar o eliminar todos los riesgos de fraude. Se enfrentan a numerosos tipos de fraude, una variedad de motivaciones detrás de ellos y una amplia gama de autores. Sin embargo, cuanto más informadas estén las personas a todos los niveles -dirección, consejo de administración y personal- mejor podrán desplegar esfuerzos razonables de mitigación e identificar el fraude o las señales de alarma que puedan indicar su existencia. Mediante la combinación de sus habilidades y experiencia únicas, los auditores internos y los examinadores de fraude pueden hacer una fuerte contribución a los esfuerzos generales de la organización. Las organizaciones pueden utilizar su trabajo para tomar decisiones más informadas sobre los enfoques de gestión del riesgo de fraude.

Pasos para prevenir la reincidencia

El 81% de las organizaciones encuestadas por la ACFE modificaron sus controles antifraude después de un fraude. El gráfico siguiente muestra los cambios más típicos en los controles que las organizaciones implantaron o modificaron. Otros controles antifraude recomendados por la ACFE incluyen la supervisión automatizada de transacciones/datos, la vigilancia y la conciliación de cuentas.



Fuente: ***Occupational Fraud 2022: A Report to the Nations*****, Asociación de Examinadores de Fraude Certificados.**

Conclusión

El papel de la auditoría interna como proveedor de tercera línea de garantía sobre la gobernanza, el riesgo y el control interno requiere estructuras, procesos y prácticas que promuevan una garantía objetiva e independiente. Pero, como se señala en el Modelo de las Tres Líneas del IIA, la independencia no implica aislamiento.

"Debe existir una interacción regular entre la auditoría interna y la dirección para garantizar que el trabajo de la auditoría interna es relevante y está alineado con las necesidades estratégicas y operativas de la organización. A través de todas sus actividades, la auditoría interna construye su conocimiento y comprensión de la organización, lo que contribuye a la garantía y el asesoramiento que ofrece como asesor de confianza y socio estratégico", según el Modelo.

Este es claramente el caso cuando la auditoría interna y los examinadores de fraude certificados encuentran un terreno común como aliados en la batalla contra el fraude.

Parte 3

La resaca: El fraude en la era post-COVID

Sobre el experto

David Domínguez, CIA, CRMA, CPA, CFE

David es Director de Auditoría y Cumplimiento de Itafos en Houston. En su carrera, David ha trabajado con empresas multinacionales de diversos sectores para establecer, dirigir y transformar funciones de auditoría interna corporativas y regionales. Ha dirigido y ejecutado proyectos de aseguramiento y asesoramiento financiero, operativo y de TI en Norteamérica, Latinoamérica, Europa y Asia. También ha dirigido y participado en numerosas investigaciones multijurisdiccionales, iniciativas de análisis de datos y una amplia variedad de auditorías internacionales de accionistas, empresas conjuntas y proveedores. Sus áreas de especialización incluyen el gobierno corporativo y organizativo, la gestión del riesgo empresarial, la gestión del riesgo de fraude, la Ley Sarbanes-Oxley de 2002 y los programas de ética y cumplimiento.

Introducción

Durante la mayor parte de dos años, COVID-19 causó disrupciones en todos los ámbitos, desde la forma en que trabajaba la gente, dónde trabajaba, cómo sus organizaciones trataban con los proveedores y los problemas de la cadena de suministro, y cómo gestionaban preocupaciones importantes, como el mantenimiento de los controles internos y la detección y prevención del fraude.

Hoy en día, el mundo respira más tranquilo a medida que lo peor de la pandemia se desvanece lentamente en la historia, pero aún así, no se debe asumir que los riesgos asociados con COVID-19 ya no son una preocupación. De hecho, las organizaciones que hagan esa suposición podrían estar cometiendo un grave error. Este Informe Global del Conocimiento (Global Knowledge Brief), el tercero de una serie de tres partes sobre fraude del Instituto de Auditores Internos (IIA), examina varios factores de fraude relacionados con la pandemia identificados en el Informe 2022 de la ACFE a las Naciones, cómo pueden afectar a las organizaciones y el papel de la auditoría interna en los esfuerzos organizativos para mitigar esos factores de riesgo de fraude.

