FRAUDE INTERNO

PREVENCIÓN, DETECCIÓN Y TRATAMIENTO

FRAUDE INTERNO

PREVENCIÓN, DETECCIÓN Y TRATAMIENTO

"Lo único que necesita para que triunfe el mal es que los hombres buenos no hagan nada"

Edmund Burke, estadista y filósofo británico.

ÍNDICE

ÍNDICE 5
Agradecimientos 7
Prólogo 8

1. El fraude interno 11
1.1. Introducción 11
1.2. Prevención y Detección del Fraude Interno 12

2. Conceptos básicos 14
2.1. Qué es un programa antifraude 14
2.2. Factores de fraude 16
2.3. Mapa de riesgos. Metodología 16
2.4. Controles antifraude 21

3. Perfil y motivaciones del defraudador 25
3.1. Triangulo del fraude 25
3.2. Tipologías de fraude más comunes en las empresas 28
3.3. Perfil del defraudador 30
3.4. ¿Cuantos Fraudes Internos se comenten? 33

4. Prevención del Fraude Intermo 34
4.1. Gestión del riesgo de Fraude 34
4.2. ¿Qué és COSO? 35
4.3. COSO II: Diseño del sistema organizativo y de control interno para la prevención del fraude 37
4.4. Principales técnicas para la prevención del fraude 42

5. Detección del Fraude Interno 45
5.1. Red Flags: Señales de alerta para de detección del fraude 45
5.2. Habilidades del Gestor de Fraude Interno 47
5.3. Cuadro de mandos: monitorización y testeo de cumplimiento 47
5.4. Indicadores de fraude interno 52
5.4.1. Administrativo 52

5.4.2. Informático 59
5.4.3. Contable 64
5.4.4. Operativo 69

6. Tratamiento del Fraude Interno 73

6.1. Como actuar frente al evento de fraude interno 73
Somos conocedores de un fraude interno….. y ahora ¿qué? 73
6.2. Sistema Disciplinario 79
6.3. Cómo analizar documentos en un Fraude 80

7. Caso de fraude en una Entidad Financiera 83

7.1. Introducción 83
7.2. Como se detectó 85
7.3. Tratamiento del fraude una vez detectado 86
7.4. Controles antifraude: El cuadro de mandos como motor detectivo de fraudes. 87
7.5. Conclusión 88

8. Colaboraciones de otros profesionales 89

8.1. Marta Cavadid 89
8.2. Isabel Casares San José-Marti 95

9. Acerca del autor: 101

Albert Salvador Lafuente 101

Agradecimientos

Agradecimientos a todos los profesionales que me han acompañado y enseñado a lo largo de mi trayectoria profesional. También a todos los que me han seguido en los blogs, cursos, seminarios. Destacar a profesionales como Nahun Frett, Marta Cavadid, Isabel Casares San José-Martí entre muchos otros, que me han colaborado en este libro.

Agradecimientos a todos los que de una manera u otra me habéis acompañado, viene n la organización de eventos, o simplemente enviado un mensaje de apoyo o felicitación.

A todos ellos: gracias.

Prólogo

El fraude interno es uno de los más grandes retos que enfrentan las organizaciones contemporáneas a nivel global. El fraude disminuye de forma significativa la capacidad de desarrollo de nuestras instituciones, distorsionan el sistema de gobierno corporativo y control de las empresas e impide que los objetivos estratégicos de las instituciones sean alcanzados. Pero, más preocupante aún es que el fraude, además, de producir enormes pérdidas económicas, limita de forma sustancial la contribución social de las empresas y perjudica no solamente a la entidad donde ocurre la irregularidad, sino, que también afecta a sus accionistas, clientes, empleados y a la sociedad en general.

Todos tenemos el compromiso de frenar el fraude interno, a través de promover la integridad y transparencia en todos los niveles de nuestras organizaciones y creando conciencia acerca de la importancia e impacto de este mal. Ante esta flagrante realidad del mundo corporativo actual, Albert Salvador Lafuente ha toma en consideración que:

"Saber lo que es bueno y no hacerlo es la peor cobardía"
Confucio, filósofo chino, creador del confucianismo

Inspirado por este axioma, Albert nos presenta esta obra sobre fraude interno, que abarca tres etapas críticas: prevención, detección y tratamiento. Este libro comparte fórmulas precisas para dar respuestas efectivas en la lucha contra el fraude interno a través de presentar principios, ideas, estrategias y metodologías de alto impacto.

Solamente a través de un esfuerzo diligente, las organizaciones pueden protegerse contra los fraudes internos. Las explicaciones habituales no bastan para describir los acontecimientos de fraudes ocurridos en el interior de nuestras organizaciones, por lo que se necesitan armas potentes para poder contrarrestar esta pandemia; y en este documento usted encontrará todo un arsenal. Es de todos conocido que:

"Si la escalera no está apoyada en la pared correcta, cada peldaño que subimos es un paso más, hacia un lugar equivocado"

Stephe R. Covey, escritor, conferenciante, religioso y profesor estadounidense

Definitivamente, es imperativo elegir el camino correcto que la velocidad con que avanzamos, por esta razón en el presente trabajo de investigación se analiza a profundidad las siguientes interrogantes claves:

¿Qué es el fraude?
¿Qué es un programa antifraude?
¿Qué es COSO?
¿Cuáles son las señales de alerta para la detección de fraudes internos?
¿Cuántos fraudes internos se cometen?
¿Cómo actuar frente al evento de fraude interno?
¿Cómo podemos ir más allá?

Nuestras empresas e instituciones exigen que el personal en todos los niveles de la organización contribuya en la lucha contra el fraude, estas tareas no sólo incluyen el seguimiento y detección de actividades fraudulentas, sino también como cada uno de nosotros pueda brindar su apoyo para establecer y fortalecer los procesos de control interno, evaluación de riesgo y gobierno corporativo. Por lo que éste no es un libro de texto exclusivo para consultores o profesionales de compliance o para auditores internos o externos, sino que el mismo es esencial para todo el personal interesado en implementar un sistema que fomente una evolución transparente, sana y eficiente de su organización.

Debemos responder al llamado, debido a que:

"El lugar más caliente en el infierno está reservado para quienes, en un período de crisis moral, se mantienen neutrales".

Date, poeta, prosista, teórico de la literatura, filósofo y pensador italiano

Usted puede maldecir la oscuridad, o puede encender una vela y lo que ha hecho Albert Salvador Lafuente es encender una espléndida antorcha que nos guía a través del laberinto del fraude interno. Usando ejemplos de la vida real, nos muestra, de forma práctica, ejemplos concretos de controles antifraude; tipologías de fraudes más comunes; técnicas para la prevención del fraude interno; herramientas para la detección; y procedimientos costo/efectivos para saber cómo actuar frente a un evento de fraude interno, con la finalidad de poder oportunamente identificar, proteger, detectar y responder ante cualquier tipo de eventualidad.

Por último, tenga presente que los tipos de fraudes internos se han diversificado enormemente, por lo que estoy completamente convencido, que el conocimiento compartido en las próximas páginas será de gran utilidad a todos los lectores de este magnífico libro. Recuerde que el conocimiento es la única cosa que crece cuando más se comparte

Nahun Frett

1. El fraude interno

1.1. Introducción

Según el Diccionario de la Real Academia de la Lengua Española en su vigésima segunda Edición la palabra fraude tiene las siguientes definiciones:

- Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quién se comete.
- Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.
- Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.

Sin entrar en términos gramaticales se puede definir el Fraude como un engaño hacia un tercero, abuso de confianza, luto, simulación, etc. El término "fraude" se refiere al acto intencional de la administración, personal o de terceros, que deviene en una representación equivocada de los estados financieros, pudiendo implicar:

- Manipulación, falsificación o alteración de registros o documentos.
- Malversación de activos.
- Supresión u omisión de los efectos de ciertas transacciones en los registros o documentos.
- Registro de transacciones sin sustancia o soporte.
- Aplicación mala de políticas contables.

Se puede considerar que hay dos tipos de fraude:

- El primero de ellos se realiza con la intención financiera clara de malversación de activos de la empresa.
- El segundo tipo de fraude, es la presentación de información financiera fraudulenta como acto intencionado encaminado en alterar las cuentas anuales.

Los dos tipos de fraude, según los autores del mismo, pueden clasificarse en:

- **Internos** son aquellos organizados por una o diversas personas dentro de una institución, con la finalidad de obtener un beneficio propio.
- **Externos** son aquéllos que se efectúan por una o diversas personas para obtener un beneficio, utilizando fuentes externas como son: bancos, clientes, proveedores,

1.2. Prevención y Detección del Fraude Interno

Aunque se pueden considerar muchos puntos de vista, incluso el filosófico, conviene entender las razones por la que se cometen los fraudes, entre las que destacan:

- Falta de controles adecuados.
- Baja / alta rotación de puestos de trabajo.
- Documentación confusa.
- Salarios bajos.
- Legislación deficiente.
- Actividades incompatibles entre sí.

Las razones anteriores pueden clasificarse en tres grandes grupos que constituyen la denominada pirámide del fraude y que son:

- Se tiene la **Capacidad**.
- Se presenta la **Oportunidad**.
- Existe un **Motivo** justificativo.

En la lucha contra el Fraude únicamente se puede actuar contra el segundo factor, Oportunidad, ya que las otras dos son intrínsecas a la naturaleza de la persona.

Fraudes ha habido siempre y siempre habrá, incrementando su volumen en épocas de crisis, incluso suponiendo que las dos primeras variables, Capacidad y Oportunidad no varían, no pasa lo mismo con la tercera, el Motivo, ya que por una parte existen mayores

necesidades financieras y por otra las reducciones de personal pueden producir un efecto justificador de la acción que se comete.

Por lo anterior, las Empresas, especialmente en épocas de crisis, tienen que aumentar sus alertas en los dos ámbitos en los cuales pueden actuar, la Prevención y la Detección del fraude.

En cuanto a la prevención, la forma más sencilla consiste en:

- Mejorar el control administrativo.
- Implementar prácticas y políticas de control.
- Analizar los riesgos que motiven a un fraude.
- Tener a los mejores profesionales existentes, bien remunerados y motivados.

Para la labor de Detección es preciso tener en cuenta diversos factores que pueden proporcionar indicios que se está realizando un fraude, siendo los más útiles:

- Existencia de patrones de comportamiento irregular.
- Alertas disparadas delante determinadas acciones.

También se pueden utilizar otros métodos más tradicionales, como por ejemplo las “Denuncias anónimas”

El problema de la Detección es que se actúa “a posteriori”, cuando el fraude ya se ha cometido al menos en parte, mientras que con la Prevención la actuación se produce antes de que el fraude tenga lugar con lo que no se produce ninguna pérdida.

Es preciso tener en cuenta que las pérdidas, tanto tangibles como intangibles (en especial las reputacionales) son mayores cuanto mayor es el tiempo en el cual el fraude se extiende, por el que es de suma importancia la existencia de alertas primerizas.

A pesar de que cada uno de nosotros pueda pensar que existe un perfil tipo de la persona que comete un fraude, estadísticamente **está demostrado que cualquier empleado es susceptible de efectuar un fraude interno, siendo esta una situación impredecible**. Esto es una premisa fundamental a tener en cuenta delante de la implantación de cualquier control, ya sea preventivo o detectivo.

2. Conceptos básicos

2.1. ¿Qué es un programa antifraude?

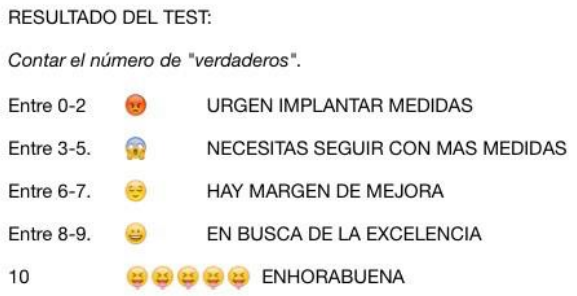
Vamos a realizar un pequeño test. Lo puedes realizar sobre la empresa donde estas trabajando, o la de algún familiar o amigo:

Test de Fraude Interno

Verdadero o Falso

1. Existe un Canal de denuncias anónimo? ___
2. Existe un Código de conducta? ___
3. Existe un Código ético? ___
4. Realizan formación o comunicaciones sobre prevención de fraude con todos los empleados? ___
5. Existen controles de prevención y detección de Fraude interno? ___
6. Caso de existir controles, la/s persona/s responsables están cualificadas? ___
7. Se realiza una valoración de riesgos de fraude? ___
8. Se realizan Auditorías Internas? ___
9. Se realizan Auditorías externas? ___
10. La Dirección impulsa el Área de control? ___

Recuerda que 8 de cada 10 empresas reconocen haber tenido un Fraude Interno!!


RESULTADO DEL TEST:

Contar el número de "verdaderos".

Entre 0-2	😡	URGEN IMPLANTAR MEDIDAS
Entre 3-5.	😱	NECESITAS SEGUIR CON MAS MEDIDAS
Entre 6-7.	😏	HAY MARGEN DE MEJORA
Entre 8-9.	😀	EN BUSCA DE LA EXCELENCIA
10	😝😝😝😝😝	ENHORABUENA

Un programa antifraude es un conjunto de medidas, muchas de ellas se desprenden del test que acabamos de realizar, gestionadas por un conjunto de profesionales que la empresa a designado para ello.

Es importante que, dentro de la estructura de las sociedades, se definida claramente la función del responsable de fraude interno. Normalmente suele recaer en Auditoría Interna, o en algún otro departamento del Área de Control (Seguridad, Cumplimiento Normativo, …). Bajo mi parecer, y dado que quien gestiona el Fraude Interno debe tener una fuerte independencia, y también acceso y conocimiento de la toda la organización, el mejor sitio es Auditoría Interna.

2.2. Factores de fraude

Los factores de fraude los podríamos definir como aquellos motivos que llevan a los defraudadores a cometer estos actos. A nivel enunciativo, vamos a mostrar los factores más importantes, segmentándoles por las 3 categorías que componen el triangulo del fraude, y del que hablaremos más adelante:

NCENTIVO/PRESIÓN
Presión por objetivos
Política empresa enfocada a resultados
Importe del Bonus variable
Presión clientes/proveedores
OPORTUNIDAD
Falta de Controles
Concentración de funciones
Conocimiento de la empresa
Política empresa enfocada a riesgos
Falta o poca Implicación de la dirección Vs Fraude
RAZONIALIZACIÓN/ACTITUD
Motivación
Autoestima
Moralidad
Éxito laboral
Respeto a la ley
Situación económica
Situación familiar
Formación

2.3. Mapa de riesgos. Metodología

El mapa de riesgos es una herramienta que tiene por objeto mostrar gráficamente el diagnóstico del proceso de evaluación de riesgos en una fecha dada. Se determina mediante la interacción de la probabilidad o frecuencia por el impacto de los tipos de riesgos en los diferentes procesos, actividades o funciones de un negocio. En simultáneo, contribuye a realizar una revisión o diagnóstico del control interno que existe para mitigar los riesgos.

En realidad ayuda mediante sucesivas diagramaciones a conocer las diversas instancias por las que pasa una evaluación de riesgos hasta definir el tratamiento de los riesgos.

Inicialmente proporciona el resultado de la evaluación de riesgos por los responsables de la gestión de riesgos.

Contribuye a decidir los desplazamientos del resultados inicial para lograr un nuevo nivel una vez propuesto el tratamiento de los riesgos, este último respetando el límite de exposición al apetito al riesgo.
Refleja el mapa de riesgos definitivo en la que se definió qué nivel del riesgo se desea aceptar, luego de decidir por asumir, prevenir, proteger o transferir parte del riesgo.

En auditoría el mapa de riesgos es quizá el más utilizado, pero es necesario recordar que existen otras herramientas a ser consultadas que proporcionan importante información para la realización de un efectivo trabajo de auditoría basada en riesgos.

