ANÁLISIS DEL PROCESO DE GESTIÓN DE SEGURIDAD PARA PREVENIR EL FRAUDE EN LAS ORGANIZACIONES

Código Estudiante: 2601065

GERMÁN AUGUSTO PÉREZ LIZCANO

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES,

ESTRATEGÍA Y SEGURIDAD

DIRECCIÓN DE POSGRADOS

ESPECIALIZACIÓN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ D.C., NOVIEMBRE DE 2016

RESUMEN

El fraude en las organizaciones requiere de tiempo para su planeación y por lo general es cometido por personas que laboran en la misma organización, junta directiva, socios y/o accionistas. Generalmente este delito es planificado por personas que poseen niveles educativos altos, con capacidad para mostrar ambientes económicos perfectos, que les permite acceder a situaciones específicas tales como contrataciones, negociaciones, desviación de recursos, falsificación, etc; pareciera que el comportamiento fraudulento se tolera abiertamente y muchas veces que estuviera institucionalizado.

Para los profesionales de la seguridad, resulta de vital importancia dentro de las organizaciones, sin importar la actividad económica, tamaño y ubicación de la organización, tomar todas las medidas necesarias para desarrollar un excelente proceso de gestión de seguridad en la organización para prevenir y detectar el fraude, teniendo en cuenta que es una labor constante revisar el ciclo de seguridad y otros factores desde el nivel estratégico hasta el operativo**,** dado que la implementación de los procesos de seguridad resultan ser en muchos casos insulsos, lo que puede ocasionar grandes pérdidas y mala imagen de la organización.

Donde se exista una actividad económica habrá la probabilidad y el interés por realizar un fraude, situación que debe ser asumida por el profesional responsable de la gestión de seguridad de la organización. La falta de procesos de seguridad efectivos generan un riesgo latente de fraude, considerado como un acto intencional que busca un beneficio ilegal a su autor o un tercero, ocasionando pérdidas económicas, afectación de la imagen y desconfianza de empleados, clientes, proveedores e inversionistas. Por ello resulta trascendental implementar estrategias efectivas tendientes a proteger los recursos y/o activos de la organización identificando las diferentes formas que adoptan los delincuentes para lograr los desfalcos, entre otras actividades, analizando el triángulo del fraude y la aplicación de procesos adecuados para minimizar el riesgo.

Resulta importante para el proceso de gestión de seguridad en una organización, el reclutamiento y la selección de personal, en ellos se deben aplicar una serie de técnicas como son la entrevista, pruebas de conocimientos, pruebas sicométricas, de personalidad y técnicas de simulación, de tal forma que se haga una evaluación que permita atraer los mejores talentos y en especial que la organización pueda mejorar. Adicionalmente, sirve para detectar posibles personas que llegan con intenciones de generar fraudes, de ahí la importancia de hacer una selección siguiendo todos los pasos.

Palabras clave: delito, fraude, gestión, organización, proceso, riesgo, seguridad.

ABSTRACT

Fraud in organizations requires time for planning and usually committed by people working in the same organization, board of directors, partners and / or shareholders. Generally this crime is planned for people who have high educational levels, capable of displaying perfect economic environment, which allows them to access specific situations such as contracts, negotiations, diversion of resources, forgery, etc; it seems that fraudulent behavior is openly tolerated and often she was institutionalized.

For security professionals, is vital in organizations, regardless of economic activity, size and location of the company or organization, take all necessary measures to develop an excellent process safety management in the company to prevent and detecting fraud, considering it is a constant work reviewing cycle safety and other factors from the strategic level to operational since the implementation of security processes are in many cases be insipid, which can cause great losses and bad image of the organization.

Where economic activity will promote the likelihood and interest in carrying out a fraud, a situation that must be assumed by the person responsible for managing enterprise security professional. The lack of processes of effective security companies generate a latent risk of fraud, considered as an intentional act that seeks an illegal benefit to its author or a third party, causing economic losses, image and confidence of employees, customers, suppliers and investors . It is therefore crucial implement specific programs effective strategies to protect resources and / or assets of the organization identifying the different forms they take offenders to achieve embezzlement, among other activities, analyzing the triangle of fraud and implementing processes to minimize risk.

It is important for the process security management in a company, the recruitment and selection of personnel, they should apply a number of techniques such as interviews, knowledge tests, psychometric tests, personality and techniques of simulation, so that an evaluation to attract the best talent and especially that the company can better be done. In addition, it serves to detect people who come with the intention of generating fraud, hence the importance of making a selection following all the steps.

Keywords: crime, fraud, management, organization, process, risk, security.

INTRODUCCIÓN

A lo largo de la historia, el fraude ha sido partícipe de múltiples escándalos a nivel mundial, entre los que se podrían mencionar se encuentran presidentes, ministros, políticos, altos cargos, niveles medios y bajos en las organizaciones de todo el mundo. En ciudades como Londres, hace 50 años resultaba difícil aceptar el fraude como problema, para ello se creó un departamento exclusivamente para investigar los casos crecientes de fraude y así en otras ciudades. A pesar de ello, solo hasta finales de los años 60 admitieron que el fraude circundaba por todo el país y crearon la división contra el fraude, dedicado exclusivamente a casos de fraude a gran escala y a las organizaciones.

El fraude es un delito que se da en mucha frecuencia, por el que gran parte de las personas reaccionan en algunos casos con violencia, pero mientras esto sucede las pérdidas a las que se ven expuestas las organizaciones son mayores por los casos en que no se realizan las investigaciones. El fraude se puede definir como el acto deliberado de abuso de confianza que valiéndose de engaños o capitalizando errores, se realiza para obtener un beneficio sin el consentimiento de la organización victimizada. Generalmente, se presenta en personas que han sido de mucha confianza y cuesta hacerse la idea de quien ha cometido el fraude.

Las organizaciones han tratado de mejorar los procesos de gestión de seguridad con el ánimo de contribuir a prevenir este delito, además de estar motivadas por las grandes pérdidas, merece especial atención los riesgos a los cuales se ven expuestos por los comportamientos de empleados desleales, corruptos, bandas delincuenciales y otros agentes que constantemente desfalcan las organizaciones en forma oculta. Tal comportamiento parece tan imperceptible, que difícilmente se levantan sospechas de los empleados u otros agentes deshonestos.

Tal parece que uno de los problemas que enfrentan las organizaciones para prevenir el fraude, se remiten a la falta de procesos efectivos en la gestión del proceso de seguridad. Aunque sea imperceptible el comportamiento de los defraudadores, es necesario que los profesionales responsables de la seguridad asuman procesos efectivos desde el mismo momento en que se vincula una persona a la organización. ¿Será posible mitigar el riesgo de fraude en las organizaciones mediante el proceso de seguridad?

Con el presente trabajo se busca analizar el proceso de gestión de seguridad en una organización, para que contribuya a prevenir la comisión de fraudes desde el proceso de reclutamiento hasta la terminación del contrato del trabajador, con base en una efectiva evaluación de riesgos, implementando el ciclo de seguridad, aplicando las técnicas de entrevista e investigación, mecanismos de control, auditorias de los procesos de la organización, reclutamiento y selección de personal. Para prevenir, detectar, investigar y perseguir los fraudulentos, se requiere del concurso y respaldo de los altos directivos de la organización; son estos el soporte del responsable del proceso de seguridad para mitigar las pérdidas por este hecho.

En las organizaciones, existen aún directivos que siguen siendo muy ingenuos o bienintencionados, que destinan pocos recursos a la seguridad, en ocasiones por la falta de recursos, otras veces por la incredulidad en los procesos de seguridad y desafortunadamente son sorprendidos. Los delincuentes, contrario a estos directivos, si actúan con dedicación de tiempo para hacer los planes y cometer el delito. Ante estas situaciones de fraude, las personas honradas no sospechan, acá se puede decir que el mal triunfa cuando la gente de bien no actúa.

Las teorías fundamentales y clasificaciones del fraude son importantes para entender sus causas principales, ayudarán a comprender los mecanismos que conllevan concretamente a su ejecución. Para determinar las causas que estimulan este delito, se citarán conceptos sobre la motivación delictiva, la posición de la organización y otras teorías que complementan el análisis, tales como la teoría de la variedad de oportunidades, de ocultación, de desviaciones y la teoría de la colusión mínima. Las técnicas de detección serán objeto de observación, su finalidad y objetivos afianzaran un adecuado proceso de gestión de seguridad.

ELEMENTOS DEL FRAUDE

Se requiere tener presente para lograr un mejor entendimiento del fraude en las organizaciones, algunas teorías que permitirán comprender los mecanismos que conducen a que se sucedan con cierta frecuencia y como reto de prevención para el profesional de seguridad.

Fraude empresarial

El fraude puede definirse como aquel comportamiento por el que una persona trata de aprovecharse de otra sorprendiéndola en su honradez (Comer, 1993, p17). Se podrían mencionar múltiples definiciones para no emplear términos técnicos ni jurídicos, interiorizando en el ser de las personas que por diferentes motivos buscan un beneficio personal, sin dar mayor importancia a la honradez. West (1993) afirma:

> El fraude puede considerarse como un delito distinto, en realidad lo es, porque es posible que quien haya cometido ese delito sea una persona a quien conoce y confía mucho en ella, a la victima le cuesta creer que aquel que cometió el fraude es la persona que menos esperaba. (p.12)

Es preciso mencionar según el autor (West 1993), no todo aquel que comete una acción que pueda interpretarse como fraude esta obrando mal. Muchos autores de estos delitos están convencidos de que actúan de esta forma para generar un bien común, por ejemplo ocultar pasivos o activos en un balance para pagar menos impuestos o dividendos mas bajos, a sabiendas que están cometiendo una falta grave, pero su intencionalidad no es beneficiarse ni desfalcar la organización. Por lo anterior, es difícil decidir qué medidas se van a seguir cuando se descubre que alguien ha cometido un fraude.