El fraude y los riesgos de fraude persisten

Los cambios relacionados con las pandemias siguen preocupando

Surgirán nuevos fraudes inspirados en COVID

En su último Informe a las Naciones sobre fraude laboral, la Asociación de Examinadores de Fraude Certificados (ACFE) descubrió que la duración media de los fraudes -es decir, el tiempo típico entre el momento en que se inicia un fraude y el momento en que se detecta- era de 12 meses.[12] Esto significa que las organizaciones siguen enfrentándose a fraudes relacionados con la pandemia que aún no han sido descubiertos**.**

Hay muchas razones por las que los cambios relacionados con la pandemia siguen repercutiendo en el riesgo de fraude. Por ejemplo, la adopción del trabajo a distancia pretendía ser temporal, pero se ha convertido en un procedimiento operativo estándar en muchas empresas. El trabajo a distancia a menudo trajo consigo cambios significativos -y en algunos casos la relajación- de las prácticas y procedimientos diseñados para identificar o mitigar el fraude. Como resultado, los riesgos asociados siguen planteando amenazas para las empresas, incluso cuando las perturbaciones relacionadas con la pandemia han disminuido.

La auditoría interna ha desempeñado y seguirá desempeñando un papel clave en la gestión de los riesgos de fraude relacionados con la pandemia. En un estudio de miembros del IIA de todo el mundo realizado por la Fundación de Auditoría Interna (IAF) y Kroll, muchos participantes en mesas redondas relacionadas consideraron que la pandemia "puso a la auditoría interna más en el asiento del conductor cuando se trata de la gestión del riesgo de fraude".[13] Esto incluye una mayor participación en las consideraciones estratégicas de los retos operativos, proporcionando una garantía continua y una mayor colaboración entre las funciones empresariales, todo ello manteniendo la independencia del auditor.

[12] *Occupational Fraud 2022: A Report to the Nations*, ACFE.
[13] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

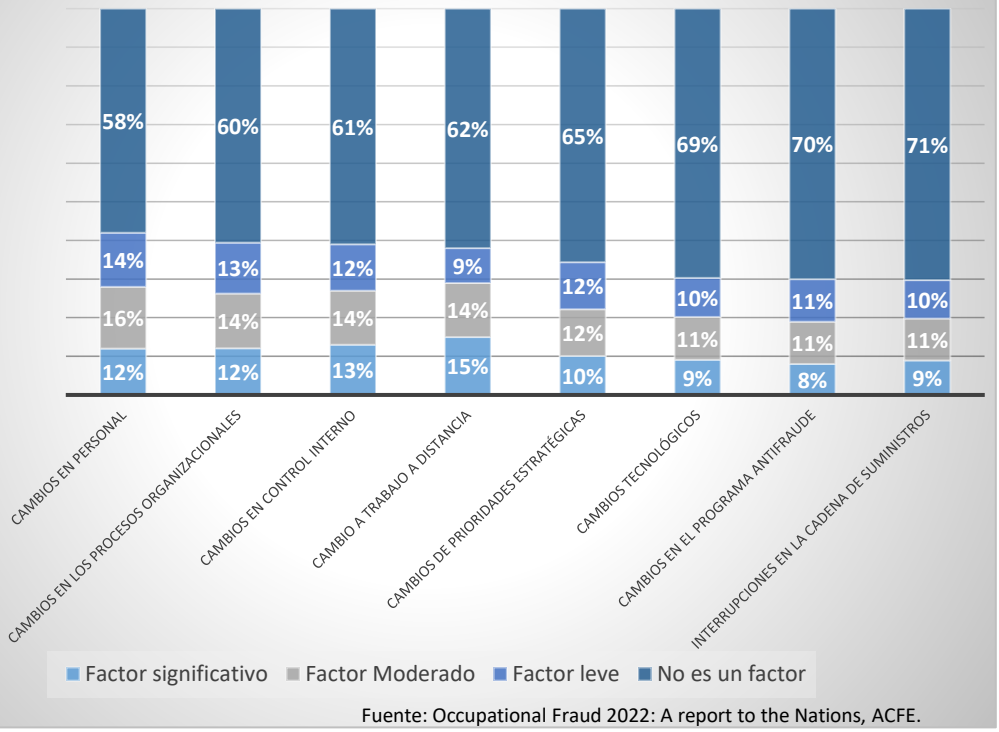
Principales riesgos de fraude relacionados con la pandemia