El análisis de los mapas de riesgos contribuye a:

- Verificar que la herramienta exista y se emplea en la evaluación de riesgos, independientemente de la decisión a que estos gráficos pueden obedecer a diversas denominaciones y escala de frecuencia e impacto. Ejemplo, pueden ser 3x3, 5x5, 7,x7 etc. Del mismo modo si su diseño es en físico, a colores o uso de diversos aplicativos.
- Su existencia contribuye a identificar la ubicación de los controles establecidos para mitigar los riesgos, es decir conocer la brecha entre el riesgo inherente y residual.
- Promueve entre los auditores a una reflexión crítica para determinar si los controles aplicados son fiables, efectivos o débiles para mitigar el tamaño de los riesgos.
- Contribuye a dar solidez y minimiza la desconfianza en la oportunidad de mejora sugeridas por el auditor, al utilizar el mismo diagnóstico de los dueños de la gestión de riesgos.

- Un mapa de riesgos actualizado permite priorizar las revisiones del inventario de materias auditables en la confección del plan anual de control, en forma conjunta con otros criterios de selección.
- Su empleo como única herramienta mejora la comunicación en entrevistas que se haga a los responsables de los riesgos del proceso auditado.
- Ante la ausencia de mapas de riesgos oficiales, es importante advertir las grandes limitaciones que tendría el auditor si decide elaborar por su cuenta estos mapas al carecer de la opinión importante de los dueños de los procesos operativos.

Existen otras herramientas prácticas que forman parte de la evaluación de riesgos, las mismas que deberían ser consultadas en simultáneo por los auditores. Estas son: autoevaluación o "Risk Control Self Assessment", indicadores de riesgo, medidas de frecuencia y severidad, análisis de escenarios, entre otros.

El resultado de las autoevaluaciones permite recoger de los dueños de los procesos su percepción actualizada del estado de los riesgos y controles, así como oportunidades de mejora inmediata.

Los indicadores de riegos se definen cómo los datos estadísticos o métricas que permiten conocer la posición del riesgo en una entidad, sobre todo para conocer el nivel de riesgo inherente y residual. Son generalmente cuantitativos o pueden ser cualitativos, cuyos valores son calculados por lo general con base en datos históricos.

Las medidas de frecuencia y severidad suelen ser registros recogidos de incidentes históricos, mediante los cuales se puede tener una idea de la magnitud esperada ante la materialización de un determinado riesgo. Por lo general se grafican en escalas de niveles de frecuencia y nivel de impacto.

Finalmente, el análisis de escenarios permite conocer que tan bien se encuentra posicionada una entidad ante posibles eventos de vulnerabilidad, por lo general experimentados en el pasado. Estos análisis pueden ser históricos (se recoge tendencias), paramétricos

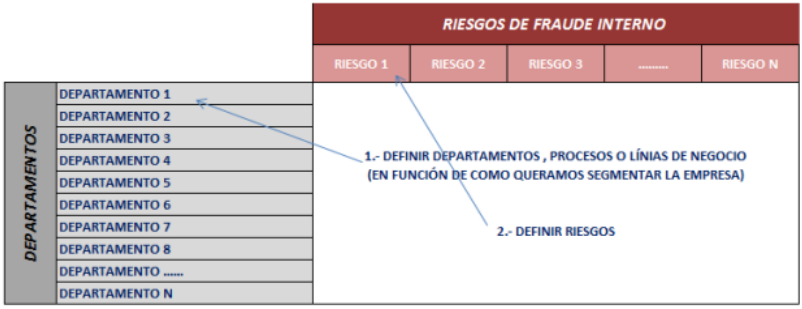
(se asume la presencia de una situación o tipo de distribución) y Ad-Hoc (resulta de la combinación de las anteriores). Una herramienta similar es el Value at Risk (VaR), medida ampliamente utilizada al cuantificar el riesgos de mercado preferentemente.

Metodología:

El mapa de riesgos es un buen punto de partido para saber los riesgos críticos que tiene nuestra empresa.

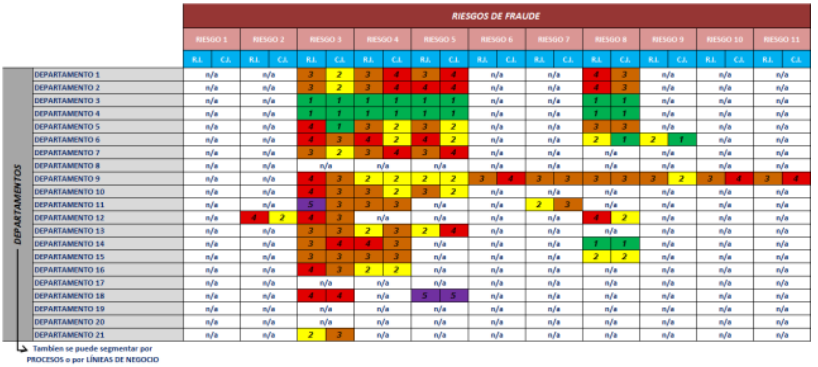
Vamos a resumir en 3 pasos como se realiza un mapa de riesgos, usando una matriz de doble entrada:

PASO 1



1. Identificar las unidades, departamentos, unidades de negocio o procesos a evaluar. La idea es segmentar la empresa en Departamentos, Procesos o Líneas de negocio, en función del tipo de empresa.
2. Inventariar los posibles riesgos de fraude. (P.e.: Manipulación contable, Obtención fraudulenta de financiación, Aplicaciones fraudulentas de Crédito, Transacciones no autorizadas, Apropiación indebida de activos, Soborno y corrupción, Blanqueo de dinero, Robo de información y violación de IP, Abuso de información privilegiada, Fraude fiscal, Abuso de mercado, Espionaje a favor de los competidores,…..)

PASO 2



	RIESGOS DE FRAUDE																					
	RIESGO 1		RIESGO 2		RIESGO 3		RIESGO 4		RIESGO 5		RIESGO 6		RIESGO 7		RIESGO 8		RIESGO 9		RIESGO 10		RIESGO 11	
	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.	R.I.	C.I.
DEPARTAMENTO 1	n/a		n/a		3	2	3	4	3	4	n/a		n/a		4	3	n/a		n/a		n/a	
DEPARTAMENTO 2	n/a		n/a		3	2	3	4	4	4	n/a		n/a		4	3	n/a		n/a		n/a	
DEPARTAMENTO 3	n/a		n/a		1	1	1	1	1	1	n/a		n/a		1	1	n/a		n/a		n/a	
DEPARTAMENTO 4	n/a		n/a		1	1	1	1	1	1	n/a		n/a		1	1	n/a		n/a		n/a	
DEPARTAMENTO 5	n/a		n/a		4	1	3	2	3	2	n/a		n/a		3	3	n/a		n/a		n/a	
DEPARTAMENTO 6	n/a		n/a		4	3	4	2	4	2	n/a		n/a		2	1	2	1	n/a		n/a	
DEPARTAMENTO 7	n/a		n/a		3	2	3	4	3	4	n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 8	n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 9	n/a		n/a		4	3	2	2	2	2	3	4	3	3	3	3	3	2	3	4	3	4
DEPARTAMENTO 10	n/a		n/a		4	3	3	2	3	2	n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 11	n/a		n/a		5	3	3	3	n/a		n/a		2	3	n/a		n/a		n/a		n/a	
DEPARTAMENTO 12	n/a		4	2	4	3	n/a		n/a		n/a		n/a		4	2	n/a		n/a		n/a	
DEPARTAMENTO 13	n/a		n/a		3	3	2	3	2	4	n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 14	n/a		n/a		3	4	4	3	n/a		n/a		n/a		1	1	n/a		n/a		n/a	
DEPARTAMENTO 15	n/a		n/a		3	3	3	3	n/a		n/a		n/a		2	2	n/a		n/a		n/a	
DEPARTAMENTO 16	n/a		n/a		4	3	2	2	n/a		n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 17	n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 18	n/a		n/a		4	4	n/a		5	5	n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 19	n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 20	n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a	
DEPARTAMENTO 21	n/a		n/a		2	3	n/a		n/a		n/a		n/a		n/a		n/a		n/a		n/a	

DEPARTAMENTOS

↳ También se puede segmentar por PROCESOS o por LÍNEAS DE NEGOCIO

TABLA DE PUNTUACIONES:

n/a	no aplica
1	R. Bajo
2	R. Medio
3	R. Medio Alto
4	R. Alto
5	R. Crítico

R.I Riesgos inherentes: mayor riesgo --> mayor puntuación
C.I. Control Interno: menor control existente --> mayor puntuación

Para cada Departamento (o segmento identificado), clasificar los riesgos previamente identificados, para saber si aplican o no aplican.

3. Valorar los Riesgos Inherentes (Probabilidad, Impacto) y los Controles de Riesgo existentes (excepto aquellos que no aplican).

PASO 3

		RIESGOS DE FRAUDE										
		RIESGO 1	RIESGO 2	RIESGO 3	RIESGO 4	RIESGO 5	RIESGO 6	RIESGO 7	RIESGO 8	RIESGO 9	RIESGO 10	RIESGO 11
DEPARTAMENTOS	DEPARTAMENTO 1	n/a	n/a	6	12	12	n/a	n/a	12	n/a	n/a	n/a
	DEPARTAMENTO 2	n/a	n/a	6	12	16	n/a	n/a	12	n/a	n/a	n/a
	DEPARTAMENTO 3	n/a	n/a	1	1	1	n/a	n/a	1	n/a	n/a	n/a
	DEPARTAMENTO 4	n/a	n/a	1	1	1	n/a	n/a	1	n/a	n/a	n/a
	DEPARTAMENTO 5	n/a	n/a	4	6	6	n/a	n/a	9	n/a	n/a	n/a
	DEPARTAMENTO 6	n/a	n/a	12	8	8	n/a	n/a	2	2	n/a	n/a
	DEPARTAMENTO 7	n/a	n/a	6	12	12	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 8	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 9	n/a	n/a	12	4	4	n/a	n/a	9	6	12	12
	DEPARTAMENTO 10	n/a	n/a	12	6	6	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 11	n/a	n/a	15	9	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 12	n/a	n/a	12	n/a	n/a	n/a	n/a	8	n/a	n/a	n/a
	DEPARTAMENTO 13	n/a	8	9	6	8	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 14	n/a	n/a	12	12	n/a	n/a	n/a	1	n/a	n/a	n/a
	DEPARTAMENTO 15	n/a	n/a	9	9	n/a	n/a	n/a	4	n/a	n/a	n/a
	DEPARTAMENTO 16	n/a	n/a	12	4	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 17	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 18	n/a	n/a	16	n/a	25	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 19	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 20	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	DEPARTAMENTO 21	n/a	n/a	6	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

TABLA DE PUNTUACIONES:

1-3	R. Bajo
4-6	R. Medio bajo
7-11	R. Medio
12-14	R. Medio Alto
15-24	R. Alto
25	R. Crítico

5. El resultado de multiplicar los Riesgos Inherentes y los Controles de Riesgo nos dará el mapeo definitivo de los riesgos de fraude de nuestra Empresa.

2.4. Controles antifraude

Podemos definir como control antifraude aquellas actuaciones, protocolos o verificaciones que se realizan con el fin de detectar una actuación irregular o anómala.

Los controles antifraude nos alertan de posibles fraudes, y sirven para poder iniciar una investigación. A parte de tener un claro enfoque de detección, su tratamiento también nos servirá como medida preventiva.

A continuación se exponen algunos ejemplos concretos de controles antifraude, tanto por información financiera fraudulenta como por una apropiación indebida de activos. Son sólo ejemplos y, por tanto, pueden no ser los más adecuados o necesarios en cada

circunstancia. Cada empresa, por su sector, tamaño y peculiaridades, necesita sus propios controles antifraude, pero sirvan estos ejemplos como guía. (el orden en que se presentan no pretende reflejar su importancia relativa):

- Visitar ubicaciones o realizar determinadas pruebas por sorpresa o sin previo aviso. Por ejemplo, observando el recuento de existencias en ubicaciones en las que no se haya anunciado previamente la visita, o realizando un recuento de efectivo por sorpresa en una fecha determinada.
- Efectuar una revisión detallada de los asientos de ajuste de final de trimestre o de cierre de ejercicio de la entidad e investigando los que resulten inusuales por su naturaleza o importe.
- Con respecto a transacciones significativas o inusuales, especialmente las que se producen al cierre del ejercicio o en una fecha cercana a éste, investigar la posibilidad de que existan partes vinculadas y las fuentes de los recursos financieros que sustentan las transacciones.
- Aplicar procedimientos analíticos sustantivos empleando datos desagregados. Por ejemplo, comparando ventas y costes de ventas por ubicación, línea de negocio o mes con las expectativas del auditor.
- Realizar entrevistas al personal relacionado con áreas en las que se ha identificado un riesgo de incorrección material debida a fraude, para obtener su opinión sobre el riesgo y sobre si los controles responden al riesgo, o el modo en que lo hacen. (Risk Assessment)
- Aplicar procedimientos de auditoría para analizar saldos de apertura de determinadas cuentas de estados financieros auditados previamente para valorar, con la ventaja que da la perspectiva temporal, el modo en que se resolvieron determinadas cuestiones que conllevan estimaciones y juicios contables; por ejemplo, una provisión para devoluciones de ventas.

- Aplicar procedimiento a cuentas u otras conciliaciones preparadas por la entidad, incluido el examen de conciliaciones realizadas en periodos intermedios.
- Aplicar técnicas asistidas por ordenador, como, por ejemplo, la extracción y posterior tratamiento de datos, para realizar pruebas sobre la existencia de anomalías. Se pueden definir cadenas de transacciones que pueden resultar alertas de operatorias irregulares.
- Realizar pruebas sobre la integridad de los registros y transacciones realizados por ordenador.
- Aplicar procedimientos analíticos sustantivos con relación a los ingresos empleando datos desagregados; por ejemplo, comparando ingresos registrados mensualmente y por línea de producto o segmento de negocio durante el periodo actual de información con periodos anteriores que sean comparables. Las técnicas de auditoría asistidas por ordenador pueden ser útiles para identificar relaciones o transacciones generadoras de ingresos inusuales o imprevistos.
- Confirmar con clientes determinados términos contractuales relevantes y la ausencia de acuerdos paralelos, ya que, a menudo, dichos términos o acuerdos influyen en la contabilización adecuada y las bases de los descuentos o el periodo al que se refieren suelen estar poco documentados. Por ejemplo, en tales situaciones suelen ser relevantes los criterios de aceptación, las condiciones de entrega y de pago, la ausencia de obligaciones futuras o continuadas del vendedor, el derecho de devolución del producto, los precios de reventa garantizados y las provisiones de cancelación o devolución.
- Indagar entre el personal de ventas y marketing de la entidad o ente el asesor jurídico interno sobre ventas o envíos realizados en una fecha cercana a la finalización del periodo y sobre su conocimiento de cualquier término o condición inusual asociados a dichas transacciones.

- Examinar los registros de existencias de la entidad para identificar las ubicaciones o las partidas que requieren atención específica durante el recuento físico de las existencias, o después de éste.
- Observar el recuento de existencias en determinadas ubicaciones sin previo aviso o realizar recuentos de existencias en todas las ubicaciones en la misma fecha.
- Realizar recuentos de existencias en la fecha de cierre del periodo de información o en una fecha cercana a ésta, para minimizar el riesgo de manipulación inadecuada durante el periodo comprendido entre el recuento de existencias y el cierre del periodo.
- Aplicar procedimientos adicionales durante la observación del recuento; por ejemplo, examinar de forma más rigurosa el contenido de artículos embalados, la forma en que se almacenan (por ejemplo, espacios vacíos) o etiquetan las mercancías, y la calidad (es decir, pureza, grado o concentración) de las sustancias líquidas, como perfumes o productos químicos. Recurrir a los servicios de un experto puede ser útil a este respecto.
- Comparar las cantidades del periodo actual con las de periodos anteriores por clase o categoría de existencias, ubicación u otros criterios, o comparación de las cantidades del recuento con los registros permanentes.
- Utilizar técnicas de auditoría asistidas por ordenador para comprobar con más detalle la compilación de los recuentos físicos de existencias. Por ejemplo, ordenar por número de etiqueta para realizar pruebas sobre los controles de etiquetas, o por número de serie de los artículos para realizar pruebas sobre la posibilidad de que se haya omitido o duplicado un artículo.
- Realizar un cotejo informático de la lista de proveedores con una lista de empleados para identificar coincidencias de direcciones y números de teléfono.
- Realizar un análisis informático de registros de nóminas para identificar duplicidades de direcciones, de números de

identidad o de identificación fiscal de empleados o cuentas bancarias.