Para la Asociación de Examinadores de Fraudes Certificados [ACFE], 2012 en el sentido mas amplio, el fraude puede abarcar cualquier delito para ganancia que utiliza el engaño como su principal modus operandi. Mas específicamente se define por el Black´s Law Dictionary como: “una declaración falsa a sabiendas de la verdad o la ocultación de un hecho material para inducir a otro a actuar en su detrimento”. Es decir que la persona actúa en forma deliberada y consciente para obtener beneficios de un tercero, mediante la astucia y el engaño.

Factores que ocasionan el fraude en las Organizaciones

A diario se escuchan las noticias de la radio, se ven en los noticieros mas populares y aún los menos sonados a nivel nacional y regional, en los periódicos, en las redes sociales, en los pasillos de las oficinas, en la calle en innumerables formas y medios; para enterar al común de las personas y poner al descubierto las mas complejas malversaciones y fraudes organizacionales. Lo que muchas veces no comprendemos o simplemente no interesa, son las motivaciones o circunstancias que aquellos protagonistas de la noticia tuvieron para llevar a cabo tal fin.

Para la ACFE el triangulo del fraude es un modelo para explicar los factores que hacen que una persona cometa un fraude empresarial; consta de tres componentes que llevan a cometer un acto fraudulento. La percepción de la necesidad económica (Motivación), representado en la presión y tal vez la mas influyente para desencadenar todas las iniciativas. La persona tiene problemas financieros y le surge la necesidad de solucionarlos por medio de la ilegalidad, tales como robar efectivo, falsificar estados contables, como una forma de resolver sus problemas, este puede ser personal o laboral.

Según la ACFE algunos ejemplos de presión para motivar a la persona a cometer el fraude pueden ser: imposibilidad de pagar facturas, adicción a las drogas o juegos, necesidad de alcanzar objetivos de productividad, deseos de mejorar el estatus (una casa mas grande, un mejor vehículo), etc.

La segunda forma del triángulo del fraude de acuerdo con la ACFE, hace referencia a la oportunidad, que define el método para llevar a cabo el fraude. En esta parte, el defraudador debe buscar la forma de no ser descubierto, toda la confianza que han depositado en él, es empleada para no levantar sospecha de su objetivo delictivo (abuso de la confianza). La persona que decide cometer un fraude debe actuar con guante blanco, es decir, debe hacerlo tan bien hecho que pueda solucionar todas sus necesidades sin que sea descubierto, ya que por sus posición perdería el estatus que tiene en la organización.

La tercera parte del triángulo se llama racionalización, normalmente estas personas no tiene pasado delincuencial, se ven así mismo como normales, honestas que les han sobrevenido situaciones difíciles y necesitan solucionarlas. Por ellos deberán justificar sus actos con algunas

frases para cometer sus actos fraudulentos; “solo estoy tomando el dinero prestado”, “me lo deben porque me lo merezco”, “es porque mi familia lo necesita”, “no me pagan lo suficiente por el trabajo que hago”.

Según Comer (1993), existen diferentes teorías acerca de la motivación delictiva; quedaría muy fácil pensar que la sociedad no puede hacer nada para reformar aquellos ladrones que nacen sin escrúpulos. En el caso de los delincuentes organizados que operan como mafias, ejecutan sus delitos sin utilizar la violencia, en especial en los fraudes crediticios o de inversión y blanquear los fondos por medio de empresas que operan legalmente, así mismo, es frecuente el uso de amenazas contra ciudadanos, cómplices o empleados de las organizaciones víctimas del delito para crear oportunidades.

Pero también existen los delincuentes primerizos. Estas personas rara vez son atrapadas en su primera acción. Según Comer y otros investigadores criminalistas que han comprendido las motivaciones que empujan a las personas no obreras a cometer un fraude, han tenido resultados diversos. La teoría de la asociación diferencial, afirma que el comportamiento delictivo se aprende por la asociación con quienes definen dicho comportamiento en términos favorables y por el aislamiento de los que lo definen como desfavorable. Para cada situación, adoptan ese comportamiento tan solo si el peso de las definiciones favorables son superiores a las desfavorables.

En la teoría de la variedad de oportunidades según Comer, todas las personas tienen la oportunidad de cometer un fraude, bien sea contra su organización, contra clientes y proveedores, contra terceros o contra organismos oficiales. En esta teoría intervienen tres factores: acceso a los locales, bienes, cuentas y sistemas informáticos, experiencia de práctica o destreza para encontrar la oportunidad y explotarla y la disposición del tiempo necesario para planear y ejecutar el fraude. Realmente en la mayoría de los casos de fraude que se conocen, esta teoría tiene gran relevancia y tal vez, es la que mas argumenta los actos delincuenciales.

Muchas organizaciones hubieran podido evitar el fraude si tan solo dedicaran tiempo para verificar los procesos de selección e incorporación, pues en la medida que ocupan cargos críticos las personas, quiebran la confianza a aquellas que la han depositado y permitido el acceso a sus puntos más neurálgicos. No se verifican antecedentes, no se hacen visitas domiciliarias, aspectos

tan sencillos y comunes, pero que se omiten por negligencia.

Cometer fraude en una organización por parte de personas que tienen la intencionalidad de beneficiarse en forma ilegal, afectando los bienes de otros, resulta sencillo. La persona que va a cometer el delito, emplea mecanismos de confusión antes, durante o después, de tal forma que le facilite ocultar o ayudar a su ejecución. Comer (1993) afirma:

> La confusión no modifica el hecho de que, cada vez que se sustrae un activo real, se genera una pérdida, o mas precisamente, un cargo contra el patrimonio neto. Se trata de una carencia que solo puede cubrirse si se devuelve ese activo o uno equivalente. La ocultación desvía la atención de la carencia; disfraza, confunde o retrasa su descubrimiento o impide la identificación del autor. (p.43)

Son premisas que el delincuente emplea con el fin de no levantar sospechas y hacer creer que todo anda bien, en el entendido de no permitir detectar el engaño para explotar la oportunidad sin vacilación, extenderla e intensificarla.

El falseamiento según Comer hace parte de la familia de la ocultación, es equivalente a la manipulación de registros. Hace referencia a un engaño que afecta las realidades físicas, comerciales o personales y se puede hacer antes, durante o después del acto. La capacidad del falsificador depende en gran parte del contacto que se tenga con la víctima, el conocimiento hacia ella y la credibilidad y codicia que se tenga; pueden generar actos de falsedad como inflación de existencias, interferencias en aparatos de control como básculas, falseamiento de realidades personales (suplantación).

Por otra parte, la colusión aporta como teoría un elemento importante de los fraudes. De acuerdo con Comer, se produce cuando se proporcionan las oportunidades, recursos o técnicas para que se pueda llevar a cabo el fraude (colusión mínima); se requieren conocimientos especializados y son manipulados por altos niveles y cuando se comparten los beneficios obtenidos por el fraude menos cualificado entre el máximo de personas (fraude institucionalizado). De esta forma se podrán tener mas argumentos a la hora de iniciar una investigación .

Para el caso de la colusión máxima generalizada, los fraudes no requieren de un nivel alto de capacitación, estos se dan en organizaciones grandes y es cuando el delito está generalizado o institucionalizado entre todos los trabajadores, por ejemplo en el sector de la panadería, ferreterías, talleres, distribuciones de leche, etc. Todos están subidos bajo la misma motivación, todos se ponen de acuerdo y esto dificulta la detección y el riesgo de que se delaten unos a otros.

Clasificación del fraude

Teniendo en cuenta las teorías de Comer, para clasificar el fraude se va a tomar como base la teoría de la variedad de oportunidades, fundamentada en la fuente originaria del riesgo de fraude, es decir, en la forma como la organización ha dado manejo a los trabajadores respecto a las funciones que desempeñan y en la medida como sus controles han surtido efecto para que estos no aprovechen las oportunidades que el mismo sistema le permite.

En ese sentido, el delincuente interno, que ha sido vinculado a la nómina de la organización, se beneficiará de los bienes de la organización por el mismo desarrollo de trabajo diario. Teniendo en cuenta su dinámica tendrá acceso a equipos, existencias, documentos, registros, facturas, etc. Entre mayor sea el nivel, mayor será el acceso a registros contables, a diferencia del que tiene menor nivel, tendrá mas acceso a existencias, es decir, refiriéndose al operario. A este tipo de defraudador, se le facilita modificar equipos mecánicos como básculas y medidores, es decir tanto el trabajador de alto y menor nivel tienen las mismas oportunidades para manipular.

Por otro lado, los delincuentes externos, que no tiene nada que ver directamente con la organización, es decir, proveedores y clientes y las personas que para estos trabajan, tiene también acceso a determinados bienes, registros e información, dependiendo de la relación que se tenga con la organización. Estas personas no tienen tanta oportunidad como los empleados internos, pero si es mayor su acceso que otros que no tienen nada que ver con la organización, es decir si va a ver una oportunidad de fraude en el transcurso de sus relaciones.

Según Comer a estas dos, se suman los delincuentes organizados. Cuando hay personas involucradas desde afuera de la organización con trabajadores internos, constituyen un riesgo mas incontrolable aun, pues sus ocultaciones y oportunidades ya pasan a otro plano como puede ser la extorsión. Podría entonces, hacer referencia a los fraudes por manipulación es decir de

carácter contable, ya que hay modificaciones en los registros y por alteración en un dato físico, personal o comercial, es decir de carácter extracontable.

Para entender un poco mas lo anterior, se tiene la siguiente tabla.

Tabla 1.