Los cambios de personal y el trabajo a distancia, principales preocupaciones

Más de la mitad considera que los factores pandémicos contribuyen al fraude

En la preparación de su informe sobre fraude laboral, la ACFE descubrió que el 52% de los encuestados informaron de que, en los incidentes de fraude que habían investigado, al menos una de las diversas cuestiones relacionadas con la pandemia había contribuido al fraude. Entre ellos, los cambios organizativos de personal relacionados con la pandemia fueron los más comunes. El 42% de los encuestados afirmaron que los cambios de personal fueron factores significativos, moderados o leves que contribuyeron al fraude laboral. El cambio al trabajo a distancia fue el factor más citado como significativo (15%), seguido de los controles internos (13%) (véase la Figura 1).

Figura 1: ¿En qué medida contribuyeron los factores relacionados con la pandemia a los fraudes laborales?



Fuente: Occupational Fraud 2022: A report to the Nations, ACFE.

Un examen más profundo de algunos de los principales problemas relacionados con la pandemia identificados en el informe de la ACFE muestra que las repercusiones pueden ser a menudo complejas y sutiles.

Los cambios de personal plantean diversos riesgos de fraude

La pandemia obligó a muchas organizaciones a encontrar soluciones provisionales o atajos para hacer frente a las numerosas perturbaciones que sufrían, como cambiar o ampliar las responsabilidades de los trabajadores o incorporar a nuevas personas que disponían de un tiempo limitado para aclimatarse a sus puestos de trabajo. Además, los despidos temporales o las excedencias derivadas de la incertidumbre económica relacionada con la pandemia se convirtieron a menudo en permanentes, señaló David Domínguez, director de auditoría y cumplimiento de Itafos, una empresa de fosfatos y fertilizantes especiales. "Sin duda aumentó el riesgo desde varios ángulos", afirmó.

Dados los numerosos ajustes y adaptaciones a las prácticas y protocolos de trabajo que puede haber creado la pandemia -y la posible curva de aprendizaje para quienes asumen nuevas tareas-, las organizaciones deben considerar qué tipos de impactos involuntarios pueden haber tenido estos cambios. He aquí algunas áreas a considerar:

Cultura

Hay varias razones para reevaluar y quizás reafirmar la cultura y los valores corporativos tras la pandemia. El "hacer que funcione" fue una virtud durante la pandemia, pero eso puede significar que se hayan olvidado algunas prácticas y actitudes éticas importantes. También es posible que los nuevos trabajadores nunca hayan experimentado una introducción adecuada a los valores éticos de la empresa. Si ese es el caso, las organizaciones harían bien en recordar a los empleados sus expectativas sobre los comportamientos éticos.

"Un enfoque proactivo de la cultura puede disuadir de varios tipos de mala conducta y promover comportamientos que pueden mejorar la moral y la productividad", afirma la ACFE en su informe. "La cultura tiene una poderosa capacidad para afectar a la forma en que la gente hace su trabajo; cómo se toman las decisiones sobre calidad, cumplimiento y otras preocupaciones críticas; y cómo se percibe la organización tanto interna como externamente."[14]

Consideraciones sobre recursos humanos

La escasez de mano de obra y las políticas cambiantes sobre el trabajo híbrido y a distancia han puesto patas arriba algunas prácticas de recursos humanos de larga tradición, como las líneas directas de denuncia anónima.

Una importante herramienta de recursos humanos para la prevención del fraude es la línea de denuncia anónima. De hecho, según el informe de la ACFE, el 42% de los fraudes se detectaron mediante denuncias, más del triple que el siguiente método más común.

La auditoría interna puede apoyar este proceso examinando si funciona según lo previsto. El primer paso podría ser determinar hasta qué punto se supervisan estas líneas directas y si se hace un seguimiento de las denuncias, explica Dominquez. Recomienda hacer preguntas a los monitores de las líneas directas, como por ejemplo:

- **¿Cómo se accede a la línea directa?** Las opciones incluyen dejar las sugerencias en un buzón de la oficina, llamar al número de la línea directa o comunicar las quejas por Internet. Tenga en cuenta que un buzón -y los carteles que promocionan la línea directa- no ayudarán a los trabajadores a distancia.
- **¿Puede la línea directa estar disponible en diferentes idiomas, si procede?**
- **¿Qué seguimiento se hace del esfuerzo?** Domínguez señaló que algunas empresas se felicitan por el bajo número de reclamaciones. Esto podría ser un reflejo exacto de una organización bien gestionada, pero también puede indicar que algunas llamadas a la línea directa no se contestan o que rara vez se da curso a las quejas.