- Revisar los expedientes de personal en busca de aquéllos que contengan poca o ninguna evidencia de actividad; por ejemplo, ausencia de evaluaciones de desempeño.
- Analizar los descuentos y devoluciones de ventas en busca de patrones o tendencias inusuales.
- Revisar la adecuación de gastos importantes e inusuales.
- Revisar la autorización y el valor en libros de préstamos a miembros de la alta dirección y a partes vinculadas a ellos.
- Revisar el nivel y adecuación de los informes de gastos presentados por la alta dirección.

3. Perfil y motivaciones del defraudador

3.1. Triangulo del fraude

Triángulo del Fraude:

Incentivo / Presión: por posibilidades de beneficios propios o presión externa a la realización del fraude

Racionalización / Actitud: factor subjetivo, responsabilidad, ética del empleado

Oportunidad: por falta de controles en el proceso o concentración indebida de funciones

Como sabemos el fraude empresarial es un riesgo que está presente en todo tipo de organizaciones y en cualquier latitud, por lo que se hace preciso concederle la grave importancia que tiene, administrándole convenientemente. Para ello, y como actuamos con cualquier otro riesgo, hemos de empezar por concretar cuáles son sus dos atributos, impacto y probabilidad.

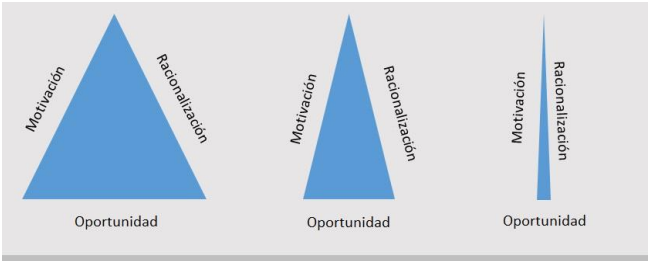
Respecto del posible impacto, de acuerdo con las estadísticas elaboradas por los especialistas, podemos decir que, en términos generales, el fraude tiene unas enormes repercusiones, estimadas, en promedio, en el equivalente al 5% del importe de las ventas de cada año. Lo que nos da idea del impacto de dicho riesgo.

En cuanto a la probabilidad de ocurrencia, este sería el segundo de los atributos con los que podríamos estimar la importancia del riesgo, tanto a nivel inherente como residual. Este dato nos lo podría facilitar la dimensión del famoso triángulo de fraude que sea aplicable en cada organización.

Recordemos que fue D. Cressey quien en 1961 expuso su conocida teoría respecto a los condicionantes para que se materialice el fraude, debiendo coexistir para ello tres situaciones:

1. **Motivación** (incentivo, presión). Cuando la Administración u otros empleados tienen un estímulo o presiones que les aportan razones justificativas para cometer fraudes.
2. **Poder** (Oportunidad). Serían las circunstancias que facilitan las posibilidades de perpetuar fraudes (por ejemplo la ausencia de controles, controles ineficaces, o la capacidad de la administración para abrogar los controles).
3. **Racionalización (**actitud). Cuando las personas son capaces de racionalizar un acto fraudulento en total congruencia con su código de ética personal o que poseen una actitud, carácter o conjunto de valores que les permiten, consciente e intencionalmente, cometer un acto deshonesto.

Teniendo presente la representación gráfica del triángulo con el que encabezamos estas líneas, creemos que la dimensión que el mismo tenga, es decir su área, determinará la probabilidad de ocurrencia, ya que si los tres factores tienen una dimensión elevada, la probabilidad también lo será; por eso, la mejor forma de combatir los riesgos de fraudes, es la de incidir sobre estos tres factores, reduciéndolos, pero no de forma simultánea, pues basta con que uno de ellos no esté presente para que el riesgo no se materialice, o en el peor de los caso que se minimice. Como representamos en el siguiente cuadro.



Como podemos observar en la secuencia gráfica, únicamente reduciendo la **Oportunidad**, el Área del triángulo, que representa la exposición al Fraude, se reduce proporcionalmente, aun manteniendo los otros dos indicadores (Motivación y Racionalización) constantes.

Como se observa en la figura anterior, el lado que hemos reducido es el que se corresponde con la oportunidad, y ello no de forma caprichosa, sino porque es el factor en el que la Organización tiene una mayor capacidad de actuaciones, puesto que si bien sobre la motivación y la racionalización las empresas pueden adoptar decisiones que se trasladen a los comportamientos de los empleados, hemos de reconocer que al final, estos dos factores (motivación y racionalización) dependen en gran medida de la postura que adopten los propios individuos, con independencia de las medidas que las empresas adopten para reconducirlos.

Por consiguiente, y siendo así, y no pretendiendo señalar que debemos desentendernos de las motivaciones y de la racionalización, pero sí para señalar que la trascendencia que tiene combatir/gestionar/administrar convenientemente el factor

"oportunidad", en donde radicaría el éxito de controlar la probabilidad de ocurrencia, de forma que si pudiésemos suprimirlo, habríamos conseguido eliminar totalmente el riesgo de fraude, a pesar de lo importante y altos que fuesen las motivaciones y la racionalización.

Como resultado de este planteamiento, y en la medida que se compartiese, deberíamos priorizar los controles con los que minimizar las "oportunidades" que puedan presentarse a los defraudadores, pues controlando estas, habremos incidido de forma eficaz en su combate, pero además si queremos que estos sean eficientes, deberemos decantarnos por los controles preventivos, que son de los que mayor beneficio obtendríamos.

3.2. Tipologías de fraude más comunes en las empresas

Según uno de los gurús en el ámbito de la auditoría interna y gestión de riesgos, Nahun Frett[1], el tipo de fraude que más frecuentemente afecta a cualquier organización es:

[1] **Nahun Frett** es un reconocido conferencista especializado en temas sobre auditoría interna, gestión de riesgo, gobierno corporativo, cambio organizacional, liderazgo y auto-evaluación de control. Motivador nato de

La malversación de activos

La malversación implica el robo o el uso indebido de los activos de una organización (por ejemplo, desvío de ingresos, robo de existencias o inventarios, fraude en la nómina). Los activos de una organización, tanto tangibles (por ejemplo: efectivo o inventarios) como intangibles (por ejemplo: derecho de autor o información confidencial), pueden ser objeto de malversación por parte de empleados, clientes o proveedores.

La organización debería asegurarse que existan controles implementados para proteger tales activos. Los esquemas más comunes incluyen malversación por parte de:

Empleados:

- Creación de y pago a proveedores ficticios.
- Pago de facturas sobrevaloradas (infladas) o ficticias.
- Facturas por bienes no recibidos o servicios no realizados.
- Robo de inventarios o utilización de activos de la organización para beneficio personal.
- Reporte de gastos falsos o sobrevalorados (inflados).
- Robo o uso de información confidencial de la organización.

Empleados en colusión con proveedores, clientes o terceras partes:

- Pagos de facturas sobrevaloradas (infladas) o ficticias.
- Emisión de notas de crédito sobrevaloradas (infladas) o ficticias.
- Facturas por bienes no recibidos o servicios no realizados.
- Precios o entregas preferenciales.

---

equipos multidisciplinarios de auditoría interna, ampliamente solicitado para dictar conferencias y proveer capacitación en cursos, talleres y seminarios.

- Manipulación de licitaciones, sorteos o proceso de adjudicar contratos.
- Robo o uso de información confidencial de la organización.

Proveedores:

- Pagos de facturas sobrevaloradas (infladas) o ficticias.
- Despachos incompletos / con faltantes o sustitución por bienes de menor calidad.
- Facturas por bienes no recibidos o servicios no realizados.

Clientes:

- Reclamos falsos por bienes dañados o devueltos así como por despachos incompletos.

La protección contra estos riesgos requiere no solamente de controles de protección física sino también de controles periódicos de detección, tales como: recuento físico de inventarios y reconciliación del auxiliar con la cuenta correspondiente del mayor general. Recuerde que un perpetrador de fraude astuto tendrá en cuenta estos controles y diseñara un esquema de fraude que evite o se oculte de ellos.

3.3. Perfil del defraudador

Vamos a destapar a nuestro defraudador: Un hombre, de entre 41 y 45 años, empleado, con entre 1 y 5 años de antigüedad en nuestra empresa, el cual nos expoliará 130.000 €:

Perfil del defraudador

Fuente: Auditool, IAI, ACME (México)

Este es el resultado estadístico del estudio realizado, a partir de la catalogación por frecuencias de fraudes y de importes de los mismos.

También es importe tener en cuenta la relación que tiene nuestro defraudador con el importe expoliado:

A mayor edad, antigüedad y cargo, mayor será el importe del fraude. O dicho de otra manera, a mayor frecuencia menor importe, y viceversa.

Los números y estadísticas dejan unos titulares muy sensacionalistas, aunque la conclusión realmente importante es la siguiente:

EL FRAUDE INTERNO PUEDE SER REALIZADO POR CUALQUIER PERSONA, INDEPENDIENTEMENTE DE SU PERFIL PERSONAL Y SITUACIÓN EN LA EMPRESA.

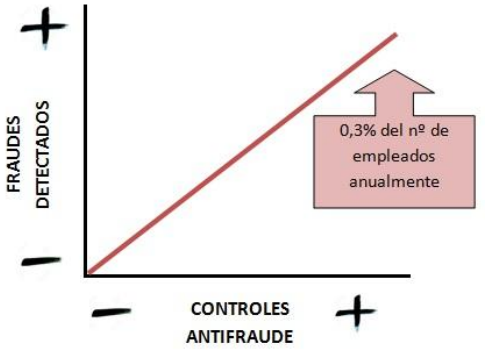
Por lo tanto, TODAS las personas de la organización, se tienen que someter a medidas anti-fraude.

3.4. ¿Cuantos Fraudes Internos se comenten?

Si hacemos caso a los datos estadísticos, podríamos concluir que a más controles antifraude implantados, más números de empleados fraudulentos hay. Y por el contrario, aquellas empresas que no tienen ningún control antifraude, no tienen ningún empleado fraudulento.

Pero esta conclusión no es cierta, ya que hay que tener en cuenta que **los fraudes existen con independencia de si estos se detectan o no**. Por lo tanto, la afirmación correcta seria que a mayor número de controles antifraude implantados, mayor número de detecciones realizaremos.

También hay que tener en cuenta la eficiencia de los controles antifraude. Hay varias estadísticas que dicen que sólo se detectan un 10% de los fraudes internos existentes.



Si tenemos en cuenta este dato, tendríamos que 30 de cada 1.000 empleados cometen anualmente algún tipo de fraude, y sólo 3 serían detectados, caso que la empresa disponga de medidas antifraude implantadas.

.

Otro tipo de enfoque seria partir de estos dos supuestos:

- El 100% de los empleados son susceptibles de realizar un fraude interno.
- Existe un residual del 0,3% de empleados que sabemos efectivamente que realizan fraudes internos.

Por lo tanto existe un 99,7% de nuestros empleados que no sabemos si cometen algún tipo de fraude o no.

4. Prevención del Fraude Intermo

4.1. Gestión del riesgo de Fraude

En cualquiera de sus categorías: apropiación de activos, corrupción, manipulación contable, uso de información privilegiada, etc., los delitos económicos han derivado en nuevas amenazas para las organizaciones de todo el mundo, los cuales conllevan un daño económico y reputacional a veces irreversible.

El aumento de los fraudes detectados y su alto impacto económico y reputacional han obligado a invertir en nuevas medidas de prevención para minimizar los daños. En este sentido, es crucial para las Organizaciones, diseñar e implantar un programa de gestión del Fraude y de la Corrupción, como elemento eficaz de prevención, detección e investigación de delitos. La mejor manera de evitar daños financieros, eventos de corrupción, de fraude interno y daños reputacionales, es implantar sistemas preventivos e instaurar una cultura ética.

En este sentido, el compromiso de la alta dirección es indispensable para instaurar un programa de gestión que, deberá constar, al menos, de los siguientes elementos:

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

Una correcta gestión integral del fraude interno nos permitirá prevenir, detectar y dar respuesta a los fraudes y conductas impropias en la empresa, instaurando un ambiente de control dentro de la organización.

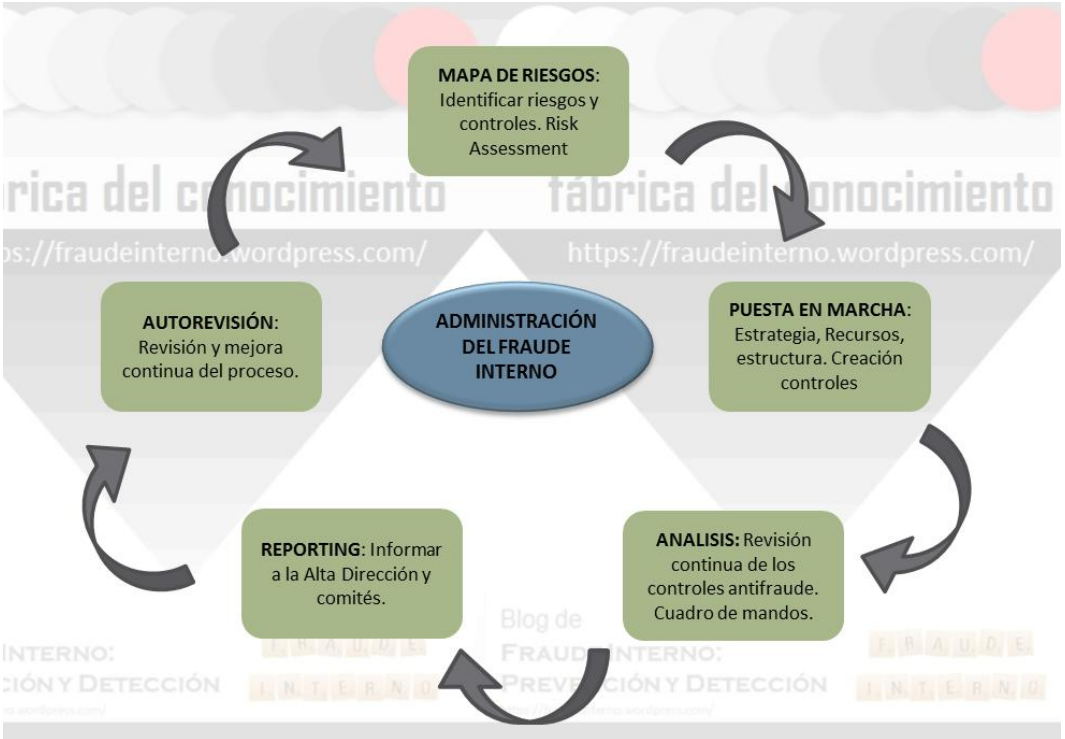
El principal objetivo debe focalizarse en la prevención y en la detección precoz de los fraudes, siendo un componente básico para la lucha contra el fraude la cultura y valores empresariales.

Ventajas

- ✓ Aporta Valor
- ✓ Favorece el Buen Gobierno
- ✓ Facilita la mejora continua de la Organización
- ✓ Aporta soluciones
- ✓ Mejora la imagen: Crea una cultura de calidad y de buenas prácticas
- ✓ Adaptación para la obtención de la certificación de
  - Sistemas de gestión de la calidad ISO 9001
  - Sistemas de Gestión de Compliance ISO 19600
  - Gestión de Riesgos ISO 31000
  - Sistema de Gestión Antisoborno ISO 37001

El siguiente esquema muestra cual sería el flujograma de la gestión y administración del fraude interno:

Gestión del riesgo de Fraude



Fuente: www.fraudeinterno.wordpress.com

4.2. ¿Qué és COSO?