Categorías de fraude según la fuente del riesgo y la vía de ocultación

Fuente y tipo	Vía de ocultación			
	Por hurto o latrocinio (sin ocultación) 1	Por falseamiento (realidad falsificada) 2	Por manipulación (cuentas) 3	Por extorsión (fuerza) 4
A. Interno: por directivos	A1	A2	A3	AB4
B. Interno: por trabajadores manuales	B1	B2	B3	
C. Externo: por personas participes en contactos empresariales	C1	C2	C3	
D. Externo: por oportunistas	D1	D2	D3	CDE4
E. Por colusión (terceros): organizado	E1	E2	E3	

Nota: Adaptada de la tabla 2.2 (pág. 49), por M. Comer, 1993, Buenos Aires. McGraw Hill por editora Roca S.A.

En la categoría A1, interno-personal directivo-hurto, hacen referencia a los fraudes sencillos cometidos por empleados de la organización y que tienen acceso limitado a bienes físicos. Por ejemplo aquellas personas que ocupan su tiempo exclusivo de trabajo para tratar negocios personales, toman servicios públicos como el teléfono para hacer llamadas diferentes a las de tipo laboral. En estos casos la ocultación no es necesaria debido a que resultan ser intangibles y no existe nada que ocultar. Suelen ser sustracciones al que se tiene accesos regularmente cuya perdida puede pasar desapercibida.

Sin embargo en la categoría A2, donde se involucra de manera interna personal directivo con falseamiento, se refiere a los fraudes cometidos por empleados de la organización pero con acceso a los registros contables y el control de los mismos. Contrario a lo anterior, tiene acceso limitado a los bienes materiales y equipos de medición y control. Posterior a ejecutar la sustracción para poder ayudar a ocultarla, se hacen falseamientos de una realidad personal, física o comercial. Por ejemplo aquellos que alteran los indicadores de las máquinas para beneficiarse de las ganancias que no se contabilizan. Por lo general el falseamiento ayuda a alejar las sospechas del fraude.

Otra clasificación de fraude según Comer, se da por personal directivo en forma interna con manipulación, con acceso y control de registros contables y acceso limitado a los bienes materiales y equipos de medición. Después de la sustracción o falseamiento realizan la manipulación para ayudar a su ejecución. Para el ejemplo se puede citar a un empleado que comienza a retrasar los informes diarios de ventas, esto con el fin de beneficiarse de dinero recibido y arreglándoselas para cubrir las faltas cometidas. Estos fraudes pueden ocurrir a corto o largo plazo pero cuya intención es acceder a dinero y a los registros contables. Por lo general, se hacen fraudes de gran magnitud.

En la categoría B1, donde se realiza el fraude en forma interna por parte de trabajadores manuales con la intención de hurto, tiene acceso generalizado a bienes materiales y equipos de medición y ejercen su control, su acceso a cuentas y registros es limitado. En este caso la pérdida no es reconocida y las sospechas serán mínimas, no hay ocultación ya que este carece de vías para hacerlo. Es el caso de los trabajadores que se llevan las herramientas de trabajo para la casa, tal vez no significará en gran proporción las pérdidas de la organización pero si deja al descubierto la intención fraudulenta de los trabajadores.

Por ultimo, la categoría AB4, se realiza en forma interna por personal directivo o trabajadores manuales, encaminados a la extorsión. Estos actos requieren de fuerza y chantaje, esto quiere decir que se eliminan las limitaciones que hay de oportunidades de sustracción y ocultación. Normalmente las amenazas las dirigen hacia los propietarios de las organizaciones que son quienes pueden tomar las decisiones y no necesitan intermediarios, lo que les ocasionaría mas trabajo.

La figura que se muestra a continuación permite aclarar lo que se ha manifestado anteriormente para la comisión de un fraude, donde la oportunidad y la motivación juegan un papel importante.

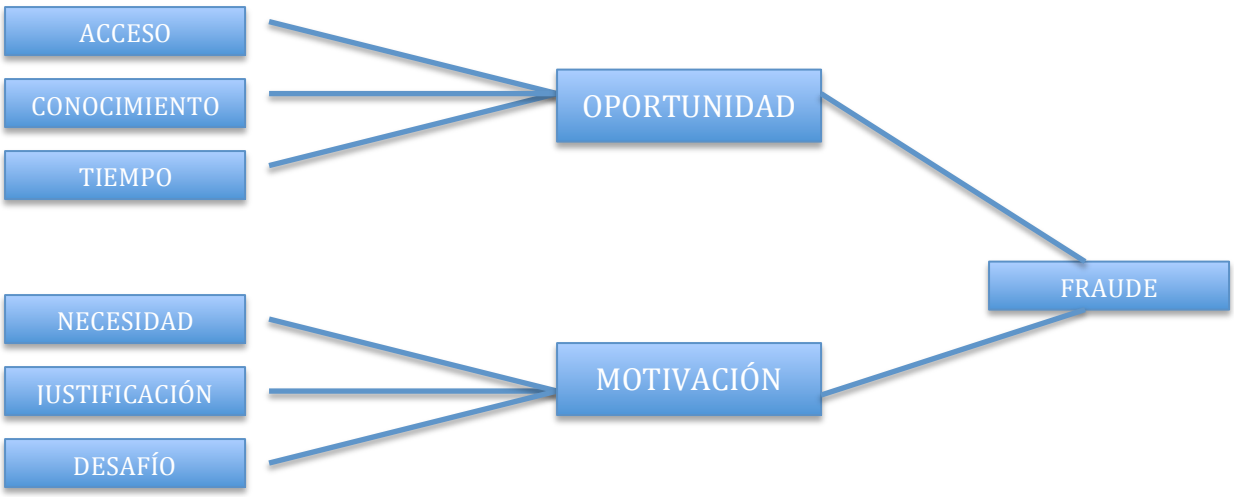

Figura 1. Factores decisivos de un fraude. El fraude en la empresa, Deusto 1993.

Para resumir, se puede decir que el fraude en las organizaciones es el resultado de una combinación de factores motivantes y de situaciones, donde el punto crítico es la oportunidad. Los oportunistas desaparecerían si la detección es efectiva, si los procesos de gestión de seguridad son acatados con máximo detalle, no solo por los responsables que la organización designe sino por todos los procesos de la cadena de suministro.

Fraude en las organizaciones

El delito que las organizaciones más temen en los países desarrollados según Estupiñan (2006), es el fraude, incluso frente a crímenes como el terrorismo, el secuestro, el sabotaje y el hurto. La sensación entre los empresarios de los diferentes sectores y países es de mucho riesgo, este delito parece no tener control y parece estar cogiendo fuerza ayudado en gran parte por una mayor complicación en los negocios debido a la globalización, dificultades con las diferentes culturas y un mayor uso de tecnologías como el internet. Los defraudadores no están siendo controlados por las organizaciones, específicamente en las áreas de sistemas y de compras.

Los fraudes mas comunes son los que hacen por medio de los computadores y tarjetas de crédito, seguido de robo de efectivo, fraudes en tesorería, impuestos, seguros o por negociación

directa, entre otros que se mencionarán mas adelante. Estos fraudes pueden prevenirse si se adopta un correcto proceso de gestión de seguridad, pues en la mayoría de los casos la actitud frente al fraude es reactiva. Se estima que más de la mitad de los fraudes de la organización son descubiertos por coincidencia, es decir por personas externas, accidentes o cambios de la administración, entre otros factores.

La falta de conocimiento de las directivas acerca de las operaciones principales y de menor grado, normalmente tienden a delegar la responsabilidad de implementar controles para prevenir fraudes de gran dimensión. Muchos determinan que los auditores son los responsables de detectar fraudes en las tareas que a ellos les corresponde, pero no siempre es así y tampoco están dispuestos a pagarles mas por la responsabilidad transferida. Los gerentes son los directos responsables de asumir la responsabilidad o verificar si aquel que tiene la responsabilidad delegada no lo está haciendo bien.

Según Estupiñan (2006), las empresas que han tenido algún tipo de fraude no los han denunciado. Esta mínima parte que no denuncia, no lo hace por temor a que se afecte su imagen, los costos que le podría implicar, la incertidumbre por los resultados. Las organizaciones optan por quedar con el problema y no toman las medidas que le son mas convenientes para que no se repita, asumiendo el riesgo y lo que es peor generando más pérdidas a la organización, son actitudes que merecen ser revisadas.

Algunas de las estrategias que emplean las organizaciones contra el fraude según Estupiñan son la capacitación de los empleados, especialmente los que tiene manejo de sistemas y cargos críticos que más adelante se definirá; la delación de los empleados de la misma compañía o información anónima, se puede realizar con líneas telefónicas y personas de la organización que actúan por fuera; el intercambio de información entre compañías; diseño de políticas claras de prevención, detección e información de casos, es decir adoptando sistemas de control adecuados; aplicación de las leyes sencillas de fraude; controles internos efectivos; investigar los indicios de fraude que se descubren con auditorías. (2006, p.374)

El fraude ha ido evolucionando, para ello se analizan las tendencias que han favorecido su desarrollo. Estupiñan (2006) afirma:

> Mayor presencia del crimen organizado, se trata de pequeñas mafias, dos o tres individuos, cuya actividad es dedicarse a encontrar objetivos fáciles. En efecto, el crimen organizado podría ser el responsable de la mayoría de los fraudes externos, recordando que estos solo pueden ser exitosos con la participación interna de un empleado corrupto. Mayor corrupción de empleados, se refiere al empleado que, por una serie de razones éticas y morales, decide que es mas fácil ganar dinero de otra forma, ya sea en colaboración con el crimen organizado o por su propia iniciativa. La aparición del tecnofraucata, este termino define a aquella gente bien preparada, muy conocedora de los negocios y de los mercados, que considera que lo importante es ganar dinero a costa de lo que sea. Desarrollo de técnicas mas asequibles de falsificación, la tecnología ha permitido lograr verdaderas maravillas que no tiene aquel aspecto artesanal de antaño. Más oportunidades de fraude por errores operativos, la necesidad de crecer y de ganar nuevos mercados, ha llevado a algunas organizaciones a reducir erróneamente los gastos. Lanzan nuevos productos sin realmente tener buenos procedimientos operativos, ni contar con una buena formación para los empleados que van a vender, administrar y procesar productos. (p.376)

A medida que la ciencia evoluciona y los mercados varían, los delincuentes internos y externos van modificando su modus operandi, así mismo las organizaciones deben estar en continuo cambio para enfrentar el fraude.