La auditoría interna puede revisar el proceso de respuesta a las reclamaciones para asegurarse de que el tiempo transcurrido desde la recepción hasta la resolución es el adecuado y de que las decisiones de hacer o no un seguimiento están bien fundadas. Las organizaciones a veces pasan por alto pistas válidas de fraude por miedo a represalias tras una denuncia. La auditoría interna puede

[14] *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, Anti-Fraud Collaboration, March 2020.

revisar si el manual corporativo o el código de conducta prohíben explícitamente las represalias. Yendo más allá, la auditoría interna también puede ayudar a la empresa a comprobar si los denunciantes tienen menos probabilidades de obtener un ascenso o más probabilidades de recibir una mala evaluación del rendimiento, señaló Domínguez. Incluso cuando una denuncia es infundada, las empresas pueden descubrir a través del proceso de respuesta políticas que necesitan ser actualizadas o aclaradas, dijo.

Otras precauciones y controles valiosos que las organizaciones deberían mantener o aplicar son:

- Comprobación de antecedentes para identificar antecedentes crediticios u otros problemas financieros o antecedentes de embargos de salarios, embargos preventivos o sentencias que puedan estar asociados a la malversación.
- Verificación de credenciales.

La ACFE informó de que el 50% de los defraudadores mostraban al menos una bandera roja relacionada con los recursos humanos antes o durante el incidente de fraude. En cuanto a los indicios de comportamiento, vivir por encima de las propias posibilidades ha sido la señal de alarma más común en todos los estudios de la ACFE desde 2008. Se identificó en el 39% de los casos, muy por delante del segundo factor más común, las dificultades financieras, con un 25%.

Inseguridad Laboral

La ACFE identificó una serie de ejemplos de incertidumbre laboral que pueden contribuir al fraude, y las difíciles condiciones económicas pueden acentuar dicha inseguridad. Las señales de alarma específicas incluyen:

- Miedo a perder el empleo.
- Denegación de un aumento de sueldo o un ascenso.
- Reducción de prestaciones.
- Reducción salarial.
- Reducción involuntaria del horario.
- Descenso de categoria

Aunque el clima económico se ha estabilizado desde los peores días de la pandemia, siguen existiendo retos en el clima empresarial mundial. No es sorprendente que el impacto de los problemas relacionados con la incertidumbre laboral siguiera siendo fuerte en 2022, según la ACFE. Es lógico que algunas de estas incertidumbres puedan seguir siendo un factor que impulse la mala conducta de los empleados.

Estas señales de alarma se aplican a los empleados en general, pero hay algunas señales adicionales que se aplican específicamente a los altos ejecutivos:

- **Acoso o intimidación.** 23% para propietarios/directivos; 8% para no propietarios/directivos.
- **Problemas de control.** 18% para propietarios/ejecutivos; 12% para no propietarios/ejecutivos.
- **Actitud fraudulenta "Wheeler-dealer".** 17% para propietarios/ejecutivos; 9% para no propietarios/ejecutivos.
- **Presión excesiva desde dentro de la organización.** 13% para propietarios/ejecutivos; 6% para no propietarios/ejecutivos.
- **Problemas legales en el pasado.** 11% para propietarios/ejecutivos; 3% para no propietarios/ejecutivos.

Deben revisarse los cambios de control interno relacionados con COVID

Los controles internos son procedimientos adoptados para garantizar que las acciones y decisiones de toda una organización se ajustan a sus políticas, requisitos de información y mandatos de cumplimiento. Los controles antifraude pueden reducir las pérdidas por fraude

y facilitar su detección más rápida. En el estudio de la ACFE, casi la mitad de las pérdidas por fraude podían atribuirse a dos factores: la falta de controles internos (29%) y la anulación de los controles existentes (20%). La implantación y el refuerzo de los controles internos pueden aportar claramente un beneficio positivo significativo a las organizaciones. La auditoría interna tiene un importante papel que desempeñar a la hora de informar sobre los controles internos y recomendar mejoras de los mismos. De hecho, la encuesta de la ACFE reveló que la pérdida media por fraude era un 50% mayor (150.000 dólares frente a 100.000 dólares) cuando no existía un departamento de auditoría interna.