El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control.

Debido a la gran aceptación de la que ha gozado, desde su publicación en el año 1992, el Informe COSO se ha convertido en el estándar de referencia.

Existen en la actualidad 2 versiones del Informe COSO. La versión del 1992 y la versión del 2004, que incorpora las exigencias de ley Sarbanes Oxley a su modelo.

Está diseñado para identificar los eventos que potencialmente puedan afectar a la entidad y para administrar los riesgos, proveer seguridad razonable para la administración y para la junta directiva de la organización orientada al logro de los objetivos del negocio.

COSO II

Hacia fines de Septiembre de 2004, como respuesta a una serie de escándalos, e irregularidades que provocaron pérdidas importante a inversionistas, empleados y otros grupos de interés.

Nuevamente el Committee of Sponsoring Organizations of the Treadway Commission, publicó el Enterprise Risk Management – Integrated Framework y sus aplicaciones técnicas asociadas.

Amplía el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo.

En septiembre de 2004 se publica el estudio ERM (Enterprice Risk Management) como una ampliación de Coso 1, de acuerdo a las conclusiones de los servicios de Pricewaterhouse a la comisión.

¿Qué se puede Obtener a través de COSO?

- Proporciona un marco de referencia aplicable a cualquier organización.
- Para COSO, este proceso debe estar integrado con el negocio, de tal manera que ayude a conseguir los resultados esperados en materia de rentabilidad y rendimiento.
- Trasmitir el concepto de que el esfuerzo involucra a toda la organización: Desde la Alta Dirección hasta el último empleado.

Ventajas de Coso

- Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión.
- Posibilita la priorización de los objetivos, riesgos clave del negocio, y de los controles implantados, lo que permite su adecuada gestión. toma de decisiones más segura, facilitando la asignación del capital.
- Alinea los objetivos del grupo con los objetivos de las diferentes unidades de negocio, así como los riesgos asumidos y los controles puestos en acción.
- Permite dar soporte a las actividades de planificación estratégica y control interno.
- Permite cumplir con los nuevos marcos regulatorios y demanda de nuevas prácticas de gobierno corporativo.
- Fomenta que la gestión de riesgos pase a formar parte de la cultura del grupo.

4.3. COSO II: Diseño del sistema organizativo y de control interno para la prevención del fraude

El 14 de mayo de 2013, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) publicó una versión actualizada de su Marco Integrado de Control Interno (Marco 2013) que proporciona unas mejoras a las entidades que utilicen el Marco de 1992, COSO Control Interno - Marco Integrado (el "Marco de 1992") para cumplir con la Sección 404 de la Ley Sarbanes-Oxley de 2002 (SOX), y la información sobre cómo hacer la transición del Marco 1992 al Marco 2013.

El Marco 2013 crea una estructura más formal para el diseño y la evaluación de la efectividad del control interno a través de 17 principios para describir los componentes del control interno relevantes para todas las entidades, desarrolla los conceptos de evaluación de riesgos, riesgo inherente, tolerancia al riesgo, tratamiento de los riesgos y la vinculación entre riesgos en las actividades de evaluación y control.

Asimismo, a diferencia del Marco 1992, incluye explícitamente el concepto de riesgo de fraude al evaluar los riesgos para el logro de los objetivos de la organización, teniendo en cuenta:

- Sesgo de la administración.
- Nivel de juicios y estimaciones en informes externos.
- Fraudes y situaciones comunes a los sectores y mercados en los que opera la entidad.
- Las regiones geográficas en las que opera la entidad.
- Los incentivos que pueden motivar un comportamiento fraudulento.
- La naturaleza de la tecnología y la capacidad de la administración para manejar la información.
- Transacciones inusuales o complejas sujetas a la influencia significativa en su gestión.
- La vulnerabilidad de la administración y los posibles esquemas para eludir las actividades de control existentes.

Además, se añaden consideraciones respecto al uso de los proveedores de servicios externalizados y una mayor relevancia de la tecnología de la información.

Se anima a las empresas a la transición de sus aplicaciones y la documentación relacionada con la actualización al Marco 2013 tan pronto como sea posible, dependiendo de las circunstancias particulares de las entidades. Durante el período de transición, establecido del 14 de mayo de 2013 al 15 de diciembre de 2014, se recomienda indicar la versión utilizada en los informes externos que se elaboren.

El Marco ERM y el Marco 2013 tienen diferentes enfoques pero los dos marcos se complementan entre sí para el diseño, implementación, realización y evaluación de la gestión de riesgos empresariales.

Las empresas que utilizan COSO para informar sobre el control interno en la presentación de reportes financieros externos podrían considerar:

- Identificación de nuevos conceptos y cambios en la norma.
- La evaluación de su formación y las necesidades de capacitación.
- El Marco 2013 afecta al diseño y evaluación del informe elaborado por las entidades debiendo establecer:

  - Evaluación de la cobertura de los principios de los procesos existentes y los controles relacionados.
  - Evaluación de los procesos actuales, actividades, y documentación disponible relacionada con la aplicación de los principios.
  - Identificación de las deficiencias existentes en el marco anterior.
  - Identificación de las medidas a tomar en la transición.
  - Formulación de un plan para la transición al 15 de diciembre de 2014 para las empresas obligadas a ella.

- Confirmación de la divulgación del marco utilizado en cada momento.
- Coordinación y comunicación interna con todos los grupos que son responsables de la implementación, seguimiento y presentación de informes de la organización.
- Discutir y coordinar las actividades con la auditoría interna y externa.

El Control Interno es un proceso llevado a cabo por el Consejo de Administración, la Gerencia y el resto del personal de la organización, diseñado para proporcionar una garantía razonable para lograr de objetivos relacionados con operaciones, reportes y cumplimiento.

En un sistema efectivo de control interno bajo el Marco 2013, cada uno de los cinco componentes y principios están obligados a estar presentes y en funcionamiento.

- **Presente** definido como "la determinación de que existen componentes y principios pertinentes en el diseño e implementación del sistema de control interno para lograr los objetivos especificados."
- **Funcionamiento** definido como "la determinación de que los componentes y los principios pertinentes siguen existiendo en la realización del sistema de control interno para lograr los objetivos especificados."

Se requieren los cinco componentes para operar juntos de una manera integrada, de tal forma que la organización de cumplir con los 17 principios:

Entorno de Control

1) Debe demostrar su compromiso con la integridad y los valores éticos.
2) El Consejo de Administración debe demostrar independencia en la gestión y ejercer la supervisión del desarrollo y ejecución del control interno.
3) La alta dirección debe establecer, con la supervisión del Consejo de Administración, la estructura, líneas de reporting, autoridad y responsabilidad en la consecución de objetivos.
4) Debe demostrar su compromiso para atraer, desarrollar y retener personas competentes.
5) En la consecución de los objetivos, debe disponer de personas responsables para atender sus responsabilidades de Control Interno.

Evaluación de Riesgos

6) Debe especificar los objetivos para permitir la identificación y evaluación de los riesgos relacionados.
7) Debe identificar y evaluar sus riesgos.
8) Debe gestionar el riesgo de fraude.
9) Debe identificar y evaluar los cambios que podrían impactar en el sistema de control interno.

Actividades de Control

10) Debe seleccionar y desarrollar actividades de control que contribuyan a la mitigación de los riesgos para el logro de sus objetivos.

11) Debe seleccionar y desarrollar controles generales sobre Tecnología de la Información.
12) Debe implementar sus actividades de control a través de políticas y procedimientos adecuados.
13) Información y Comunicación
14) Debe generar la información relevante para respaldar el funcionamiento de los otros componentes de Control Interno.
15) Debe compartir internamente la información, incluyendo los objetivos y responsabilidades para el control interno, necesaria para respaldar el funcionamiento de los otros componentes de Control Interno.
16) Debe comunicar externamente las materias que afecten al funcionamiento de los otros componentes de Control Interno.

Actividades de Monitorización

17) Debe llevar a cabo evaluaciones continuas e individuales, con el fin de comprobar si los componentes del control interno están presentes y funcionando.
18) Debe evaluar y comunicar las deficiencias de control interno.

Los principios introducen ciertos cambios en los componentes del Control Interno, destacando la evaluación de los riesgos que, a partir que ahora, ha de incluir los conceptos de velocidad y persistencia de los riesgos como criterios para evaluar la criticidad de los mismos.

Velocidad de riesgo se refiere a la rapidez con la que impacta un riesgo en la organización una vez este se ha materializado. Persistencia de un riesgo se refiere a la duración del impacto después de que le riesgo se haya materializado. Adicionalmente, el Marco 2013, ha modificado la información acerca de las tareas y responsabilidades de los distintos participantes en el proceso, tales como:

- Responsabilidades del CEO y CFO para que formalmente asuman la efectividad del control interno en ciertas jurisdicciones.
- Actividad a desarrollar por los distintos tipos de Comités y su campo de actuación.
- Necesidad de incorporar, además de los auditores externos, a otros proveedores de servicios externalizados (evaluadores) para completar los diferentes tipos de revisión que puede realizar una entidad sobre su control interno (riesgos medioambientales, prácticas de comercio justo o seguridad laboral, etc.).
- Exigencias reguladoras y legislativas para certificar la eficacia del control interno de la compañía sobre el reporte financiero.
- Responsabilidad en la gestión de los riesgos de los procesos externalizados, debiendo implementar un programa para evaluar dichas actividades realizadas por otros en su nombre, y evaluar la eficacia del sistema de control interno sobre las actividades realizadas por dichos proveedores externos de servicios.

4.4. Principales técnicas para la prevención del fraude

Todas las compañías son susceptibles de padecer algún tipo de fraude, ya que cuando hay colusión e intención, es difícil detectarlo y frenarlo. A pesar de esto, se ha visto que este riesgo se mitiga sustancialmente cuando las empresas cuentan con un programa integral que permite combinar mecanismos de cambio cultural con controles internos en los procesos de negocio.

Un adecuado sistema de administración de riesgos debe partir de una estructura sólida de gobierno corporativo. Todos en la organización desempeñan un papel importante en el proceso de supervisión y monitoreo, tanto el Consejo de Administración como el Comité de Auditoría, la gerencia y los auditores internos.

Si tu empresa no tiene ninguna medida antifraude, puedes empezar por implantar algunas medidas sencillas y sin coste para la empresa. A continuación te propongo alguna de ellas:

1. **Instaurar un código ético**: Un código de ética fija normas que regulan los comportamientos de las personas dentro de una empresa u organización. Aunque la ética no es coactiva (no impone castigos legales), el código de ética supone una normativa interna de cumplimiento obligatorio. No divulgar información confidencial, no discriminar a los clientes o los compañeros de trabajo por motivos de raza, nacionalidad o religión y no aceptar sobornos, por ejemplo, son algunos de los postulados que suelen estar incluidos en los códigos de ética.
2. **Instaurar un código de conducta**: Un código de conducta de empresa es un documento redactado voluntariamente por una empresa en el que se exponen una serie de principios que se compromete unilateralmente a seguir.
3. **Instaurar un Organigrama**: El contar con él y que lo conozca el personal es esencial para tener una buena estructura empresarial y mantener un **ambiente de control optimo,** que favorecerá el logro de los objetivos de la empresa:
   - Identificación de las áreas que conforman la empresa.
   - Delegación de responsabilidades y obligaciones.
   - Segregación de funciones.
   - Eficiencia y fluidez de la comunicación entre áreas.
   - Una optima supervisión o vigilancia de las áreas bajo mando.
   - Líneas de reporte bien definidas.
4. **Creación de un comité de disciplina**: Su labor es vigilar la conducta de los empleados, y que no se violen ni las disposiciones ni los Reglamentos que sean aprobados por los órganos de Gobierno de la empresa. Recae sobre este comité la de someter a sanciones ante el Comité Ejecutivo para todos aquellos empleados en los que se observen mala conducta y que violen las disposiciones y reglamentos establecidos, incluyendo a los propios miembros del Comité Ejecutivo.

5. **<u>Canal de comunicación o de denuncias</u>**: Se trata de un canal de comunicación confidencial entre clientes, proveedores, accionistas, etc… a través del cual se podrá comunicar cualquier posible irregularidad o incumplimiento relacionado con malas prácticas financieras, contables o de control, que puedan tener un impacto en los estados financieros, la contabilidad, la auditoría o los controles implantados.

6. **<u>Divulgación y formación</u>**: a través de los canales existentes en la empresa, impulsar la divulgación de las mejores prácticas para la consecución de los objetivos dentro de la empresa.

	Como evitar el Fraude Interno?	
	PREVENCIÓN	DETECCIÓN
Como	Evaluación de riesgos de fraude	Vigilancia :
	Controles de Riesgos	- Auditoria
	Código de conducta	- Supervisión
	Código ético	Monitorización
	Comunicación/Formación	Análisis forense
	Canal de denuncias anónimo	
Objetivo	Crear ambiente de Control y evitar el Fraude	Detectar Fraudes Internos (mitigarlos y elaborar controles nuevos para prevenirlos)

El 80% de las empresas de todos los sectores reconoce haber sido víctima de algún tipo de fraude, y curiosamente más de la mitad no implanta un sistema de integral contra el fraude interno.

http://cincodias.com/cincodias/2007/10/23/economia/1193118986_850215.html)

http://www.forodeseguridad.com/artic/discipl/disc_4046.htm

Los objetivos principales de un programa integral de administración de riesgos de fraude son: prevenir, detectar y dar respuesta a los fraudes y conductas impropias en la empresa.

5. Detección del Fraude Interno

5.1. Red Flags: Señales de alerta para de detección del fraude

Si partimos de la premisa que detrás de cada persona que comete un fraude, delito o actividad corrupta hay un comportamiento o circunstancia que lo ha motivado, podemos analizar de una manera empírica cuales son estos comportamientos y circunstancias. Una vez analizados, podemos establecer cuáles son aquellos más comunes, a los que llamaremos "red flags" o banderas rojas.

Por lo tanto, tenemos que detrás de un acto fraudulento existe una bandera roja, pero es importante tener en cuenta que la existencia de una bandera roja no significa necesariamente la existencia de un fraude.

Las banderas rojas, pues, son una serie de alertas que debemos observar y tener en cuenta tanto en la prevención como en la detección del fraude.

A continuación os detallo algunas de las banderas rojas en los comportamientos de las personas (ver también fig.1):

- Signos de riqueza externos
- Relación de confianza con clientes/proveedores
- Problemas de adicción (juego, alcohol, drogas)
- Doble vida
- Problemas familiares / divorcio reciente
- No delegación de funciones
- Irritabilidad, actitud defensiva
- Conflictividad laboral
- Presión comercial excesiva
- Inestabilidad ante las circunstancias de la vida
- Comportamientos anómalos

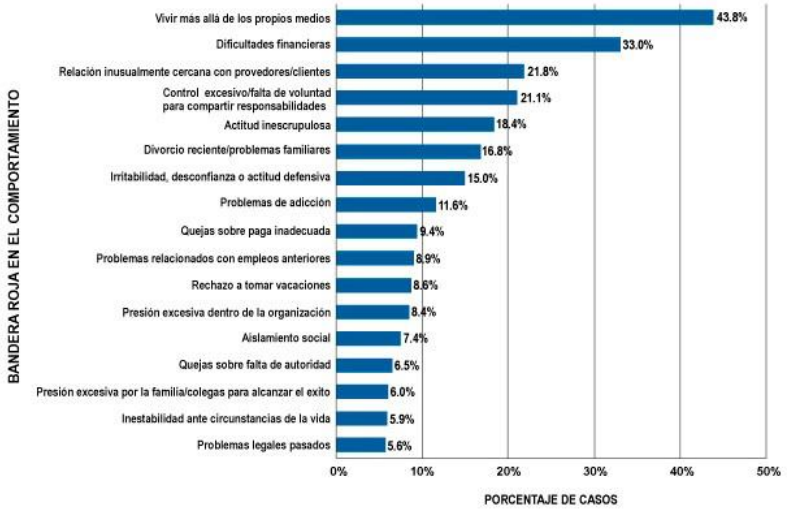


Fig. 1

A partir de las banderas rojas podemos crear una serie de alertas y controles, especialmente en aquellos casos que exista la confluencia de varias. Estos controles, juntamente con otros, forman parte del programa antifraude, siendo este un elemento crucial en la gestión del riesgo de fraude y corrupción.