Las modalidades de fraude de acuerdo a Estupiñan, se pueden resumir de la siguiente manera: manejo circulante, ingenieros contables, manejo indebido de los activos, uso indebido de claves de acceso, manejo de títulos, facturas o documentos negociables, evasión y elusión de impuestos, combinación de modalidades. Además, las personas con intención de defraudar cometen otros tipos de actos fraudulentos, como falsificación de documentos, sustracción de información, sustracción de bienes, los cuales deben ser contra restados por los responsables de la seguridad.

Fraude en Colombia. De acuerdo a las cifras de EY Conductas corporativas indebidas – consecuencias individuales (2016) en la Encuesta Global de Fraude; las amenazas del cibercrimen, el financiamiento del terrorismo y la corrupción han presionado a los gobiernos para que tomen acción y a las organizaciones para analizar los riesgos y mitigar el fraude. En este

estudio se encuestaron mas de 3000 ejecutivos de 62 países, en Colombia fueron encuestados mas de 50 empresarios de diversas industrias, quienes reconocieron que es necesario investigar bien con quien se hacen los negocios.

Los resultados reflejan que a pesar de los esfuerzos, la búsqueda de herramientas para lograr mayor transparencia y presión sobre las organizaciones, la percepción de corrupción y de fraude no disminuye, siendo aun mayor que la encuestas de 2014, donde el 80% de los empresarios colombianos encuestados considera que la corrupción y el fraude están presentes en Colombia. Además, los responsables de estos actos de fraude de economías emergentes no están respondiendo, el 48% considera que así los gobiernos quieran enjuiciar a estas personas no son lo suficientemente efectivos.

El 30% de los ejecutivos encuestados según EY, estarían dispuestos a ejecutar bajo presión actos no éticos con el fin de justificar el negocio, haciendo pagos indebidos o falsificar resultados financieros, esto por encima de países del resto de Sur América, lo cual implica que se tomen medidas de ética proactivas tendientes a implementarlas en los procesos y que sean de conocimiento de la alta gerencia.

Siendo así, los directivos de las organizaciones deben propender por fortalecer sus procesos de seguridad, con capacitaciones, tecnología, concienciación de las personas que lideran los procesos de toda la organización no solo el proceso de seguridad o de recursos humanos, o a quien tengan delegado para gestionar este tipo de actos delictivos. La seguridad debe ser holística y deben comprometerse todos los trabajadores, con medidas efectivas y protocolos bien establecidos, de tal manera que no se improvise ante las intenciones de fraude, pues en todo momento es latente.

Legislación del fraude en Colombia

A pesar de los diferentes obstáculos jurídicos para facilitar al proceso de seguridad cumplir con su tarea, aun cuando los que cometen los fraudes son personas de la entera confianza de sus directivos y han trabajado por años en una organización incluso cuando sin tener un tiempo estimado en la organización son conducidos por quienes si llevan un tiempo considerable. Las normas jurídicas en ocasiones, confunden a los encargados de administrar justicia, por ello se

debe establecer con claridad y con suficientes pruebas los actos, para que de esta manera exista coherencia entre los actores de la investigación, producto de un proceso efectivo.

Se hace necesario realizar un seguimiento prudente, exacto y coordinado entre los que se involucran en la comisión del fraude. Estupiñan (2006) afirma:

> Una vez se comprueben los hechos indicadores, la premisa que prueba la acción conduce necesariamente a un resultado que se conoce como hecho indicado. El conjunto de los hechos indicados que guarden unidad, convergencia, gravedad y conexidad, será la prueba indiciaria que hará parte de la valoración jurídica de la investigación. (p. 379)

Lo anterior requiere que las pruebas objeto de investigación, se encuentren alineadas con el proceso desde su origen, con las políticas de la organización y las leyes establecidas, lo cual facilita su investigación.

Tabla 2.

Panorama penal internacional del delito

Normatividad Internacional y tipificación de los delitos y el fraude	
Marco general de delitos tipificados en los códigos penales	
Testaferrato Lavado de dinero y activos Enriquecimiento ilícito Contrabando Receptación Encubrimiento Complicidad Competencia desleal Dumping Usura Evasión de impuestos Absorción Desviación de crédito Captación masiva indebida Reserva bancaria	Prevaricato Peculado Cohecho Concusión Colusión Contratación indebida Trafico de influencias Abuso de autoridad Abuso de confianza Usurpación Hurto Estafa Extorsión Chantaje

Clasificación del delito
1. Contra la fe y la administración pública 2. Contra el patrimonio natural y económico 3. El delito informático

Nota: Adaptada de la (pág. 49), por R. Estupiñan, 2006, Bogotá. Ecoe Ediciones.

En Colombia existen unas normas rectoras para el tema en referencia relacionado con delitos contra el patrimonio económico, de gran ayuda para encausar las conductas de las personas involucradas en el fraude. De acuerdo a (Ley 589, 2000) algunos de estos importantes artículos contenidos en el titulo VII son el Art. 239 hurto; el art 246 estafa; el art 248 fraude mediante cheque, art 249 abuso de confianza; art 251 de las defraudaciones; art 252 aprovechamiento de error ajeno o caso fortuito; art 254 sustracción de bien propio; art 257 Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones; art 258 Utilización indebida de información privilegiada.

GESTIÓN DEL RIESGO EN EL FRAUDE

Para que el responsable del proceso de gestión de seguridad en una organización tenga éxito, indudablemente la gestión del riesgo se convertirá en el baluarte de prevención del fraude en todos los procesos, desde la alta dirección hasta el nivel operativo.

Riesgos generados en la organización

Es de vital importancia para el proceso de gestión de la seguridad, tener en cuenta la gestión del riesgo empresarial que Mejía (2006) define: "como la posibilidad de ocurrencia de cualquier evento (interno o externo) que pueda afectar una organización, ocasionándole pérdidas que disminuyan la capacidad para lograr sus objetivos estratégicos y generar valor para sus accionistas, grupos de interés y beneficiarios". Lo anterior implica un análisis en todos los procesos y en consecuencia darle el manejo adecuado.

El riesgo al fraude se encuentra presente en todas las actividades y procesos que se desarrollan en una organización, aunque resulta difícil eliminarlo, si es posible mitigarlo mediante la implementación del ciclo de gestión del riesgo que mas adelante se explicará, Mejía (2006) hace referencia a que las empresas pueden verse inmersas en una serie de riesgos propios, específicos

e individuales, entre los que se encuentra el riesgo de reputación. Se da cuando se desprestigia la organización y puede ocasionar la pérdida de credibilidad y confianza del público por fraude, entre otras por la conducta irregular de empleados, falta de capacitación, errores en los procedimientos, etc.

Existen otros riesgos que tienen que ver con el fraude en las organizaciones. El riesgo estratégico y operativo. Según Mejía (2006), el riesgo estratégico se da cuando se generan pérdidas ocasionadas por malas decisiones del nivel directivo, errores de diseños en los procesos, asignación de recursos y la ineficiencia en la adaptación de los cambios constantes del entorno empresarial. El riesgo operativo hace referencia a las pérdidas ocasionadas en la ejecución de los procesos, bien sea por los modelos implementados o fallas de las personas.

Todas las organizaciones son diferentes, tienen misiones y objetivos que alcanzar que se diferencian según su razón social; pero a todas las hace común los riesgos que deben enfrentar dependiendo de las circunstancias. Los riesgos pueden ocasionarse en cualquier parte del proceso y se le debe dar la misma importancia ya que representa pérdidas materiales y de la imagen si no se le da el tratamiento adecuado. Para la gestión de riesgo se tendrá en cuenta el contexto, la valoración (la identificación, evaluación, análisis), el tratamiento, el monitoreo y la comunicación.

Los procesos de una organización en su totalidad deben estar comprometidos con el manejo del riesgo, no solo es responsabilidad del proceso de seguridad o de recurso humano de la organización. Los cargos y funciones deben estar definidos con la administración del riesgo, con el propósito que cada trabajador se comprometa y se pueda garantizar en forma integral en todos los procesos desde el nivel directivo/estratégico hasta el nivel operativo. Se debe conformar un comité de riesgos y debe ser liderado desde el gerente con políticas definidas de los riesgos.

Administración del riesgo al fraude

La organización según Mejía (2006), debe tener un responsable de la gestión del riesgo dependiendo del tamaño y la complejidad de la organización, este debe coordinar todas las acciones con los responsables de cada proceso que la conforman. La persona responsable depende directamente de la alta dirección con el fin de tener todo el apoyo y respaldo de sus

acciones, tanto en lo económico como en su implementación en los demás cargos. La alta dirección debe comprometerse indiscutiblemente para que le de valor al proceso de seguridad, pues en últimas las consecuencias se verán materializadas en costos.

Para la gestión es necesario que el profesional de seguridad manifieste a la alta dirección la importancia dentro del proceso, que sea visto como una inversión. Para ello la seguridad debe estar basada en la prevención del fraude, con suficiente capacidad de análisis. Se deben gestionar para evitar ocasionar un daño por falta de inversión. Si la organización realiza una detallada recolección de información a través de encuestas, entrevistas, revisión permanente de la documentación con herramientas que permitan la exploración dentro de la organización, seguramente se podrán desarrollar las etapas de la administración del riesgo y de esta forma prevenir el fraude con seguridad física, de personal y en la información.