Los auditores internos que respondieron a la encuesta de IAF/Kroll creían que "el marco de control interno se había debilitado debido a los retos del trabajo a distancia y, en muchos casos, a la reducción de personal por enfermedad, excedencias y reducción de plantilla".[15]

Es posible que las nuevas personas que se incorporan a las organizaciones en tiempos de crisis no hayan recibido suficiente formación o transferencia de conocimientos, o que sólo hayan aprendido protocolos de emergencia que no incluían procesos y controles de larga duración, según Domínguez. "Los controles se diluyeron o tal vez simplemente se perdieron", dijo. Por el camino, estos atajos pueden convertirse -y seguir siendo- un procedimiento operativo estándar, a pesar de que sólo debían utilizarse durante un periodo de tiempo específico o en una situación concreta.

Esta preocupación ha provocado cambios positivos en muchas organizaciones. Por ejemplo, aproximadamente tres cuartas partes de los miembros de comités de auditoría que respondieron a una encuesta conjunta del Center for Board Effectiveness de Deloitte y el Center for Audit Quality afirmaron haber actualizado sus controles internos en el último año debido al entorno de trabajo a distancia.[16]

Las deficiencias en los controles internos pueden contribuir al fraude al crear o promover un entorno en el que es más fácil descuidar o anular medidas antifraude sólidas. Por ejemplo, durante la pandemia, la segregación de funciones -una medida antifraude común y eficaz- puede haberse dejado de lado porque era más difícil de llevar a cabo con trabajadores dispersos por diferentes lugares o debido a recortes o escasez de personal. Este es el tipo de control interno que una empresa debe revisar ahora para asegurarse de que se ha restablecido y funciona eficazmente.

La auditoría interna puede ayudar a las organizaciones a hacer frente a estos riesgos garantizando la existencia de protocolos y procesos vitales. Utilizando la tecnología de mapeo de procesos, pueden realizar un seguimiento de los procesos durante un periodo reciente -seis meses o un año- e identificar variaciones con respecto a las directrices adecuadas o las mejores prácticas. "Se pueden ver las desviaciones de los procedimientos o políticas estándar e identificar qué procesos deben actualizarse o aplicarse", explica Domínguez.

Otras áreas que deben revisarse son los controles internos relacionados con las adquisiciones, la emisión de cheques, las conciliaciones bancarias, los reembolsos de gastos o cualquier área relacionada con consideraciones financieras.

El trabajo a distancia sigue siendo un factor de fraude crítico

El drástico giro hacia el trabajo a distancia -cerrar oficinas y permitir a los trabajadores realizar su trabajo en casa- fue probablemente el cambio más significativo para la mayoría de las organizaciones durante la pandemia. En consecuencia, este nuevo enfoque fue el factor más citado como contribuyente significativo al fraude en el informe de la ACFE. En circunstancias normales, una empresa podría pasar meses considerando el impacto estratégico de tal movimiento, pero esto era esencialmente imposible en medio de la incertidumbre y la urgencia de las primeras semanas de la pandemia. Por lo menos, trabajar solo y fuera de la vista de colegas y supervisores puede facilitar la comisión de diversos fraudes. Según la ACFE, las personas que vayan a realizar o hayan realizado un

[15] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[16] *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, January 25, 2022.

cambio permanente hacia el trabajo a distancia o híbrido deberían planificar la gestión del cambio "para descubrir las líneas de falla que pueden tener consecuencias catastróficas si no se abordan".[17]

A través de este proceso, hay varias líneas de fallo potenciales en las que la auditoría interna podría centrarse. Por ejemplo, las dificultades de gestionar eficazmente a las personas en un entorno remoto fragmentado y su impacto en la cultura se citaron como áreas clave a abordar, según el informe IAF/ Kroll.[18] El comportamiento ético es a menudo algo que se aprende y se refuerza a través de las interacciones con otros trabajadores que lo demuestran en el trabajo. El acceso a compañeros con más experiencia puede ayudar a los empleados a entender cómo responder en circunstancias confusas o sospechosas, como cuando otro trabajador parece estar actuando de forma inadecuada o ilegal.