Las banderas rojas son mucho más que un elemento único de detección del fraude, ya que forman parte del puzle de controles y alertas que nos ayudaran a gestionar el fraude de una manera eficaz. También son una excelente medida preventiva si son tratadas a tiempo.

Ahora ya tenemos la teoría, pero para que todo este sistema funcione, es imprescindible el factor humano, ya que no existe una máquina ni sistema que detecte el fraude.

5.2. Habilidades del Gestor de Fraude Interno

Existe una serie de habilidades personales que debemos exigir y potenciar a todas aquellas personas que luchan contra el fraude:

- **Curiosidad**: Pregúntate el porqué de las coses, te ayudará a adquirir nuevos conocimientos constantemente
- **Perspicacia**: No dejes escapar ningún detalle, por pequeño que sea.
- **Flexibilidad**: Adopta diversos puntos de vista y maneras de trabajar.
- **Ingenio**: Aporta nuevas idees de valor, que ayuden a llagar a tu objetivo de manera más eficaz y eficiente. Se imaginativo.
- **Rigurosidad**: Analiza con completitud. Documenta todo tu trabajo de manera que exista trazabilidad en todo lo que haces.

Pensar como ladrón para atrapar al ladrón

5.3. Cuadro de mandos: monitorización y testeo de cumplimiento

Formamos parte de una sociedad en que el 80% de las empresas de todos los sectores reconoce haber sido víctima de algún tipo de fraude y que, a pesar de esto, más de la mitad no implanta un sistema de gestión integral contra el fraude interno.

Una sociedad que arrastra 8 años de crisis económica, en que las empresas han focalizado los recursos humanos hacia las áreas que los ejecutivos consideran más relevantes para la supervivencia empresarial, provocando una reducción de recursos internos en la lucha contra los delitos económicos. Así mismo, la reducción de costes de las empresas pasa en la mayoría de casos por una reducción generalizada de los recursos humanos, que puede acarrear una concentración de funciones en una misma persona, o bien

recortes salariales. Y por último, las presiones para la consecución de los objetivos son cada vez mayores. **Todo esto hace que los 3 elementos principales del fraude (Incentivo, Oportunidad y Racionalización), se vean incrementados y por lo tanto, la probabilidad de un fraude interne se incremente**.

Para combatir el fraude interno, se necesita un adecuado sistema de administración de riesgos, que debe partir de una estructura sólida de gobierno corporativo. Sin duda un programa efectivo de administración de fraude requiere que toda la organización participe en la gestión del riesgo de fraude (modelo de 3 líneas de defensa), **siendo esencial el apoyo e implicación de la alta dirección**.

Un programa de gestión integral del fraude interno, debe contar con todos los elemento posibles a nuestro alcance, tanto preventivos como detectivos. **El elemento diferenciador en la gestión del fraude interno es disponer de un sistema integral que aglutine alertas y controles** (cuadro de mandos), así como la dotación necesaria de recursos humanos con un elevado grado de "expertis".

Por lo tanto, el cuadro de mandos pasaría a ser el motor de la Gestión del Fraude Interno, y del que podríamos destacar 5 fases:

1ª fase: Creación de Alertas y Controles.

Cada alerta de fraude consta con numerosos registros que indican un potencial riesgo de fraude. Se generan periódicamente de manera automática a partir de la monitorización u otras fuentes de información existentes. Una alerta se puede diseñar a partir de algo muy concreto, o bien de manera compleja, mediante el encadenamiento de ciertos comportamientos. Los controles, serian aquellos que generan y reportan otros departamentos (no Auditoría Interna) de la organización, es decir las 2ª y 3ª LdD (Línea de Defensa). Auditoría Interna debe revisar que los controles sean eficientes y se realizan de manera metodológica, así como proponer la creación de nuevos controles.

Para diseñar una alerta, hay que ser creativo y ponerse en la piel del defraudador, buscando comportamientos u operatorias potenciales de fraude interno que sean de generación automática, medibles y asignables a una persona y/o centro.

Algunos tipos de análisis que permiten detectar indicios de fraude:

- **Frecuencia**: Análisis del número de transacciones realizadas por cada uno de los usuarios que realizan tareas similares.
- **Patrones Numéricos**: Cuantías de las transacciones, identificando cifras o tendencias poco frecuentes en una operativa normal de la organización.
- **Materialidad**: Cantidades acumuladas manejadas en las transacciones, tanto para transacciones concretas como para acumulados por cuentas contables o usuarios.
- **Horario**: Fecha y hora de ejecución de las transacciones, identificando aquellas efectuadas en momentos inusuales respecto a la operativa del negocio.
- **Descripción**: Descripciones introducidas para las transacciones, identificando transacciones con descripciones inusuales.

2º fase: Creación del Cuadro de Mandos.

Se agruparan las Alertas y Controles en bloques o temáticas (máximo 4 o 5 bloques), ponderándolos en función de su probabilidad y gravedad. Cada Alerta y Control tendrá asignado un empleado y/o centro responsable y una puntuación propia (p.e. por “deciles”). Las puntuaciones han de ser homogéneas entre alertas y controles. (p.e. puntuación máxima de 10 y mínima de 0)

3º fase: Generador de información.

A través del cuadro de mandos se pueden realizar consultas; por empleado o por centros, mostrando puntuaciones, gráficos de evoluciones y datos estadísticos. Así mismo, nos proporciona los ránquines y los informes necesarios para realizar las revisiones,

4ª fase: Revisión.

A partir de los ránquines e informes, se realizan las revisiones que previamente estarán definidas en el correspondiente manual de procedimientos, A nivel general podemos dividir las revisiones entre aquellas individuales, alertas que se definan como de “alta probabilidad de fraude”, y globales, en función del resultado de la suma de todas las alertas y controles. Una buena práctica es una

revisión no basada solo en las puntas o “tops”, sino también una parte aleatoria sobre indicadores intermedios o bajos.

5ª fase: Análisis.

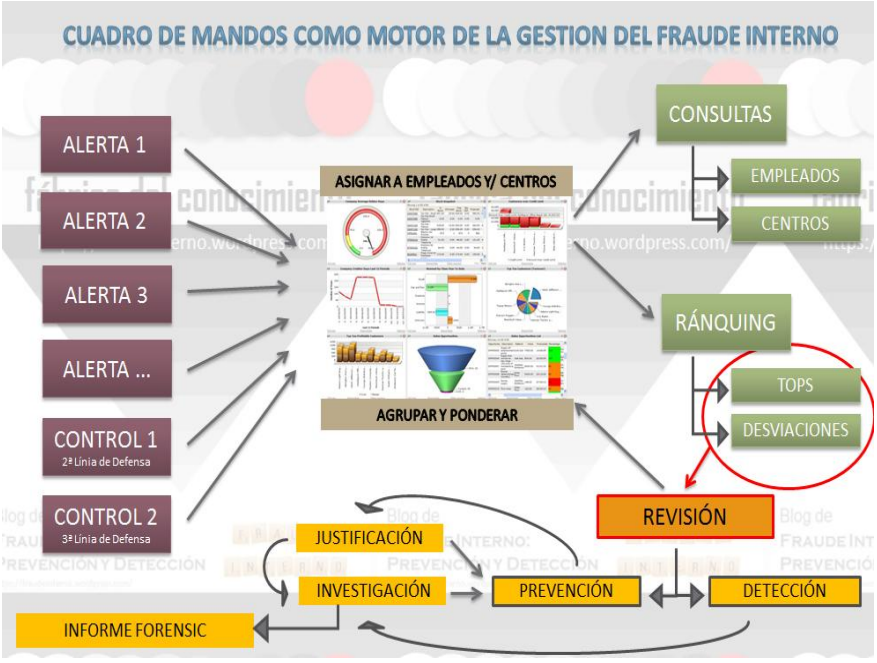
A pesar de los avances tecnológicos, no existe una herramienta que detecte los empleados que cometen un fraude. Esto implica la necesidad de una revisión manual. En el análisis manual de cualquier alerta potencial de fraude interno, debemos establecer si aplicamos un protocolo de Prevención o bien de Detección:

En el protocolo de prevención, se debe solicitar justificación por parte del empleado o centro de la operatoria detectada. Dependiendo de las justificaciones, la revisión pasará a formar parte de una medida preventiva, o bien si estas nos indican que puede haber un indicio de Fraude Interno, activaremos el protocolo de detección, abriendo una investigación.

El protocolo de Detección, se aplicara si fruto de la revisión consideramos que existen indicios de Fraude Interno, abriendo la correspondiente investigación. Una investigación puede concluir con una “falsa alarma”, y por tanto habremos realizado una labor preventiva, o bien con informe forensic y su presentación al comité de disciplina.

Sea cual sea el resultado de la revisión, se deberá documentar todas la pruebas, evidencias, comunicados e informes que realicemos, con especial atención a aquellas que vayan ligadas a una investigación que finalice en un informe forensic.

Cuadro de mandos: monitorización y testeo de cumplimiento



Fuente: www.fraudeinterno.wordpress.com

5.4. Indicadores de fraude interno

5.4.1. Administrativo

Se enumeran en este capítulo los indicadores relativos al fraude interno dentro del ámbito administrativo.

Se puede considerar fraude administrativo al producido en relación con la actividad de gestión básica de la Entidad, no siendo en este caso un fraude que se produce única y exclusivamente en el entorno financiero sino que es aplicable a cualquier Empresa, con las lógicas diferencias que se producen en relación con los activos de las mismas.

Tal como se indica en la Introducción al presente trabajo, la mejor forma de evitar la realización del fraude consiste en la existencia de una serie de controles que cumplan dos labores fundamentales:

- El aviso temprano de que puede estar produciéndose una situación anómala que tal vez convenga analizar en profundidad.
- La dificultad añadida que tiene la persona que quiere cometer el fraude cuando conoce que hay una serie de alarmas que pueden activarse, aunque no sepa cuáles son.

Consideramos que existen tres grandes grupos en los que se pueden agrupar los indicadores de fraude administrativo:

- Facturas y Proveedores.
    - Facturas incompletas, indocumentadas …
    - Pago a proveedores inexistentes.
    - Pago múltiples a proveedores.

- Retribuciones y Gastos de Empleados.
    - Exceso de autorizaciones.
    - Cargos auto-autorizados.

- Cargos sobre partidas presupuestarias no autorizadas.
- Alteraciones presupuestarias.
- Incumplimiento de políticas de autorización.

- Otros Indicadores sobre Empleados.
  - Indicadores Vacacionales / Presenciales / Rotacionales en relación con el puesto de trabajo.
  - Uso inadecuado de las tarjetas de crédito de la Empresa.

Las fuentes para la obtención de los datos dependerán de los Sistemas Informáticos de cada Entidad, siendo los siguientes Departamentos los que tendrían la información:

- Seguridad y/o Seguridad Informática para todos los aspectos relacionados con accesos físicos o lógicos, así como los informes sobre la situación de los empleados.
- Calidad, que recogerá las reclamaciones de los clientes.
- Control para los asuntos contables.
- Administración para lo referente a proveedores.
- Inmovilizado que posee la información referente a los inventarios.
- Recursos Humanos para los datos de los empleados, tanto personales como salariales.
- Medios de Pago para los indicadores relacionados con las tarjetas de crédito, débito o Empresa.

Facturas y Proveedores

1. Existencia de relaciones familiares o de negocios entre el personal que interviene en los procesos de facturación y los proveedores o clientes implicados en la misma.
2. En relación a los elementos inmovilizados se proponen como indicadores del nivel de riesgo el número de errores producidos en los pagos periódicos correspondientes a los

edificios y vehículos como:

- Alquileres.
- Seguros.
- Tasas.
- Tributo.

3. En el caso de que se emitan facturas, se propone como indicador de nivel de riesgo de fraude:

   - Porcentaje de facturas emitidas:
     - Erróneas.
     - Duplicadas.
     - Devueltas..

   - Porcentaje de anulación de los apuntes contables relacionados con la emisión de facturas.

4. Igualmente, con respecto a las facturas emitidas, se propone como indicador del nivel de riesgo la existencia de pagos con fecha anterior a la de emisión.

5. Para las facturas emitidas por los proveedores, los indicadores propuestos son:

   - Porcentaje de pagos contabilizados con posterioridad a la fecha en que teóricamente se realizaron.
   - Porcentaje de pagos trasladados de Ejercicio contable.

6. Coste del bien o servicio suministrado se encuentre por encima del importe de mercado de un producto de similares características.

7. Número de partidas presupuestarias excedidas cuyo nivel de

autorización no es el adecuado.

8. Errores encontrados en la revisión de los datos identificativos de los proveedores existentes en la aplicación.

9. En el caso de existencia de una lista de proveedores autorizados para diferentes productos, se propone como indicador la existencia de pedidos de productos no autorizados al proveedor o la contratación a un proveedor no autorizado.

Retribuciones y Gastos de Empleados

1. Con respecto a las autorizaciones para la realización de horas extraordinarias los indicadores propuestos son:

   - Existencia de auto-autorizaciones.
   - Autorizaciones para “días valle” y falta de ellas para épocas con carga de trabajo estacional.

2. En relación a las horas extraordinarias:

   - Porcentaje de variación con respecto al mismo período del Ejercicio anterior.
   - Porcentaje de variación de horas totales en un período entre dos centros de trabajo de similares características.

3. En relación con el uso de “Vales Comida”, “Cheque Carburante” y demás documentos acreditativos de pago en especie como “Ticket de Taxis”, “Facturas de Hoteles”, “Billetes de Medio de Transporte”:

   - En el caso de que el documento tenga fecha de caducidad: porcentaje de utilizaciones realizadas en las fechas próximas a las que se podría usar.
   - Disparidad en la periodicidad de su uso, como estar un período sin gastarlos y después utilizar varios en un corto intervalo de tiempo.

- Uso de los mismos en fecha y hora, en principio, incompatibles con el período al que están designados, como:
  - Su uso en Festivos.
  - Uso de varios consecutivos en el mismo establecimiento.

4. En el caso de que exista la figura de “Anticipos para Gastos” que luego son reintegrados, los indicadores que se proponen son:

   - Peticiones consecutivas de “Anticipos” por un importe muy superior al justificado aunque se reintegre.
   - Peticiones de “Anticipos” posteriormente anuladas y por tanto reintegradas.
   - Peticiones de “Anticipos” cercanos a fechas de cargos conocidos como, amortización de préstamo, cuotas de tarjetas, …

5. Con respecto a la aplicación de Nóminas:

   - Errores encontrados en la revisión de los datos dados de alta o modificados en el período.
   - Diferencias existentes en el cotejo entre las modificaciones producidas y su correspondiente autorización.
   - Tiempo que pasa entre las revisiones del log de la aplicación.

6. Con respecto a los préstamos concedidos a los empleados:

   - Errores encontrados en las características de los mismos en relación con los estándares de la Entidad.
   - Cuando el préstamo no es estándar, los errores existentes en relación con la autorización existente.

7. En relación con las Tarjetas de Empresa para el pago de gastos:

- Errores existentes en la petición de las mismas bien por personas sin el suficiente nivel de autorización o para beneficiarios que tampoco lo están.
- Errores producidos en las liquidaciones debido a la existencia en las mismas de gastos particulares, no asumibles por la Entidad.
- Uso de las mismas para obtener Reintegros en Efectivo.

8. En cuanto al seguimiento de otras malas prácticas y usos indebidos de los recursos de la entidad, para evaluar el nivel de riesgo se proponen los siguientes indicadores:

   - Medios de pago de la empresa (tarjetas de crédito, cheques gasolina, VIA-T, etc.).

9. Utilización desmesurada de teléfono, Internet, etc.

Otros indicadores sobre empleados

1. En el caso de que para acceder al puesto de trabajo se necesite hacer uso de una llave, o tarjeta de autorización, un indicador de riesgo es el porcentaje de pérdidas de la misma que se producen en relación con el número de empleados.