En la siguiente figura se puede apreciar las etapas del proceso de administración del riesgo, con el fin de ser tenido en cuenta en la gestión del riesgo del fraude en las organizaciones. El profesional se seguridad debe aplicarlo para su prevención.

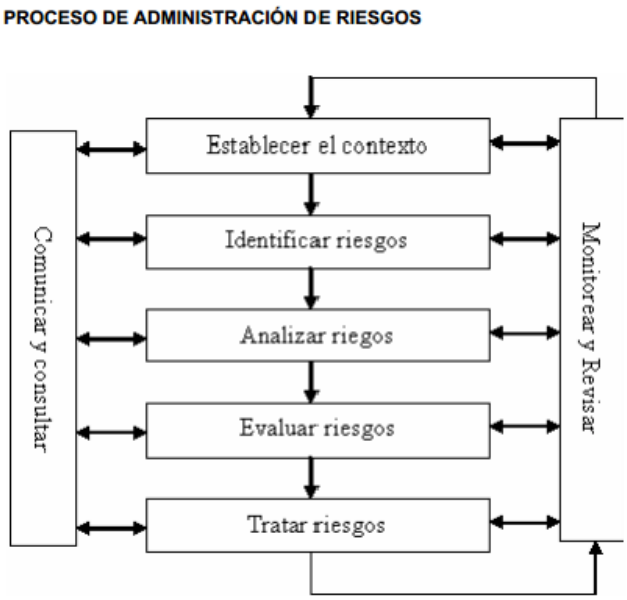

Figura 2. Etapas en la administración del riesgo. Gestiopolis 2010

Para la aplicación de las etapas del proceso de administración del riesgo al fraude, como se mencionó anteriormente, se requiere conocer la organización, su naturaleza, la caracterización de

las instalaciones, tener clara la misión, los procesos que se desarrollan, las entradas y salidas en el contexto interno y externo (dentro de la organización y en el mercado respectivamente). Es fundamental tener claro el alcance, la DOFA de la organización y todas aquellas amenazas a lo largo de la cadena de suministro; lo anterior debe estar documentado.

Basados en la International Organization for Standardization [ISO 31000] (2009), la valoración del riesgo significa determinar el tamaño y cantidad del riesgo actual y por consiguiente deberá ser tratado y este depende de la identificación, análisis y evaluación. Para la identificación se establecen los activos críticos operacionales y esenciales para la continuidad del negocio, analizar qué le podría pasar a esos activos y como afectaría la continuidad el negocio. Conocer el contexto podría ayudar a determinar cuáles son los activos críticos y como contribuyen al cumplimiento de los objetivos y a la operación, el intercambio de información con las partes interesadas y la experiencia aportan para determinar como afectaría los activos.

La identificación de los riesgos permite según Mejía (2006) poner al descubierto situaciones y tomar conciencia de las posibilidades y peligros de fraude. Sería oportuno formularse algunas preguntas que permiten la identificación de riesgos. ¿Qué puede ocurrir? ¿Cómo puede suceder? ¿Quién puede generarlo? ¿por qué se puede presentar? ¿Cuándo puede ocurrir?. Algunos riesgos son de fácil identificación por ser visibles, pero existen otros que son imperceptibles o que no son tenidos en cuenta por parecer sin importancia. Se debe tener en cuenta que si un riesgo no es identificado, difícilmente podrá ser administrado. Existen diferentes métodos para identificar riesgos, como el método Hazop, el árbol de fallas, el árbol de eventos.

Posterior a la identificación del riesgo, se determina qué tan representativo y que tan probable es para la organización el riesgo, al respecto Mejía (2006) dice:

> Para ello se realizan dos análisis: uno sobre la probabilidad de ocurrencia del riesgo (frecuencia) y otro sobre el impacto o potencial de pérdida que puede causar en caso de su materialización. La calificación del riesgo se obtiene al multiplicar el valor asignado a cada una de estas dos variables. (p.48)

Este paso, es de vital importancia para que el responsable de seguridad establezca la calificación del riesgo y le permita tomar medidas acertadas.

En el análisis del riesgo existen diferentes métodos, uno es el método cualitativo (frecuencia) y se usa cuando la organización no tiene suficiente información sobre la ocurrencia de riesgos. En este análisis se utilizan descripciones para demostrar que los riesgos se pueden presentar (bajo, medio, alto) y el impacto (leve, grave, catastrófico). Los métodos cuantitativos (probabilidad) emplean modelos matemáticos, con datos de eventos que se hayan podido presentar con una frecuencia. En los métodos semicuantitativos (estimación subjetiva) se les asigna unos valores a los cualitativos de acuerdo a la información de los empleados u otras fuentes y se elaboran unas escalas, ajustadas a las necesidades de la organización.

En la etapa de la evaluación según la ISO 31000 (2009), establecerá qué tan grave es la consecuencia del impacto y será mas grave en la medida en que se comprometa una participación considerable del valor de la organización, cuyos parámetros de medición dependerán exclusivamente de sus directivos. Luego de haber obtenido la probabilidad y la consecuencia se procede a trasladar los datos a una matriz, teniendo en cuenta los tipos de riesgo que se están estudiando. Algunos riesgos analizados requerirán de tratamiento inmediato por los daños que se puedan ocasionar, otros podrán ser tratados a mediano y largo plazo y otros solo con medidas de control pueden ser mitigados.

En la evaluación del riesgo se tiene en cuenta la clasificación del riesgo y la forma como quede expuesta la organización. Dicha clasificación tiene que ver con los criterios que establezca la organización para medir el nivel de tolerancia al riesgo, el cual lo definen los directivos, soportado en las necesidades propias de la organización, estos niveles pueden ir desde aceptable hasta inaceptable cuando el riesgo no se puede evitar o debe ser tratado de inmediato. (Mejía, 2006). Con la evaluación del riesgo se podrá establecer si es crítico para la organización, posteriormente su forma de tratamiento.

Tratar el riesgo de fraude en una organización requiere tener en cuenta los niveles del riesgo producto de la valoración como se explicó anteriormente, es decir ante riesgo como fraude que muy alto se debe evitar, a riesgos bajos retener, a riesgos intermedios trabajarlos para llevarlos a que sean manejables dependiendo del impacto que puedan generar a la organización. Para Mejía

(2006), se presentan seis formas de tratar un riesgo a fraude: como medidas de control evitar, prevenir y proteger. Como medidas de financiación de las pérdidas aceptar, transferir y retener.

Para evitar el fraude se debe prácticamente eliminar la actividad, la probabilidad o el impacto, es decir evitar el riesgo. Para prevenir se debe trabajar en la anticipación, es decir establecer qué puede ocurrir y de esta forma establecer políticas y normas. Las formas más destacadas para prevenir el riesgo de fraude son: inspecciones y pruebas de seguridad, entrenamiento, inversión en información, diversificación, disminución del nivel de exposición, segregación o dispersión, políticas de seguridad. Mientras la prevención hace referencia a la anticipación, la protección se refiere a la acción en el momento de peligro o presencia del riesgo. (Mejía, 2006). Para cada riesgo se requiere aplicar la medida tratamiento más adecuada.

Para que el monitoreo sea efectivo, se debe tener en cuenta el comportamiento del riesgo en cada uno de los procesos a los cuales se le haya identificado, se deben emplear los indicadores de riesgo y efectuar autoevaluaciones o realizar la evaluación con personal que no tenga nada que ver con la administración, de tal forma que pueda emitir otros puntos de vista acerca de la efectividad de la administración de riesgo al fraude. Durante el monitoreo y la comunicación se establece si el riesgo fue identificado y evaluado en forma correcta, con el fin de aplicar los correctivos necesarios.

MANEJO DE RECURSO HUMANO EN LA ORGANIZACIÓN

Sin duda la administración del recurso humano es el principal modo de lograr que los procesos funcionen correctamente en la organización, en interacción con otros recursos disponibles para cumplir los objetivos.

Reclutamiento y selección

En el mundo actual las personas y las organizaciones están constantemente interactuando para complementarse unos con otros, cada una busca atraerse mutuamente para obtener informaciones y haciéndose opiniones para seleccionar lo más conveniente. Las organizaciones deben implementar un proceso de reclutamiento que no puede ser simple, con el fin de garantizar atraer candidatos que sean potencialmente calificados y capaces de ocupar cargos. En otras palabras es un sistema de información para divulgar y ofrecer las oportunidades de empleo a un

buen número de candidatos para que exista un modo adecuado de selección (Chiavenato, 2000).

Existen tres fases para el reclutamiento que se constituyen por una secuencia. Para Chiavenato (2000) está dada por las personas que la organización requiere, lo que el mercado de recurso humano puede ofrecer y las técnicas de reclutamiento por aplicar. De ahí se desprenden tres etapas: investigación interna sobre necesidades, investigación externa del mercado y definición de las técnicas de reclutamiento que se utilizarán. Dicha planeación lo que busca es cumplir con el propósito de estructurar el sistema de trabajo que se desarrollará, como se muestra en la siguiente figura.

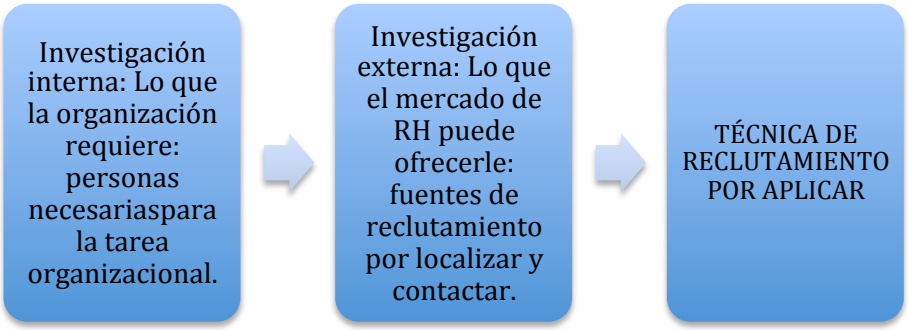

Figura 3. Las tres fases de la planeación del reclutamiento. Administración de Recursos Humanos, Chiavenato A 1990.