Entre los tipos de fraude específicamente asociados al trabajo a distancia se encuentran:

- **Robo de tiempo o declaraciones inexactas sobre las horas trabajadas.** Esto puede ser más fácil cuando alguien no está bajo supervisión directa.
- **Robo de datos o uso indebido o intercambio de información confidencial o delicada.** Esto puede ser realizado por aquellos que pueden acceder a los dispositivos de un empleado o por empleados que se sienten más cómodos haciendo un mal uso de los datos cuando están fuera de la oficina.[19]

Otro problema es que los empleados a distancia realicen trabajos secundarios. Por ejemplo, un empleado puede realizar tareas de consultoría o temporales para otra empresa durante las horas que se supone que debería estar trabajando para su empleador principal, explica Domínguez. Esto es sin duda robo de tiempo, pero el uso indebido de recursos de la empresa, como ordenadores portátiles o teléfonos, también puede exponer a la empresa a problemas de ciberseguridad. El trabajo paralelo también puede ser un conflicto de intereses si el empleado está trabajando para un competidor, especialmente si comparte información que beneficia a la competencia. La auditoría interna puede ayudar a abordar este problema cuestionando el tipo de formación que reciben los empleados y si el manual del empleado y las políticas se han actualizado para los nuevos entornos de trabajo, dijo Domínguez.

Cambios tecnológicos crean el "estira y encoge" del fraude

La tecnología puede permitir a las organizaciones aplicar procedimientos eficaces en ámbitos como los controles internos y el trabajo a distancia. Las organizaciones ya estaban realizando mejoras e inversiones en tecnología para abordar los problemas de ciberseguridad, y la pandemia estimuló a las empresas a acelerar y reforzar sus sistemas. Muchas funciones de auditoría interna se incluyeron en la actualización tecnológica. De hecho, el 29% de los auditores internos han añadido el análisis de datos como herramienta para identificar el fraude y la corrupción desde que comenzó la pandemia.[20]

Al mismo tiempo, el uso incorrecto o negligente de las herramientas tecnológicas puede facilitar el éxito de las tramas de fraude. Como se ha señalado, el robo de datos es una de las preocupaciones asociadas al trabajo a distancia. Las posibles soluciones a los riesgos de robo de datos, según la ACFE, incluyen exigir a los trabajadores que protejan su red doméstica y no la compartan con otros miembros de la familia. El uso de redes privadas virtuales (VPN) y de contraseñas y configuraciones más fuertes y complejas para proteger los ordenadores domésticos son también fundamentales. Otras opciones son la autenticación multifactor y la formación anual de los empleados sobre seguridad y privacidad de los datos. Las organizaciones también deben desarrollar políticas sobre el uso aceptable de los dispositivos electrónicos, las redes sociales y los datos de la empresa, así como exigir a los empleados que las lean y reconozcan que las entienden.

Las organizaciones que trabajan en un entorno remoto o híbrido también tendrán que asegurarse de que los empleados actualizan el software y los parches de seguridad en sus dispositivos domésticos, así como educar a los trabajadores sobre las mejores formas de

[17] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[18] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
[19] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[20] *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

evitar el phishing y otras amenazas de hackers. [21] Por supuesto, las empresas que se apresuraron a hacer frente al impacto de la pandemia deberían revisar sus propias medidas de ciberseguridad para asegurarse de que siguen estando al día.

Para ayudar a abordar estas preocupaciones, Domínguez recomendó que la auditoría interna pueda investigar qué protocolos de seguridad se aplican, qué herramientas de prevención de pérdida de datos utiliza la organización, si exige autenticación multifactor y VPN, y si las cuentas se desactivan oportunamente cuando los empleados se marchan.