2. En cuanto a los hábitos de conducta de los empleados, se propone el siguiente conjunto de indicadores para medir el de nivel de riesgo:

   - Empleados con presencia continuada.
   - Días de vacaciones no consumidos.
   - Número de empleados con la marca (subjetiva) de hábitos de vida ‘poco saludables’ (juego, drogas, alcohol, etc.).

- Número de empleados con ratio de rotación de puesto de trabajo con desviación respecto a umbral de la media.

3. Acerca del comportamiento de los empleados:
   - Número de empleados con la marca (subjetiva) de problemáticos o conflictivos.
   - Altas / Bajas médicas coincidiendo con fechas especiales en las que se realizan mas operaciones que un día normal, y donde, por consiguiente, aumenta también el porcentaje de incidencias.
   - Número de usos indebidos de información reservada.
   - Número de no devoluciones de elementos acreditativos (tarjetas de visita, llaves de mobiliario, llaves/tarjetas de acceso especiales, etc.).

4. En el caso de que el empleado tenga acceso a la operativa contable de la entidad:
   - Ingresos de efectivo en las cuentas del empleado o de sus familiares.
   - Operaciones contables ínter centros.
   - Abonos manuales de intereses.

5. En cuanto a la situación económica del empleado:
   - Empleados con riesgos vencidos y no liquidados.
   - Incrementos sobre umbral en el riesgos en otras entidades de crédito.
   - Número de empleados con marca (subjetiva) de signos externos de riqueza por encima de sus posibilidades, sin respuesta satisfactoria como herencia, sorteo, …

6. En el caso de tarjetas, de claves de coordenadas, pines, y firmas electrónicas:

- Número de quejas de los clientes con respecto al extravío de la documentación.
- Número de errores encontrados en la revisión de cuentas canceladas que todavía tienen asociada alguna tarjeta.
- Número de anulación de comisiones, incremento de límites, autorización de descubiertos, fraccionamiento de pagos, y demás operaciones realizadas sobre instrumentos asociados a cuentas de empleados, sus familiares, vecinos, …

5.4.2. Informático

En este capítulo se enumeran indicadores de alto nivel que nos pueden alertar si hay algún riesgo de fraude interno informático. Entendemos por fraude interno informático aquel fraude que se consigue mediante el uso indebido de las plataformas informáticas que soportan las aplicaciones que existan en la entidad y que dan soporte al negocio de la entidad.

Se han agrupado los indicadores según el entorno en el que aplican:

- Control de Acceso.
- Integridad y Disponibilidad.
- Económicos.

Para cada uno de ellos, y en cada entidad, se deberá considerar desde qué repositorio de datos se deben obtener, y qué mecanismos y umbrales se fijan para evitar falsos positivos.

Las fuentes de datos pueden ser:

- registros de actividad del sistema o del servicio.
- ficheros o parámetros de configuración.
- librerías de programas.

- diarios del sistema.
- o los proporcionados por herramientas de seguimiento y control.

También debería especificarse el área de control que debería hacer el seguimiento.

Estas áreas de control son las que deben tener los indicadores con mucho más detalle, y agrupados por diferentes conceptos, empresas, día/hora, transacciones, etc. según su experiencia, así como los umbrales o niveles a partir de los cuales generar alertas, o correlacionar con otros indicadores relacionados.

En las páginas siguientes se proponen algunas de las posibles agrupaciones.

Indicadores de Control de Acceso

1. Respecto a la gestión de usuarios, se proponen como indicadores de nivel de riesgo:
   - Número de usuarios activos en los sistemas importantes de la entidad, clasificados según sean Internos o externos.
   - Número de autenticaciones incorrectas en los diferentes sistemas.
   - Número de usuarios bloqueados en los diferentes sistemas por autenticaciones incorrectas.
   - Número de usuarios de sistemas sin fecha de caducidad.
   - Número de autorizaciones temporales (24h) de acceso a sistemas, ficheros, transacciones y entornos. (solamente en el caso que se dispongan de sistemas de autorización temporal).
   - Número de usuarios de Sistemas Medios con permisos de administrador que no están gestionados de forma centralizada ya sea manualmente o mediante herramientas automáticas.

2. Respecto a la gestión de los entornos a los que dichos usuarios tienen acceso:
   - Número de entornos para los que se han pedido autorizaciones temporales de acceso
   - Número de ficheros para los que se han pedido autorizaciones temporales de acceso
   - Número de transacciones para las que se han pedido autorizaciones temporales de acceso.

3. En cuanto al tipo de información a la que se accede:
   - Número de accesos a información sensible: tarjetas de crédito, planes de pensiones, datos de clientes, etc. diferenciando a los clientes VIPs.
   - Número de accesos a la operativa financiera desde empresas subcontratadas utilizando un número de empleado de la Caja.
   - Número de accesos a la operativa financiera por parte de personal externo con permisos iguales o superiores al de Director de Oficina.
   - Número de usuarios especiales de Host que se han utilizado.
   - Número de transacciones realizadas por personal externo
   - Número de empleados externos que ha ejecutado transacciones de consulta de datos personales de clientes.

4. En cuanto a los accesos que se realizan desde puntos fuera de las instalaciones de la entidad, se propone realizar seguimiento de indicadores del tipo:
   - Número de accesos vía entornos tipo VPN/Proxy inversos.
   - Número de accesos infructuosos vía entornos tipo VPN/Proxy inversos.

- Número de usuarios bloqueados en los entornos VPN/Proxy inversos.

Indicadores de Integridad y Disponibilidad

1. En cuanto al uso fraudulento de la infraestructura en beneficio propio se propone realizar el seguimiento de:

   - Número de transacciones de los diferentes sistemas finalizadas con error.
   - Número de accesos a las BBDD, por medios técnicos al margen de las transacciones financieras, para consultar o modificar información.
   - Utilización herramientas de modificación masiva tipo INSYNC para modificar datos del entorno de producción.
   - Número de traspasos de programas y entidades al entorno de producción.
   - Número de traspaso de programas y entidades en el entorno de producción en período crítico.
   - Número de días con incidencias en el backup de datos (o días sin backup).
   - Número de interrupciones (Abends) de programas en producción.
   - Porcentaje de PCs con el antivirus actualizado versus PCs con el antivirus obsoleto.

2. En cuanto a modificaciones de los filtros de seguridad:

   - Número de cambios en las políticas de Firewalls.
   - Número de cambios en las firmas de IDS/IPSs.

- Número de servicios activos en los servidores y equipos de comunicaciones que no son necesarios y que pueden comportar riesgos.
- Número de Servicios FTP anónimo en los servidores y equipos de comunicaciones que no son necesarios y que pueden comportar riesgos.
- Porcentaje de comunicaciones cifradas.

3. En cuanto a totales de control:

   - Totales de control que implican la agrupación manual de transacciones en la fase de entrada y un recuento en la fase de salida, lo que permite establecer un control total sobre todo el grupo. Los totales más habituales pueden ser:
     - recuento de documentos.
     - conteo de líneas.
     - totales numéricos.
     - totales de efectivo.

Indicadores Económicos

1. En cuanto al uso ineficiente de la infraestructura que pueda esconder algún tipo de irregularidad:
   - Número de transacciones con mayor consumo de CPU.
   - Número de Servidores con poca o nula actividad.
   - Número de Servidores instalados obsoletos.
   - Número de servidores activos versus número de equipos en mantenimiento.
   - Número puestos de trabajo activos versus número de empleados.

2. En cuanto a la calidad del software que utiliza la infraestructura:
   - Número de firmas de código malicioso detectadas por los sistemas de control.
   - Número de correos SPAM rechazados o marcados por la infraestructura de correo de la entidad.

5.4.3. Contable

Se enumeran en este capítulo los indicadores relativos al fraude interno dentro del ámbito contable.

Por fraude interno contable se ha entendido aquél que tiene su origen en el uso indebido de los datos, los procedimientos ó los sistemas que soportan el conjunto de la información contable de la entidad.

Los indicadores se han agrupado en las siguientes familias:

- Generales.
- Apuntes manuales.
- Ambiente TI.

Como fuentes de datos típicas para alimentar los indicadores propuestos en páginas siguientes, se plantean principalmente:

- bases de datos que soporten la información contable básica (diario, mayor, etc.).
- bases de datos que soporten la información contable derivada (facturas, presupuestos, etc.).
- registros y logs de los sistemas que almacenan los datos de los dos puntos anteriores.

Conviene recalcar que en cuanto los indicadores de este capítulo cobra especial relevancia todo lo que tiene que ver con el apoyo en

datos históricos, y su explotación comparativa para la generación de los indicadores propuestos.

La “sintonización” de dichos indicadores en cuanto a parámetros, umbrales, etc. quedará al arbitrio y la experiencia de uso del auditor, para evitar la aparición excesiva de falsos positivos y promover la generación de resultados relevantes y con valor añadido.

Generales

1. Respecto a los plazos de cierre de ciclo contable, se propone como indicador de nivel de riesgo:
   - Número de apuntes demorados respecto al cierre sobre umbral temporal determinado por usuario (o, alternativamente, por centro operante).
   - Número de apuntes de corrección efectuados tras el cierre de ciclo por usuario.

2. Respecto a la realización de apuntes contables por importes que se consideren excepcionales:
   - Incremento superior a un umbral por usuario (o, alternativamente, por centro) y período de tiempo de este tipo de apuntes, tanto por número de operaciones como por importe agregado de las mismas.

3. En cuanto al número total de asientos contables que se realizan:
   - Incremento superior a un umbral por usuario (o, alternativamente, por centro) y período de tiempo del número total de apuntes efectuados, con independencia de su importe.

4. En cuanto al importe agregado total de los asientos contables realizados:

- Incremento superior a un umbral por usuario (o, alternativamente, por centro) y período de tiempo del importe total de los apuntes efectuados, con independencia de su importe.

5. Respecto a las partidas pendientes de aplicación, se propone el siguiente conjunto de indicadores de nivel de riesgo, todos ellos definidos por usuario y/o centro durante un período de tiempo:
   - Número y/o importe agregado de partidas pendientes por un plazo superior a un umbral determinado.
   - Incremento ó decremento superior a un límite del número ó importe agregado de partidas pendientes.
   - Existencia de partidas sin autorización de centro responsable.
   - Existencia de partidas por importe atípico.
   - Existencia de partidas sin concepto informado.

6. En relación con las partidas con saldo inconsistente, se propone como indicador de nivel de riesgo:
   - Existencia por centro de partidas con saldo inconsistente con antigüedad superior a un umbral determinado, con independencia de su importe.

7. Sobre las partidas imputadas entre centros, se propone el siguiente conjunto de indicadores de nivel de riesgo, todos ellos definidos por usuario y/o centro de origen del apunte durante un período de tiempo:
   - Número y/o importe agregado de apuntes pendientes de corresponder por un plazo superior a un umbral determinado.
   - Incremento ó decremento superior a un límite del número ó importe agregado de apuntes con un mismo centro de inicio y destino.

- Existencia de apuntes no correspondidos en el centro de destino después de un plazo de espera superior a un umbral definido.
- Existencia de apuntes por importe atípico.
- Existencia de apuntes sin concepto informado.

8. Respecto a la coherencia de los apuntes efectuados y partidas existentes con el Plan de Cuentas vigente en la Entidad:
   - Existencia por centro de apuntes incoherentes con el Plan.

Apuntes manuales

1. Sobre el marcado de todos los apuntes contables efectuados manualmente:
   - Incremento superior a un umbral por usuario y período de tiempo del número de apuntes ó del importe agregado de operaciones manuales.
   - Existencia de apuntes sin concepto informado.
   - Si el sistema no presenta cortapisas que invaliden el método, grado de ajuste de los importes por centro y/o usuario a la Ley de Benford por debajo de un umbral determinado.

2. En cuanto a los apuntes contable que requieren autorización en función del importe, centro operante y cuenta en la que se asienta manualmente:
   - Incremento superior a un umbral por usuario y período de tiempo del número de apuntes ó del importe agregado de operaciones manuales sujetas a autorización.
   - Parejas usuario autorizador-usuario autorizado en que el volumen de autorizaciones, por número ó importe, es anormalmente elevado en términos relativos, o sufre un incremento superior a un umbral determinado.

Contable

3. En relación con las transacciones realizadas manualmente y rechazadas por el sistema. Propuesta de indicador:
   - Usuarios con número de transacciones rechazadas (o, alternativamente, un importe agregado) superior a un umbral determinado por período de tiempo.
   - Usuarios con un incremento superior a un umbral determinado del volumen de transacciones, por importe agregado ó número y período de tiempo.

4. Sobre los apuntes manuales de corrección:
   - Usuarios con número de transacciones de corrección (o, alternativamente, un importe agregado) superior a un umbral determinado por período de tiempo.
   - Incremento superior a un umbral por usuario y período de tiempo del número de apuntes (o, alternativamente, del importe agregado) de operaciones corrección.

Ambiente TI

1. En cuanto al acceso en modo usuario a los aplicativos de contabilidad de la Entidad:
   - Intentos de acceso no autorizado.
   - Incremento superior a un umbral por usuario y período de tiempo del número de accesos.
   - Accesos en horario atípico.
   - Accesos con el usuario en situación de baja, vacaciones, etc.

2. En relación con el acceso directo a tablas contables, se propone el indicador de nivel de riesgo:
   - Por usuario: escritura directa en tabla.

3. Sobre el cambio de versiones ó introducción de nuevos aplicativos en el software de contabilidad:
   - Cambios de versión recurrentes por encima de umbral.
   - Cambios de versión ó introducciones no validadas por responsable.
   - Cambios de versión ó introducciones realizadas al margen de un calendario de planificación, ó violando lo estipulado por éste.

4. En cuanto a la modificación manual de los ficheros de interfaz:
   - Por usuario: cambios efectuados.

5. En relación con la modificación manual de los logs del sistema:
   - Por usuario: cambios efectuados.

5.4.4. Operativo

Entendemos por fraude interno operativo, aquel que se realiza mediante la manipulación directa de elementos disponibles durante la realización de la operativa habitual. Esto incluye fraudes de tipologías diversas como la sustracción de efectivo, el desvío de fondos de clientes o la apropiación de riesgos concedidos a clientes ficticios, entre otros.

La utilización de los mecanismos disponibles para la realización normal de la operativa es posiblemente el método al alcance de un mayor número de empleados que pudieran tener la intención de cometer un fraude. Por este motivo, siguiendo los principios establecidos en las metodologías de gestión de riesgos, la primera cuestión a abordar consistiría en adoptar un conjunto de salvaguardas adecuadas para mitigar los riesgos más significativos que se hubieran podido identificar tras la realización de un análisis de riesgos. Este conjunto de salvaguardas, consistirán habitualmente en controles a incorporar en las aplicaciones y procesos, que dificulten o impidan la realización de operaciones inadecuadas o no autorizadas.

Aunque como se ha indicado, el riesgo de fraude puede reducirse notablemente cuando existan controles adecuados, ya sea por limitaciones prácticas o por fallos en el diseño de estos, los controles no van a poder impedir habitualmente la totalidad de situaciones posibles de fraude. Por este motivo, resulta necesario disponer de mecanismos de vigilancia adicionales que posibiliten detectar los posibles fraudes que hubieran podido perpetrarse, aún a pesar de la existencia de dichos controles.

En este punto es donde se ubican los indicadores que a continuación van a exponerse. Son elementos de alerta que pueden indicar la posible existencia de fraudes internos realizados a través de la operativa habitual. Se quiere recalcar el hecho de que por sí solos no indican la existencia de un fraude (a día de hoy no resulta posible detectar fraudes de manera exclusivamente analítica), pero si constituyen señales de alerta que avisarían de que algo anómalo puede estar sucediendo y que tras el análisis de los mismos por personal experimentado, puede deducirse que detrás de ellos pudiera existir algún tipo de fraude e iniciar una investigación al respecto.