La planeación para el reclutamiento debe estar presente en todas las organizaciones, si bien es cierto que no es una responsabilidad directa del proceso de gestión de seguridad, si es necesario que haga revisiones y se vincule al proceso, pues a futuro puede ocasionar algún tipo de fraude que se debió haber evitado en cualquiera de sus fases, por ejemplo en el análisis de verificación de confiabilidad por medio de herramientas tecnológicas que permiten detectar malas intenciones que podrían afectar la imagen de la organización, como se verá mas adelante.

El proceso de reclutamiento varía según la organización y depende de la decisión que tome la alta dirección.

> En consecuencia, el órgano de reclutamiento no tiene autoridad para efectuar ninguna actividad de reclutamiento si el órgano que tiene la vacante no toma la decisión de llenarla. Dado que el reclutamiento es una función de staff, sus actos dependen de una decisión de la línea, que se oficializa mediante una especie de orden de servicio, generalmente denominada solicitud del empleado o solicitud de personal. Este documento debe llenarlo y entregarlo la persona que quiere llenar una vacante en su departamento o sección. (Chiavenato, 1990, p.217)

De esa forma se garantizará en cierta medida que la persona que se vincule posteriormente cumpla con los requisitos que la organización exige y no por otros intereses que puedan ocasionar algún tipo inadecuado de incorporación y pueda afectar en su interior los procesos.

La selección del personal se da después del proceso de reclutamiento y hace parte del proceso de vinculación, según (Chiavenato, 1990) la selección es una actividad de comparación, de elección de la opción mas conveniente para que posteriormente se decida; pero en la selección también se encuentran los filtros de entrada que en determinado momento puede restringir que una persona ocupe la vacante. La misión principal del proceso de selección es escoger entre muchos candidatos reclutados, los que mejor se adapten a las necesidades de la organización y que lo puedan desempeñar en forma correcta.

Existe una gran variedad de circunstancias entre las personas que las diferencian entre unas y otras como son los aspectos físicos, entre ellos la estatura, peso, sexo, etc; aspectos sicológicos como el temperamento, el carácter, la aptitud, la capacidad intelectual; que conllevan a que las personas tengan mas éxito y aprendan a realizar una tarea de una forma mas adecuada y rápida que otras. Garantizar estas condiciones es una de las tareas que tiene el proceso de selección, basados en datos e información que se tenga respecto al cargo y el estudio de la persona, que confrontados podrían dar como resultado una buena decisión de selección.

En la gráfica que se muestra a continuación se podrá tener un panorama mas amplio que permite establecer las dos variables confrontadas y al mismo tiempo exigir el análisis y la descripción del cargo y se de con mayor rigor la selección del candidato.

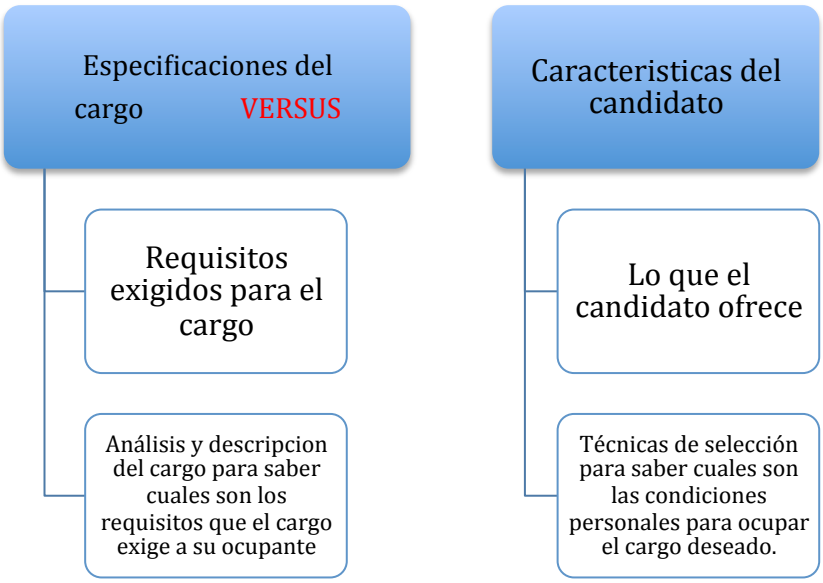

Figura 4. Selección de personal como proceso de comparación. Administración de Recursos Humanos, Chiavenato A 1990.

La comparación entre los dos parámetros permiten que haya una aproximación con calidad a la necesidad de la organización. Si el resultado está lejos de las especificaciones se rechazará y se devolverá a su inicio en reclutamiento.

Desde el punto de vista del proceso de gestión de seguridad, para la vinculación o selección de personal a una organización se debe tener en cuenta el perfil del candidato desde el punto de vista de la seguridad, como se había anunciado anteriormente sin importar que el proceso de gestión de recurso humano realice las diferentes fases. Antes de la inducción se debe realizar el estudio de seguridad, de acuerdo a su resultado se deben repetir procesos o la utilización de polígrafos si el cargo por su criticidad lo amerita.

Verificación de confiabilidad y desvinculación de la organización.

De acuerdo con Comer muchas organizaciones contratan personal sin realizar el más mínimo análisis de la historia e idoneidad, muchos de los candidatos han sido personas que han cumplido penas por delitos cometidos en otros cargos y nuevamente intentan volver a delinquir debido a que el proceso de vinculación no se realizó en forma exigente en las comprobaciones que se debían realizar. Se deben tener en cuenta el bienestar y seguridad de los empleados y activos de la organización asegurándose que no es peligrosa la vinculación de una persona poco recomendable.

Uno de los hechos mas frecuentes para ser vinculado a una organización es la falsificación del curriculum. En el se presentan documentos e información falsa como diplomas y certificaciones; el candidato al cargo lo hace según Comer con la posibilidad de averiguar que es lo que busca la organización y para quedar bien ante quien efectúa el análisis, por conseguir el puesto a como de lugar, querer presentarse como una persona socialmente valiosa y aceptable, la organización no se dará cuenta si esta siendo sincero o no.

Para Comer toda organización debe exigir la comprobación de los antecedentes sin violar los derechos humanos o cometer algún acto de discriminación por sexo, religión, color, etc; y lo debe hacer principalmente por protección de los empleados, selección de la persona más idónea para el puesto, protección del patrimonio y de la información, creación y mantenimiento de una ética empresarial de honradez, por coherencia.

Existen diferentes métodos para la verificación de la información que ha sido aportada por el candidato, se puede hacer mediante referencias escritas, referencias telefónicas, entrevistas al proceso de recurso humano, pruebas de polígrafo, pruebas sicológicas, investigaciones si es el caso mas detalladas, comprobaciones en las páginas web de fiscalía, procuraduría, contraloría, sijin, dijin, policía nacional, registraduría, ICBF, data jurídica, rama judicial, etc., de tal forma que facilite encontrar información que no ha sido revelada por el candidato o corroborar datos reflejados en documentos.

Las entrevistas según Comer son un sistema que ayudan a la organización a blindarse de actos malintencionados. Para ello, cuando el candidato asiste a la entrevista por parte de recurso

humano, se le entregará un impreso de solicitud de empleo y se le advertirá la importancia del puesto que va a ocupar, la rapidez con que se requiere el cargo y el seguro para prevención de riesgos por infidelidad. Se le pedirá que diligencie el formato en su totalidad con su nombre al final y unos documentos como pasaporte, licencia conducción, títulos profesionales, fotografía reciente, se advertirá que eso no garantizará la asignación del puesto.

Posteriormente el candidato al cargo se presentará a otra entrevista y si todo parece indicar que va ser el elegido, el proceso de gestión de seguridad procederá a realizar la entrevista presentando nuevamente los documentos. El responsable debe hacer la entrevista de seguridad, lo hará a solas y expondrá cual es la política de la organización en cuanto a ética empresarial y profesional y así mismo le explicará que se debe hacer una comprobación de los antecedentes de los candidatos que quedaron en la lista definitiva. Con los documentos aportados el entrevistador buscará enmiendas en nombres y fechas, diferencias en datos consignados anteriormente.

Otras fuentes de información importantes para el proceso de gestión de seguridad que garantizarán el grado de confiabilidad del candidato a vincular a la organización, en cuanto a datos de estudio el Ministerio de Educación, la Secretaria de Educación, instituciones educativas, embajadas y consulados, ICFES. En cuanto a empleos Cámara de Comercio, empleadores anteriores, superintendencias, Embajadas, datos en internet. En cuanto al aspecto social referencias familiares y personales, clubes, redes sociales, vecindario, etc. El aspecto económico en Asociación Bancaria, data crédito, catastro, entidades aseguradoras.

La visita domiciliaria también es un factor de suma importancia que permite corroborar y/o desvirtuar información aportada en el proceso de vinculación, permite conocer al candidato en su entorno familiar y personal y como medida de prevención de futuras actividades ilícitas al que se vea expuesto por cambios en su estilo de vida. Debe obedecer a un formato que contenga un enfoque de seguridad que permita establecer el grado de confiabilidad. La visita debe contener una comunicación sencilla, un lenguaje de respeto y cordialidad.