Las "renuncias silenciosas" repercuten en el cumplimiento de las normas y la ética

"La "renuncia silenciosa" se refiere a una práctica en la que los trabajadores sólo hacen el mínimo de lo que se les exige en su trabajo. Según una estimación de Gallup, este tipo de trabajadores constituyen al menos el 50% de la mano de obra estadounidense. El nivel de trabajadores comprometidos se situaba en el 32%, pero el de los que estaban activamente desvinculados era del 18%. Gallup señala que esto es especialmente problemático en una época en la que muchos trabajos son colaborativos o en la que puede ser necesario dar un paso más para satisfacer las necesidades de los clientes. Y aunque se ha prestado mucha atención a la tendencia a renunciar en silencio, los empresarios deben ser conscientes de que los que renuncian en voz alta, es decir, las personas que expresan activamente y tal vez propagan su insatisfacción, siguen existiendo. .[22]

Esta tendencia puede ser una mala noticia para la productividad, la eficiencia y la retención. Al mismo tiempo, puede tener un efecto negativo en la gestión de riesgos. "La gente no presta tanta atención a lo que debe hacer", afirma Domínguez. Y, como señala *Corporate Compliance Insights* el éxito de un programa de cumplimiento y ética requiere la participación y el apoyo de todos los miembros de una organización. "Cuando se combina una visión relativamente negativa del trabajo con un enfoque de trabajo mínimo viable, los extras en los que confían los profesionales del cumplimiento y la ética para asegurarse de que la gente plantee los problemas a menudo desaparecen", señala. [23]

Lo mismo puede decirse de un programa de gestión del riesgo de fraude. Los empleados pueden estar dando el visto bueno a aprobaciones y transacciones o ignorando anomalías, o pueden plantear una anomalía sólo para descubrir que su siguiente nivel de dirección la ha ignorado porque está renunciando en silencio.

La auditoría interna puede examinar las encuestas de satisfacción de los empleados, los índices de rotación y las entrevistas de salida para hacerse una idea de los problemas en el compromiso de los empleados. Las tendencias recientes pueden compararse con la actividad anterior a la pandemia para entender qué impacto puede haber tenido, dijo Domínguez.

[21] "Organizational Vulnerabilities in a Protracted Work-from-Home Scenario," Savita Nair, ACFE, January 12, 2023.
[22] "Is Quiet Quitting Real?" Jim Harter, Gallup Workplace, September 6, 2022.
[23] "Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions," Lisa Beth Lentini Walker, *Corporate Compliance Insights*, September 14, 2022.

Conclusión

¿A cuánto asciende todo esto? Según la ACFE, las organizaciones pierden cada año un 5% de sus ingresos por fraude, con una pérdida media de 117.000 dólares y de 1.783.000 dólares. Normalmente, las pérdidas por fraude pueden alcanzar una media de 8.300 dólares al mes. Se trata de consideraciones serias para cualquier organización.

Durante y desde lo peor de la pandemia, las organizaciones han recurrido a los auditores internos para ayudar a los responsables de la toma de decisiones estratégicas a reevaluar y mejorar los procesos operativos. Esta práctica debe continuar, especialmente en la evaluación de los controles internos antifraude. El mundo puede haber emergido de la pandemia, pero no necesariamente se ha sacudido de las amenazas de fraude relacionadas con la pandemia.

Desde que comenzó la pandemia, se ha apreciado aún más la contribución que puede hacer la auditoría interna para mitigar o detener el fraude. En el pasado, a menudo se recurría a la auditoría interna cuando ya se había producido un incidente de fraude. Esto está cambiando; ahora es menos probable que las organizaciones esperen a detectar el fraude y esperan atajarlo antes de que se produzcan demasiados daños. Para ayudar a conseguirlo, están involucrando a los auditores internos en conversaciones basadas en la prevención, en otras palabras, pidiéndoles que consideren los controles antifraude antes de que se produzca el fraude, dijo Domínguez. La auditoría interna también está facilitando debates sobre la evaluación del riesgo de fraude y los marcos de evaluación del riesgo de fraude, considerando la frecuencia y eficacia de esas evaluaciones y pruebas de control, y tomando nota de cualquier cambio en el perfil de riesgo actual de la empresa. "En lugar de esperar a detectar el fraude, los auditores internos se están moviendo hacia el lado preventivo", dijo Domínguez.

Acerca del IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin ánimo de lucro que cuenta con más de 230.000 miembros en todo el mundo y ha concedido más de 185.000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite theiia.org.

Disclaimer

El IIA publica este documento con fines informativos y educativos. Este material no pretende dar respuestas definitivas a circunstancias individuales específicas y, como tal, sólo pretende servir de guía. El IIA recomienda buscar asesoramiento experto independiente relacionado directamente con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Copyright

Abril 2023

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad.

Traducción al Español Auspiciada por:
FLAI
Fundación Latinoamericana de Auditores Internos

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101