Como información de partida para la elaboración de estos indicadores se utilizarán principalmente las siguientes fuentes:

- La disponible en aquellos ficheros (diarios de terminal y de aplicaciones) en donde quede recogida la operativa realizada por cada empleado.
- La recogida en aquellos ficheros donde esté almacenada la información sobre clientes y sus contratos.
- La almacenada en los ficheros donde se recojan los movimientos realizados sobre los contratos.
- La contenida en ficheros que recojan la actividad de aplicaciones que impliquen intercambios económicos entre entidades (cheques, transferencias).

Quebrantos de moneda

Se propone el siguiente conjunto de indicadores:

- Oficinas con un mayor número de diferencias (ponderadas en función del número de operaciones de efectivo que realizan).
- Oficinas con un mayor importe de diferencias (ponderadas en función del número de operaciones de efectivo que realizan).
- Patrones anómalos en la distribución de importes de las diferencias de una oficina.
- Patrones anómalos en la distribución temporal de las diferencias de una oficina (días del año en que dichas diferencias).
- Variaciones (incrementos) en el número de diferencias en una oficina respecto de las que se produjeron en años precedentes.

Sustracción de activos físicos materiales

En relación a las posibles sustracciones o apropiaciones indebidas de activos físicos materiales de la empresa por parte de empleados, se proponen los siguientes indicadores (medidos siempre en importe del activo echado en falta):

- Faltas de material promocional.
- Faltas de material de oficina.
- Falta de material de decoración (cuadros, lámparas, etc.).
- Falta de equipos informáticos (o de componentes).
- Falta de objetos de biblioteca (libros, CD's, etc.).

Manipulación de datos de clientes

En relación a la identificación de clientes:

- Número de documentos de identificación cuya numeración no sea válida o que no parezca lógica atendiendo a otros criterios (por ejemplo la edad registrada).

- Número de clientes cuyo nombres, asociado al documento de identidad, pudiera no coincidir tras cruzarlo con otras fuentes.

En cuanto a las direcciones de clientes:

- Por centro, direcciones anómalas dadas de alta (no válidas o que no parezcan lógicas atendiendo a otros conceptos, con especial atención al uso de códigos postales).
- Cruce de clientes con direcciones anómalas con otros datos de los clientes y sus productos.

Anomalías en los patrones operativos de un empleado

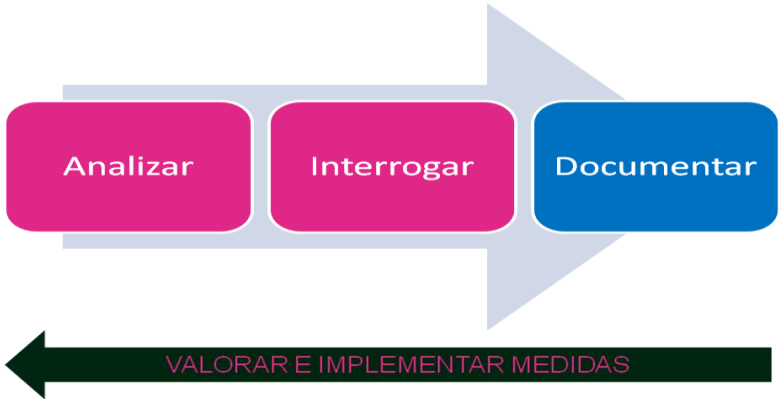
En cuanto a la operativa de un empleado fuera de su centro de trabajo habitual:

- Número de empleados con operativa fuera de su centro habitual, sin motivo para ello.
- En relación a la operativa fuera del horario habitual:
- Número de empleados que trabajan fuera de su horario habitual (teniendo en cuenta que el término habitual puede variar según cada perfil de empleado), teniendo en cuenta el perfil de los clientes sobre los que se realizan operaciones.
- En cuanto a la operativa de empleados que realizan operaciones encontrándose de baja, de vacaciones ó ausente por cualquier otra causa tipificada:
- Número de empleados que operan estando de baja o vacaciones, teniendo en cuenta el perfil de los clientes sobre los que se realizan operaciones.
- En relación a los patrones anómalos en la operativa de un empleado respecto de su perfil:
- Empleados con desviación anómala (sobre umbral) en su patrón operativo: variaciones en los volúmenes y/o importes de las operaciones de cada tipo que realice y que no se correspondan con un cambio de función.

6. Tratamiento del Fraude Interno

6.1. Como actuar frente al evento de fraude interno

Somos conocedores de un fraude interno….. y ahora ¿qué?



Una vez que la empresa es conocedora de una actuación sospechosa de fraude interno, sea cual sea la fuente de información está deberá activar el protocolo que debe estar previamente definido para estos casos. Por ello es importante, como hemos señalado que exista un órgano que realice la función de gestionar el fraude interno.

Es importante que cuantas más fuentes de información tengamos para la gestión del fraude, mucho mejor (denuncia de un cliente, canal de denuncias interno, resultado de una auditoría, servicio de atención al cliente, mystery shopper, etc…). Si la denuncia llegará a través del canal de denuncias y se estimará que carece de fundamento, se comunicará al denunciante la decisión de no proseguir con la investigación, con la finalidad de dar opción a añadir nueva información i/o evidencias.

A continuación, vamos a detallar a grandes rasgos, los pasos que debe tener un protocolo de actuación en este ámbito:

El Departamento o persona que tiene la función de tratar los casos de Fraude Interno (debe estar definido en el Organigrama y definición de funciones), será quien centralizará toda la información y realizará:

1. ANALISIS/INVESTIGACIÓN:

Una investigación en profundidad del caso. Se debe analizar y **documentar toda la investigación**. La fase de investigación, no finalizará hasta que se tenga la seguridad razonable de la culpabilidad o no culpabilidad del presunto defraudador.

Puede ser aconsejable en función de la gravedad y elementos objetivos de culpabilidad dar un permiso retribuido al presunto defraudador, hasta la finalización de todo el proceso.

En relación a las investigaciones, puede ser necesaria la externalización de estos servicios hacia empresas de investigación privada. No hay que olvidar que la Ley 5/2014 de Seguridad Privada habilita de manera exclusiva a los detectives privados para la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares.

La propia Circular de la Fiscalía General del Estado Destaca que muchas de estas funciones podrán ser realizadas de manera más eficaz de forma externa, como sucede por ejemplo con la posible externalización de los canales de denuncia o de la propia investigación.

Somos conocedores de un fraude interno….. y ahora ¿qué?

Fuentes internas

- Monitorización de datos
- Imágenes
- Documentación
- Interrogatorios
- Controles (existentes o nuevos)

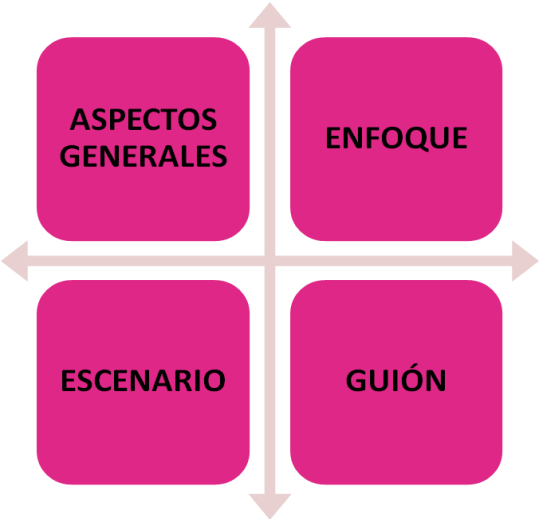
Fuentes externas

- Internet
- Detectives privados
- Entrevistas
- Documentación
- Forensics

2.ENTREVISTAS PERSONALES / INTERROGATORIOS:

Entrevista personal con el presunto defraudador, aportando toda la documentación y hechos objetivos que se han detectado durante la investigación. Además se realizaran entrevistas a las personas vinculadas con la investigación.

Podemos agrupar las fases de los interrogatorios en 4:



Aspectos Generales

- No hay que mermar esfuerzos en la preparación.
- La investigación previa del delito debe ser amplia, documentada y cargada de evidencias.
- Se ha de proceder con absoluta discreción. El mejor escenario es aquel que ningún empleado es conocedor de la existencia de una investigación. El efecto sorpresa evitará posibles interferencias y actos que frustren nuestro objetivo.
- Factores favorables: Asertividad y Empatía.

Enfoque

- Definir los objetivos de la entrevista.
- Definir las técnicas que utilizaremos
- Iniciar la entrevista con aspectos más triviales para ir focalizando cada vez la entrevista hacia nuestro objetivo.

Escenario

- Escoger el lugar. A poder ser el habitual del empleado a entrevistar.
- Ambiente. No tiene que ser tenso.
- Número de personas: Se recomienda un equipo de dos personas. Recuerda que es legal poder gravar las conversaciones en las que participas, sin necesidad de avisar previamente.

Guión

- Predecir lo impredecible.
- No interrumpir las intervenciones del empleado, y jugar con los silencios
- Pruebas y evidencias todos los hechos, hasta aclarecer lo acontecido
- Qué tipo de preguntares se realizaran? Abiertas o Cerradas?
- Utilización de preguntas sugestivas
- Reflexiones
- Acorralar

Errores más típicos:

- La influencia de las preguntas sobre las respuestas.
- Las distracciones.
- Las evaluaciones precipitadas.
- Las prisas. Querer concluir antes de tiempo.
- La contaminación de las entrevistas.
- Perder el control de la entrevista.

3 ELABORACIÓN DE UN INFORME:

Realizar un informe completo de la investigación, y presentarla al Comité de disciplina o, caso de no existir, departamento de Relaciones Laborales. Este informe debe emitirse a partir de hechos **objetivos y documentados.**

El Comité de disciplina, a partir del informe y exposición de los hechos, si se demuestra que hubo una actuación fraudulenta debe abrir un expediente disciplinario y emitir una sanción con los siguientes posibles escenarios:

- Despido
- Apertura de un procedimiento penal.
- Apertura de un procedimiento civil.
- Amonestación
- Establecimiento de medidas disciplinarias. Es necesaria la graduación de las mismas en función de la gravedad.
- Solicitar una reclamación al seguro contratado.
- Continuar con la investigación, implantando nuevos procedimientos.
- Implantación de nuevos procesos de negocio y de control.

6.2. Sistema Disciplinario

El apartado 5 del artículo 31 bis del Código Penal establece que los modelos de organización y gestión deberán contar, entre otros requisitos, con el establecimiento de un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el propio modelo. Añade que además se deberán realizar verificaciones periódicas del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

En definitiva, para la implementación correcta de un programa de compliance es imprescindible establecer un procedimiento sancionador preciso. Es fundamental que todos los miembros de las organizaciones sean conocedores de las sanciones aplicables a aquellos que incumplen el contenido del programa de cumplimiento. Evidentemente las sanciones previstas deberán ser conformes a la normativa vigente.

Una vez se ha quebrado el contenido del programa de cumplimiento, hay que demostrar fehacientemente el fraude o acto

ilícito, todo ello habrá que documentarlo con pruebas que corroboren que se ha producido el acto fraudulento detectado.

Las actuaciones de la empresa en relación a la toma de decisiones relativas a la ejecución de su sistema disciplinario deben tomarse sin dilación, es la mejor medida preventiva, y sin duda la mejor decisión empresarial. Las actuaciones fraudulentas del infractor deben acarrearle consecuencias negativas.

6.3. Cómo analizar documentos en un Fraude

Los examinadores del fraude a menudo obtienen gran cantidad de documentación como parte de la evidencia cuando están conduciendo una investigación por fraude. Es fundamental que el investigador entienda la relevancia de ésta evidencia y cómo debe ser tratada y presentada.

Un documento puede salvar o herir una investigación dependiendo de cuál sea y cómo sea presentado

A pesar de que muchos investigadores pueden quedarse horas y horas examinando documentación, deben tener en cuenta que los documentos no definen un caso, éstos lo definen los testigos.

REGLAS DE MANIPULACIÓN

La relevancia de los documentos es difícil de establecer al inicio de una investigación, es por ello que al principio todos los documentos son relevantes y deben ser manejados siguiendo estas reglas:

- Obtenga los documentos originales de ser posible.
- Haga copias a estos documentos para trabajar sobre ellos.
- No manipule los documentos originales más de lo necesario, estos podrán ser sometidos a análisis forense.

- Mantenga una buena clasificación, sobre todo cuando son demasiados los documentos adquiridos. Perder un documento puede ser catastrófico.
  Mantenga una adecuada cadena de custodia sobre la documentación original y almacene los documentos en un lugar seguro.
- Una vez se entiende la importancia de la relevancia, del manejo con cuidado de la documentación y su clasificación, pasamos al análisis forense.

ANÁLISIS FORENSE DE DOCUMENTOS

Existen muchos tipos de análisis forenses que se realizan sobre documentos físicos. Independiente de los métodos utilizados, el investigador debe:

- Detectar firmas falsificadas, lograr demostrar que la firma no corresponde con el individuo identificado.
- Identificar a los escritores de las firmas y los textos, cotejar estos documentos con otros.
- Detectar documentos alterados, tomar fotografías y usar software de acercamiento.
- Detectar borrones y tachones, analizar elementos utilizados para tal fin de modificación.
- Determinar si el documento fue preparado o generado, en qué impresora y en que software.
- Detectar si el documento fue modificado respecto al original, buscar trazabilidad de movimientos.
- Comparar papeles y tintas usadas, su composición, nivel de gramaje y fabricante.
- Determinar si los documentos provienen de una misma resma, de un mismo cajón de oficina.

- Examinar pliegues y secuencias de arrugas, revisar si en otros documentos también existen
- Comparar rasgados y cortes, cotejar estas características con documentos de los sospechosos en el caso.
- Examinar las copias del documento vía FAX, hora y fecha del envío, revisar cámaras de seguridad.
- Identificar la fuente que lo generó, el computador, la impresora, la persona, la hora, el lápiz, el borrador y la tinta.
- Identificar sobres forzados y cerrados nuevamente, buscar sellos rotos y sobres originales en la basura.
- Detectar texto incrustado entre párrafos, analizar anomalías entre espacios y tipos de parágrafos.
- Revisar los sellos sobre los documentos, intensidad, textura y tinta
- Revisar los estampados mecánicos, de números, fechas de radicación y logos a presión.

Qué sucede si el investigador no tiene las habilidades para llevar a cabo un análisis forense sobre los documentos?,

Se debe acude a fuentes expertas en la exanimación de documentos, que además nos reforzaran con informes probatorios ante un eventual juicio:

- Expertos forenses de compañías privadas: en cualquier clase de casos. En algunos países se requiere que tengan licencia otorgada por el gobierno.
- Grafólogos: podrían identificar la personalidad, carácter, moral y estado mental del escritor basado en el análisis de su escritura.
- Laboratorios del gobierno: en casos donde exista un delito. Puede estar limitado por el acceso a los recursos y el tiempo que tome su reserva.

7. Caso de fraude en una Entidad Financiera

RESUMEN

En este trabajo se describe un caso de fraude interno en una entidad financiera, así como la metodología empleada para su detección, tratamiento y funcionamiento de las herramientas de control. Con el fin de mantener la confidencialidad, las referencias han sido modificadas.

PALABRAS CLAVE

Fraude Interno, controles antifraude, auditoría Interna, apropiación indebida.

7.1. Introducción

Todas las empresas son susceptibles de padecer algún tipo de fraude, ya que cuando hay colusión e intención, es difícil detectarlo y frenarlo. A pesar de esto, se ha visto que este riesgo se mitiga sustancialmente cuando las empresas cuentan con un programa integral que permite combinar mecanismos de cambio cultural con controles internos en los procesos de negocio.

Las Entidades Financieras, bien sea por imperativo legal, bien sea por cultura propia, poseen de una estructura organizativa en la que el control interno tiene un papel cada vez más importante. El modelo de las “Tres líneas de defensa” (3LoD, en inglés) suponen un parámetro de referencia para describir las responsabilidades mediante capas o niveles de actividad que contribuyen a garantizar que los riesgos se gestionan y se supervisan de forma eficiente y eficaz, tal como reconoce el Instituto de Auditores Internos (IIA).