Es necesario en la verificación del grado de confiabilidad definir los cargos críticos. Según Bussines Alliance for Secure Commerce [BASC], (2016) debe existir un procedimiento documentado para evaluar los candidatos con posibilidades a ser contratados y realizar verificaciones periódicas de los empleados y trabajadores actuales. Para administrar los riesgos

se debe tener en cuenta la competencia y la confiabilidad, para hacer énfasis en la segunda se refiere a los principios, valores, educación, formación, experiencia y la habilidad del candidato al cargo crítico.

Para BASC la organización debe ejercer los controles sobre todos los procesos, especialmente sobre aquellos que son críticos, con procedimientos documentados de la selección y contratación (referencia laborales, personales, solicitudes de empleo, antecedentes, visita domiciliaria, pruebas alcohol y drogas, seguridad social, fotografía, huella dactilar, firma); mantenimiento (verificaciones periódicas, visitas domiciliarias cada dos años, actualización de datos, programa de concientización de adicciones, pruebas de alcohol y drogas) y terminación (eliminación controles de acceso, eliminación sistemas de información, control de dotación logos e imagen).

En algunas ocasiones las actividades de control constantes en los procesos de gestión de seguridad dan como resultado la realización de investigaciones mas profundas. Una vez realizadas las investigaciones por otros organismos o instituciones debido a que se salen del alcance de la organización, se recomienda la desvinculación del empleado lo cual debe ser apoyado por un profesional del derecho laboral con el fin de no propiciar futuras demandas que traen consecuencias a la imagen.

La confiabilidad está en manos de todos. La alta dirección define la autoridad, asigna las responsabilidades y establece mecanismos de control, el proceso de recursos humanos selecciona y contrata, esta constantemente actualizando y verificando y aplica controles, la seguridad también actualiza y verifica, investiga y hace seguimiento y constantemente se encuentra ejerciendo los controles necesarios a cada proceso. Deben ser eficaces, eficientes, efectivos y oportunos para generar el suficiente grado de confiabilidad.

En el proceso de desvinculación se debe evitar que el empleado salga con resentimientos contra la organización, jefes y compañeros, que se presente desviación en las investigaciones y haya manipulación por interés de terceros. La desvinculación se puede dar por voluntad propia o por decisión de la organización y debe darse bajo ciertas condiciones para darle un adecuado manejo; debe estar incluido dentro de los acuerdos laborales, se debe conocer la trayectoria dentro de la organización, debe hacerse de acuerdo al motivo de desvinculación una entrevista por parte de un experto.

Algunos de los temas que deben ser abordados durante la entrevista son el motivo del retiro, la opinión acerca de la organización, opinión sobre el jefe inmediato, horario de trabajo, las condiciones físicas del ambiente de trabajo, beneficios que otorgan, salario, las relaciones humanas, las oportunidades de progreso, la moral y actitud de los demás compañeros de trabajo, oportunidad de progreso, conceptos de seguridad y aportes que dejo a la organización, las actividades futuras, los riesgos del cargo y sugerencias para mejorar el cargo que desempeñaba.

Ética organizacional

Hablar de fraude en las organizaciones sin mencionar la ética empresarial no sería productivo para la reflexión que se está haciendo como análisis de prevención en un proceso de seguridad. Transparencia por Colombia (2016) hace referencia a un programa de ética empresarial como el mejor negocio que busca formar organizaciones íntegras y transparentes para el fortalecimiento de prácticas éticas, cuyo principal objetivo es llevarla a la acción como modelo de gestión y crear valor y confianza en las relaciones de negocio.

Los principales beneficios que se buscan con la práctica de la ética en las organizaciones son la mejora de la imagen corporativa, incrementar la productividad y competitividad, incrementar la toma de decisiones con sentido ético, favorecer la generación y la implementación de buenas prácticas empresariales, incentivar la rendición de cuentas y el sentido de pertenencia para contribuir a un entorno de negocios más ético. La implementación de los programas de ética deben hacerse a cualquier tipo de organización. (Transparencia por Colombia, 2016)

En el post acuerdo es importante combatir la corrupción, lo cual se convierte para el país en uno de los mayores retos. Para que se construya una paz estable y duradera se deben hacer compromisos desde lo público pero también desde lo privado. Bajo esa premisa las organizaciones deben ser conscientes de cumplir sus objetivos estratégicos en el mercado de manera ética como mejor negocio, crear una cultura a nivel global de carácter permanente, que conlleve a mantener lo más preciado después del recurso humano, es decir la reputación.

En una medición realizada por Transparencia por Colombia donde se valora el grado de transparencia y ética empresarial con las que se gobiernan, gestionan y conducen las organizaciones, además permite evaluar los mecanismos y políticas para identificar las fallas que

pueden convertirse en posibles riesgos de corrupción, los principales hallazgos donde se destacan los temas de integridad corporativa y lucha anticorrupción, las organizaciones se ubicaron en un promedio de 69,4% es decir riesgo medio de corrupción. Los componentes de controles internos en tuvieron un resultado de 70,6%, es decir riesgo medio, lo cual evidencia que se deben fortalecer los procesos de auditoría y medidas para prevenir, detectar, investigar y sancionar las acciones de corrupción.

Las recomendaciones presentadas por Transparencia por Colombia para el estudio realizado a las organizaciones se enfatiza en el fortalecimiento de mecanismos de detección y sanción por hechos de corrupción, implementar medidas para transparentar prácticas de donaciones, patrocinios en dinero o especie, regalos, gastos de representación y hospitalidad, afianzar sistemas de gestión contractual y gestión humana para garantizar procesos de abastecimiento y contratación transparentes y vinculación de personal con altos niveles de meritocracia, equidad y publicidad.

La ética debe estar presente en todas las actuaciones, si se desea un mejor país, las organizaciones están obligadas a determinar en sus políticas la cultura de la ética, con compromisos claros y contundentes de cero tolerancia con actos de corrupción, conscientes del rol que desempeña cada trabajador. Si por cualquier motivo la organización en los estudios realizados es propensa a actos de corrupción, deben establecerse las medidas que permitan implementar planes de mejoramiento en la seguridad y se fortalezca no solo al interior sino en su entorno.

TÉCNICA DE DETECCIÓN DEL FRAUDE

Las organizaciones deben garantizar un entorno seguro mediante la prevención de pérdidas fraudulentas, la detección es una acción que lleva a la investigación y recuperación de lo que se ha perdido, por tanto las técnicas deben ser aplicadas con sumo cuidado.

He aquí algunas normas básicas que cabe aplicar, en términos generales, a la detección de fraudes. 1. Nunca pasar por alto lo evidente. La mayoría de los fraudes se limitan a explotar huecos manifiestos en los sistemas de control y, además dejan síntomas palpables. Quien aspira a detectar un fraude ha de permanecer siempre alerta, reconocer sus síntomas y, cuando

aparecen, seguirlos hasta el final, sin contentarse con la primera explicación o excusa. 2. Buscar las desviaciones, no la solución mas compleja. Los investigadores inexpertos suelen buscar explicaciones complicadas a los síntomas de fraude mas evidentes. El enfoque correcto consiste en comenzar examinando las soluciones mas obvias y después, si es necesario, proceder por eliminación. 3. Concentrarse siempre en el punto mas sencillo y débil del fraude. La mayoría de ellos tiene tres elementos: acto de sustracción, ocultación y conversión fraudulenta. 4. Si se han manipulado las cuentas o destruido los registros, aquella persona cuya culpabilidad hubiera resultado más evidente. 5. Si tras la investigación de todos los hechos, el culpable perece ser determinada persona, es más que probable que realmente lo sea: esta es otra regla con sentido común. 6. La prevención y detección de fraudes no constituye una actividad esporádica, sino que debe formar parte rutinaria de la actividad empresarial (Comer, 1993, p. 222)

Es por ello que los responsables de realizar las acciones de detección deberán tener presentes las anteriores normas para tener éxito en el proceso de gestión de seguridad y garantizar el patrimonio de la organización.

Auditoría en puntos críticos

Comer (1993) señala que "La auditoría de puntos críticos es una técnica merced a la cual, mediante el examen de cuentas y registros, cabe detectar los síntomas de las manipulaciones y conversaciones fraudulentas; se trata pues de un filtro" (p. 225). Casi todas las organizaciones presentan procesos que son más vulnerables al fraude que otros y se podrían presentar ciertas acciones previsibles, que pueden beneficiar a la persona que tiene la intención fraudulenta ya que los efectos quedan ocultos entre todas las operaciones de la organización.

La probabilidad de detección de una auditoría de puntos críticos para que se ponga al descubierto los síntomas de un fraude es superior a la que se hace porcentualmente. Normalmente el delincuente siempre deja registros que han sido manipulados por la codicia o por medio de otra falsificación deja otros rastros. Para Comer (1993) esa probabilidad depende de tres factores: el tamaño de la organización y el numero de operaciones, cuentas, registros

fraudulentos y no fraudulentos que estén disponibles para examen, número de puntos que se examinan y de puntos fraudulentos.

Por lo anterior, normalmente las organizaciones son engañadas no solo por una persona sino que requieren de varias externas e internas para darle alcance, además a una sola persona si la organización es de un tamaño considerable le resultaría complejo realizar todos los movimientos sin ser descubierto a no ser que no haya ningún tipo de control o la ocultación sea tan arraigada que sea evidente descubrir un desfalco o daño al patrimonio.

Para la planeación de una auditoría según Comer (1993), dado que esta requiere un trabajo considerable, se debe planear cuidadosamente con anticipación. El personal que ha de ser seleccionado no debe tener ninguna afinidad con el proceso que se va a auditar. Las personas que van a auditar deben conocer la organización, con la formación pertinente para el caso y se asignará un mínimo de dos personas, dependiendo del procesos y su complejidad. El alcance de la auditoría debe darse por unidad de proceso para que se audite en forma separada y se debe tener en cuenta la tendencia de registros consolidados.

La periodicidad de la auditoría debe ser, si no existen sospechas de fraude y el personal de la sección no ha cambiado, con intervalos de tiempo de doce meses, ya que no se obstaculizará el desarrollo de las actividades normales, ya se habrá dado tiempo de tramitar los cheques y documentos necesarios, contabilización de cuentas transitorias, elaboración de datos estadísticos. Los métodos a emplear según Comer (1993) son el análisis histórico, proporcional e interempresarial y las pruebas especificas. Las primeras se centran en el examen de la racionalidad de los asientos de las cuentas e implican comparación en cuanto a rendimiento. El filtro se basa en las cuentas finales, saldos de comprobación y registros presupuestarios.

“Las comparaciones históricas presentan una doble utilidad. Por un lado, sirven para detectar los síntomas de fraudes por falseamiento o manipulación y, por otro, detectan síntomas de conversiones fraudulentas en las cuentas clientes y proveedores” (Comer, 1993, p. 229).

Las pruebas específicas pueden ser enfocadas directamente sobre las compras, cheques emitidos, ventas y marketing, cheques recibidos, existencias, nómina y personal, registros estadísticos, contabilidad general, maquinaria de control, transporte, clientes y proveedores. Las pruebas mencionadas permiten hacer comparaciones para determinar si han alterado informaciones, si ha habido casos de manipulación, incrementos en las compras o supresiones de ventas o algún tipo de ocultación en los inventarios.

CULTURA DE SEGURIDAD CORPORATIVA

La seguridad hoy día debe verse como un Sistema de Gestión en Control y Seguridad, aplicable a todos los procesos. BASC afirma que para que exista gestión deben existir objetivos e indicadores de gestión. Los indicadores generan un cambio en la cultura organizacional ya que impulsan a la transformación, facilitan cambios en los paradigmas, se crean condiciones para nuevos modelos de gestión, involucran a todos los trabajadores en los resultados de la organización, permiten responder a mercados y clientes cada vez mas exigentes, aseguran competitividad y facilitan anticiparse al cliente y al mercado.

Pero la cultura de seguridad se debe adquirir con importantes inducciones a las personas que se incorporan a la organización, cambiando los paradigmas, es decir creando un conjunto o modelo de ideas hacia la seguridad como algo que genera bienestar y tranquilidad en el entorno interno y externo de la organización, capacitando constantemente y haciendo auditorias que permitan crear conciencia y hábitos de prevención y detección de acciones indebidas que podrían acarrear situaciones incómodas de desprestigio y mala imagen.

Gran cantidad de organizaciones no son conscientes de la seguridad corporativa, la American Society for Industrial Security, [ASIS], (2016) afirma que más de la mitad de las organizaciones no cuentan con una autoridad o encargado central de la seguridad y los planes de seguridad solo se limitan a la instalación de elementos electrónicos y barreras perimetrales, En realidad no le dan el sentido verdadero a la seguridad, no crean la cultura de seguridad organizacional porque desde la alta dirección que son los responsables de ella no la asumen. En su gran mayoría encargan las actividades de seguridad como cargos adicionales, es decir que pasaría a un segundo plano, por evitar invertir 100% en seguridad.

Existen seis condiciones según ASIS que pueden facilitar alinear la organización con la cultura de seguridad. La primera es que el responsable de la seguridad debe convencer a todos los líderes de los procesos, actuar bajo esa premisa, sin tratar de hacer seguridad para o por la organización. La segunda es que se debe estimular el cambio y no imponerlo, apoyado en la influencia confiable de redes sociales. En la tercera condición los departamentos de seguridad no deben permanecer estáticos, deben responder a los nuevos retos y las preocupaciones del negocio conforme a las políticas de la organización.

Otra condición es que la seguridad existe en una organización no solo para prevenir los riesgos, sino para asumirlos dentro el desarrollo del negocio. La seguridad debe ser vista como una actividad de manejo estratégico y operativo. Por último, la confiabilidad del proceso de gestión de seguridad no solo proviene de la experiencia sino del conocimiento pleno del negocio, las habilidades personales, la capacidad de administración de la seguridad y la forma de comunicarse con las demás personas en la organización.

CONCLUSIONES

El fraude en las organizaciones es un delito que busca un beneficio personal, donde no da ningún valor a la honradez y es aprovechado cuando sus jefes o compañeros del trabajo depositan la confianza del manejo de recursos o información para sacar beneficio.

La motivación, la oportunidad y la racionalización son los elementos del triángulo del fraude que inciden para que una persona cometa el fraude en las organizaciones. Para algunos investigadores existen diferentes motivos para que el ser humano acceda a esta conducta impropia y puede estar asociado a sus propios escrúpulos.

En casi todas las organizaciones la teoría que más resultado tiene es la teoría de variedad de oportunidades, cuando se tiene acceso información, cuentas, bienes, con suficiente tiempo de planeación es más dado que se cometa el delito.

El falseamiento hace parte de la familia de la ocultación y hace referencia a un engaño que afecta las realidades físicas, comerciales o personales y se puede hacer antes, durante o después del acto de fraude. Seguramente es el más común en las organizaciones.

Existen delincuentes internos y externos que pueden ocasionar daño a la organización, los primeros hacen referencia a los trabajadores, los segundos a proveedores entre otros, resulta más incontrolable la comisión del delito.

El personal directivo y operativo no están exento de cometer fraude, cada uno desde sus accesos pueden interferir en cambios sustanciales para desfalcar la organización haciendo manipulaciones para no distraer el funcionamiento normal de las operaciones.

Normalmente las organizaciones que han sido víctimas de fraude no denuncian por temor a que se desprestigie su reputación o sean objeto de amenazas por parte de los defraudadores.

Se pueden resumir las modalidades de fraude como: manejo circulante, ingenieros contables, manejo indebido de los activos, uso indebido de claves de acceso, manejo de títulos, facturas o documentos negociables, evasión y elusión de impuestos, combinación de modalidades.

En Colombia existen una serie de normas que ayudan a combatir el fraude en las organizaciones, aunque en algunos casos confunden. Es necesario realizar un seguimiento detallado de todo el proceso de gestión de seguridad para coadyuvar a su judicialización.

A pesar de todos los esfuerzos por mejorar los procesos para evitar el fraude, Colombia sigue siendo uno de los países con mayor porcentaje de corrupción con el 80% a nivel nacional según los empresarios encuestados.

La gestión del riesgo debe estar presente en el proceso de gestión de seguridad como la posibilidad de ocurrencia de un evento que pueda afectar la organización.

El manejo del recurso humano es de suma importancia para realizar el reclutamiento, la selección y/o vinculación, verificar el grado de confiabilidad y la desvinculación de la organización.

La detección debe darse en las organizaciones por parte del responsable de seguridad, debe ser preocupación de la alta gerencia para generar un ambiente de seguridad y evitar ser reactivos ante un posible fraude, para ello se realizan auditorías a fin de tomar las acciones pertinentes.

La cultura de la seguridad corporativa solo es posible cuando el responsable de seguridad convence con hechos y no impone con fuerza las razones de crear conciencia de seguridad en la organización.

REFERENCIAS BIBLIOGRÁFICAS

ASIS INTERNACIONAL (2016). Prevención de Fraudes. Recuperado el 1 de julio de 2016 en http://www.manualdeseguridad.com.mx/aprende_a_protegerte/prevencion_de_fraudes/

ASIS INTERNACIONAL (2016). Seguridad Corporativa.. Recuperado el 24 de octubre 2016 en http://www.manualdeseguridad.com.mx/aprende_a_protegerte/seguridad_corporativa/seguridad_corporativa2.asp

BUSSINES ALLIANCE FOR SECURE COMMERCE. (2016). Definición de cargos críticos y de responsabilidades. (BASC, Ed.) Recuperado el 23 de 02 de 2016, de http://www.bascbogota.com/es/material_curso/Cargos%20criticos%20logo%20BASC.pd

CHIAVENATO A., Administración de recursos humanos, Mc Graw Hill, México 1990.

Colombia. (2000). Código Penal Colombiano, Ley 599 de 2000. (Colombia, Ed.) Recuperado el 28 de 01 de 2015, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

COMER M., El fraude en la empresa, Deusto 1993.

DINERO – EMPRESAS (2014). Colombia dentro de los 10 países con mayor fraude corporativo. Recuperado el 3 de octubre de 2016 en http://www.dinero.com/empresas/articulo/fraude-corporativo-colombia/199621

ESTUPIÑAN R., Control Interno y Fraudes, Ecoe, 2002. ISBN 958-648-296.

EY CONDUCTAS CORPORATIVAS INDEBIDAS – CONSECUENCIAS INDIVIDUALES (2016). Encuesta Global de Fraude. Recuperado el 28 de septiembre de 2016 en http://www.ey.com/co/es/services/assurance/fraud-investigation---dispute-services/ey-global-fraud-survey-2016

López W. (2012). El triángulo del fraude. Recuperado el 3 de julio de 2016 en http://forum-empresarial.uprrp.edu/volumenes/17-1/3.pdf

MEJIA R. (2006) Administración de Riesgos Un Enfoque Empresarial, Fondo Editorial Universidad EAFIT.

Quesada Madriz Gilberto. (2010). Administración de riesgos empresariales: definición y proceso. Recuperado el 5 de octubre de 2016 en http://www.gestiopolis.com/administracion-de-riesgos-empresariales-definicion-y-proceso/

TRANSPARENCIA POR COLOMBIA. (2016). Ética empresarial: el mejor negocio. Recuperado el 24 de octubre de 2016 en http://transparenciacolombia.org.co/etica-empresarial-el-mejor-negocio/

WEST H., Cómo evitar el fraude en la empresa, Deusto 1993.