A continuación se detalla un caso de fraude interno de una entidad financiera, detectado a partir de los controles antifraude que realiza la propia entidad.

El fraude interno consistió en la apropiación indebida de saldos de clientes por parte de un empleado de la red comercial de una entidad financiera, el cual realizaba las funciones de Gestor de Banca Privada, y era el responsable de gestionar clientes del segmento de Banca Privada de una zona de Galicia. El segmento de Banca Privada es el que se asigna a aquellos los clientes con saldos superiores a 100.000 €.

El modus operandi del empleado, en adelante Sr. X, consistía en realizar reintegros en efectivo de las cuentas de los clientes (pazos fijos y fondos de inversión), en cantidades entre 1.000 € y 25.000 €, sin el conocimiento ni consentimiento de los titulares de los saldos. Mayoritariamente las personas afectadas por este fraude tenían una edad superior a 70 años, y disponían de la plena confianza del empelado, por haber sido su gestor personal al menos los últimos 5 años.

A lo largo de los 4 años que duró está operatoria, hasta que fue detectada, los reintegros en efectivo se realizaban desde diferentes oficinas y por diferentes empleados de la Entidad. Al final de la investigación, se detectaron un total de 6 clientes afectados por un importe total cercano al **millón de euros**.

Con el fin que los clientes no se alertaran del fraude, el Sr. X tomaba las siguientes precauciones:

- Les decía a los clientes que a veces hacia inversiones en Andorra y por eso no constaban registradas en el ordenador.
- Entregaba documentación a los clientes con de las posiciones globales de saldos, con los importes manipulados. Estos documentos eran de confección manual (en Word) y simulaban los documentos reales de la Entidad.
- Ponía indicadores informáticos en las cuentas de los clientes con el fin que estos no recibieran información directamente de la Entidad Financiera.

- En ocasiones, abría una cuenta corriente a nombre de los clientes, sin su conocimiento, con el fin de canalizar toda la operatoria fraudulenta a través de estas cuentas "full".
- Realiza ingresos en efectivo en las cuentas habituales de los clientes, simulando que correspondían a las rentabilidades de los saldos que previamente había usurpado. En la confección de estos ingresos, indicaba literales como "abono de intereses", "plusvalía fondo", "intereses".
- Tenía la plena confianza de los clientes, procurando ser siempre el único interlocutor entre cliente/banco.
- Los periodos vacacionales del Sr. X, no eran nunca superiores a una semana.

7.2. Como se detectó

La entidad financiera dispone de una serie de controles informáticos, formados por más de 100 alerta susceptibles de operatorias irregulares. Estas alertas se revisan sistemáticamente desde el Departamento de Auditoría Interna con la ayuda de un cuadro de mandos y mediante revisiones a distancia, a la vez que también se realizan visitas periódicas "in situ" a las oficinas.

La operatoria fraudulenta del Sr. X se detectó a partir de la revisión de una de las alertas, concretamente una que está dirigida a detectar ingresos manuales en cuentas de clientes que contengan literales sospechosos. A nivel de ejemplo, se utilizan palabras clave como: "intereses", "complemento", "devolución", "complemento", "comisiones", etc…

En el caso de Sr. X, la Oficina donde estaba asignado presentaba una operatoria inusual, en comparación al resto de oficinas, de ingresos en efectivo en los últimos 12 meses con literales "sospechosos". Analizando los ingresos, se detectó que uno de los clientes tenía un ingreso en efectivo de 27,34 € en concepto de "abono de intereses", y este se realizaba de manera trimestral. Estos ingresos comenzaron a realizarse coincidiendo con la cancelación anticipada de una imposición a plazo fijo de 10.000 €, los cuales tenían un rendimiento del 1,35 % anual:

- 10.000 € al 1,35 % = 135 € anuales = 33,75 € trimestrales.
- Si aplicamos una retención fiscal de 19% (que es lo que el banco aplica en estos casos), tenemos que: 33,75 € son intereses brutos, 6,41 € retención y **27,34 €** seria el neto a abonar el cliente, que **curiosamente** coincide con el importe abonado mediante un ingreso en efectivo al cliente, bajo un concepto engañoso.

A partir de esta primera operatoria susceptible de ser irregular, se revisó ampliamente el cliente y personas vinculadas, observando 15 reintegros en efectivo dudosos por importe de más de 300.000 €.

Adicionalmente se amplió la revisión en búsqueda de otros clientes perjudicados, detectándose hasta 5 clientes con operatorias similares. También se estableció el origen de esta operatoria, situándola 4 años atrás, si bien al principio era muy puntual. Por este motivo había eludido los controles anteriores.

7.3. Tratamiento del fraude una vez detectado

Se realizó entrevistas con estos empleados que efectuaban los reintegros a los clientes perjudicados, siendo sus manifestaciones las siguientes:

- El Sr. X era quien gestionaba en exclusiva a los clientes afectados, en su condición de gestor de banca privada.
- Los reintegros en efectivo de las cuentas de los clientes se realizaban siguiendo instrucciones del Sr. X, dado que él no tenía acceso al efectivo.
- Uno de los empelados entrevistados, manifiesto que el Sr. X le solicitaba efectuar reintegros en efectivo de las cuentas de los clientes, a pesar que estos no estaban físicamente en la Oficina. El Sr. X le manifestaba que tenía que entrevistarse con ellos fuera de la Oficina y que sería él quien le haría la entrega del efectivo en mano. El comprobante firmado se los entregaba durante la mañana o bien el día siguiente.
- Otro de los empleados, manifestó que en ocasiones el Sr. X utilizaba su terminal con su usuario, dado que no tenía costumbre de bloquear el ordenador.

Se realizó entrevista con los clientes perjudicados, confirmando que ellos no eran conocedores de los reintegros, a pesar de la existencia de comprobantes firmados por los clientes. Se detectaron algunas firmas presuntamente falsificadas, que posteriormente un forense las reconoció como tales. A todos los clientes se les detalló las irregularidades detectadas, con el fin de comprobar que no existían otros importes expoliados. Una vez cerrados los importes con los clientes, y con la correspondiente carta de conformidad de los hechos acontecidos, se procedió al abono de las cantidades expoliadas por el Sr. X a los 6 clientes afectados.

Paralelamente con las entrevistas a los clientes, se efectuó una entrevista con el Sr. X, el cual inicialmente lo negó todo. Ante las numerosas evidencias documentales que se mostraron y expusieron al Sr. X, este no tardó en reconocer el fraude, incluso colaboró proporcionando un listado con los importes y clientes afectados, el cual coincidía en su práctica totalidad con los previamente detectados por Auditoría Interna. Al Sr. X, se le abrió un expediente disciplinario que concluyo con el despido y una demanda penal de los hechos.

Con el fin de descartar otros casos no detectados, se realizó un envío de masivo de cartas de conformidad de saldos a una serie de clientes de la oficina: todos los clientes que gestionaba el Sr. X, clientes con saldos superiores a 100.000 € y una muestra aleatoria.

7.4. Controles antifraude: El cuadro de mandos como motor detectivo de fraudes.

El cuadro de mando aglutina más de 100 alertas de operatoria irregular, las cuales se alimentan mensualmente. Estas alertas tienen un peso específico diferente en función de una catalogación previa de riesgo. Cada alerta da una puntuación a cada oficina y/o empleado. Esta puntuación se realiza por metodología comparativa entre los diferentes centros o empleados. Así mismo, la herramienta contiene datos históricos, alertando las variaciones significativas de un centro o empleado entre un periodo determinado. Por tanto, a través del cuadro

de mando podemos obtener un ránquing mensual de centros con alertas potenciales de ser irregular, o bien de centros o empleados con variaciones significativas de alertas.

El cuadro de mandos no es una herramienta de revisión en sí, es una herramienta detectiva de alertas de operatoria irregular. Las revisiones siempre se realizan de manera manual, analizando no sólo la alerta como tal, sino el conjunto de alertas y toda la operatoria del cliente en general. El resultado del tratamiento de las alertas lo podemos dividir en tres niveles:

1. Operatoria OK y no se realiza ninguna acción adicional.
2. Operatoria NO OK, reclamando al empleado una explicación o documentación que justifique la operatoria. Esto sirve, a la vez, de medida preventiva.
3. Operatoria susceptible de FRAUDE. En estos casos, no se alerta a nadie y se analiza el caso de manera global, ampliando las alertas con parámetros más restrictivos si es necesario, hasta descartar que existe un fraude (pasaría a nivel 1 o 2), o confirmar que es un posible fraude. En este último caso se inicia una amplia investigación que finaliza con la realización de un informe al comité disciplinario correspondiente.

Las alertas de operatoria irregular se revisan periódicamente, añadiendo nuevas alertas fruto de la detección de nuevas operatorias de fraude, o bien originadas de la propia evolución de los sistemas informáticos.

7.5. Conclusión

Gracias a los mecanismos de control interno de esta entidad financiera y del correcto tratamiento de los controles antifraude, se pudo detectar la operatoria fraudulenta que estaba realizando el Sr. X., y alertar a los clientes afectados sin que estos sufrieran un quebranto económico.

La detección prematura de los fraudes, tiene un triple efecto beneficioso para la empresa; evita que la propagación del fraude sea

de mayor dimensión, mitiga el riesgo reputacional de la empresa y sirve como elemento altamente preventivo de futuros fraudes.

Desgraciadamente el porcentaje de fraudes internos detectados prematuramente es bajo. Esto se debe a que no existe un perfil tipo de la persona que comete un fraude, estadísticamente está demostrado que cualquier empleado o directivo es susceptible de efectuar un fraude interno, siendo esta una situación impredecible.

8. Colaboraciones de otros profesionales

8.1. Marta Cavadid

Experto Examinador de Fraude (CFE), Especialista Certificado en Anti lavado de dinero (CAMS) y Anti lavado de Dinero y Financiamiento al Terrorismo (AMLCA

Transparencia profesional para combatir los crímenes económicos

El reconocimiento de los delitos económicos como uno de los mayores problemas sociales, políticos y financieros en el mundo y ha sido el punto de partida del movimiento global contra los delincuentes y organizaciones criminales que a través de diferentes tipos de negocios o actos delictivos se apropian de la economía formal dejando a su paso graves consecuencias y pérdidas. De ahí que se hace urgente avanzar en temas educativos acerca de tan espinoso tema, dado que la gran mayoría de personas no tiene pleno conocimiento de lo que representan tales crímenes y sus delitos subyacentes o conexos; y en muchas oportunidades personal administrativo y gerencial asumen riesgos innecesarios involucrándose en actividades comerciales ilícitas con terribles resultados.

La Organización de las Naciones Unidas (ONU) es sus diferentes convenciones ha reconocido como el tráfico ilícito de estupefacientes y sustancias sicotrópicas, terrorismo y financiación del terrorismo,

delincuencia organizada transnacional y corrupción son actividades criminales que afectan la economía global y por lo tanto requieren de toda nuestra atención. Así mismo, ONU invita a la adopción de buenas prácticas y políticas para luchar contra la industria criminal desde el orden gubernativo hasta empresarial.

Sin quedarse atrás en la maratónica tarea de proteger el patrimonio económico, organismos multilaterales como Fondo Monetario Internacional (FMI), Banco Mundial (BM), Banco Interamericano de Desarrollo (BID), Unión Europea (UE), Organización de Estados Americanos (OEA), Grupo de Acción Financiera Internacional contra el Lavado de Activos y la Financiación del Terrorismo (GAFI), Organización para la Cooperación y Desarrollo Económico (OCDE), entre otros, se han pronunciado y unido para fomentar la implementación del sistema de administración del riesgo de lavado de activos y educar en todos los niveles gubernamentales y corporativos acerca de buen gobierno, ética y transparencia.

Así las cosas, prevenir, detectar, reportar e investigar actividades criminales precedentes o fuentes del blanqueo de capitales tales como el uso indebido de información confidencial o privilegiada y manipulación del mercado, tráfico de seres humanos y tráfico ilícito de inmigrantes, explotación sexual, tráfico ilegal de armas, tráfico de mercancías y bienes robados, corrupción, extorsión y soborno, fraude, falsificación de dinero, piratería de productos, delitos ambientales y minería ilegal, secuestro, privación ilegítima de la libertad y toma de rehenes, contrabando y evasión y elusión fiscal son una obligación más, que cualquier ciudadano y en especial contadores, auditores, asesores empresariales y abogados deben contemplar en el diario hacer. Adicionalmente, tal como lo sostienen los diferentes entes reguladores; los profesionales relacionados con las áreas contables, financieras, auditoría y leyes son sujetos obligados para reportar operaciones inusuales y sospechosas de lavado de activos.

Sin embargo, la labor como profesionales debe ir más allá del cumplimiento normativo global y local acerca de la lucha contra el blanqueo de capitales y los delitos fuentes. Cada profesional debe adoptar una postura preventiva que le permita anticiparse a los potenciales hechos criminales que de alguna forma se puedan cometer en la organización sin importar el tamaño, tipo de industria,

zona geográfica o mercado. Contadores, auditores, abogados y asesores empresariales son los primeros llamados a entrenarse sobre los crímenes económicos y la importancia de la prevención y detección temprana.

Igualmente, cada profesional tiene la obligación moral y ética de adoptar una actitud férrea frente a cualquier actividad criminal organizacional. El riesgo a la mala reputación no solo atañe a las corporaciones, más bien, recae sobre los hombros de aquellos profesionales que dedican su experiencia y conocimiento al replanteamiento socio económico de las Organizaciones. Tener un comportamiento ético y ejemplar donde quiera que encuentren debe ser la prioridad diaria, en la cual la cultura ética se construye en cada instante, con cada decisión y actitud en el ejercicio de la profesión como en la vida personal. No dejarse tentar por el maquiavélico mundo criminal debe ser una política de vida, como también la mejor forma de cerrar las puertas a cualquier posible participación en negocios oscuros. Cada profesional tiene un papel activo en la sociedad y por ende en la economía, el cual se debe basar en la ética, valores y moral, para no darle entrada a los agentes delictivos que atentan contra la transparencia y buen gobierno corporativo, teniendo siempre la legalidad de las acciones como el pilar fundamental para el desarrollo de la profesión.

Es una tarea diaria reflexionar sobre el rol en la sociedad y la responsabilidad que se lleva a cuestas como profesionales para participar activamente en la lucha contra los delitos económicos que socaban las organizaciones y por ende la economía global. La ética, los valores y la moral no tienen precio y no se negocian.

R.H. La piedra angular de la disuasión

Como es bien sabido el factor humano es fundamental para el desarrollo del mundo empresarial; y a pesar que los medios de producción son cada vez más automatizados o robotizados, la mano de obra y el talento siguen fortaleciendo las industrias en el mundo. Sin embargo, el éxito empresarial se ve manchado por aquellos que de alguna forma se dejan conquistar por los antivalores y actúan en contra las organización para alimentar fraudulentamente sus bolsillos.

Es por ello que los programas administración de riesgo de fraude deben incluir los procesos de reclutamiento, selección y contratación del personal.

La elección del empleado ideal tiene que ir más allá de la búsqueda subjetiva de candidatos idóneos que cumplen con las condiciones técnicas e intelectuales del cargo a suplir, ya que en términos de administración de riesgos dicha búsqueda debe ser el primer factor de disuasión frente al fraude. Por lo tanto, los departamentos de personal, talento humano o recursos humanos son la piedra angular de la prevención del fraude corporativo y ocupacional, y el primer mecanismo de disuasión.

Si bien es cierto el análisis de las aptitudes físicas y mentales de los solicitantes por medio de entrevistas, pruebas psicométricas y exámenes médicos son vitales para contratar el personal adecuado, también debe estar en la mira y ser un objetivo primordial encontrar el talento humano que realmente esté y quiera estar alineado con los valores de la corporación.

Como es bien sabido los perpetradores se encuentran en todas las esferas y hacen todo lo necesario para romper las normas con el único fin de incrementar su patrimonio y sostener su ritmo de vida. El perpetrador monitorea y detecta las oportunidades, deficiencias y falta de control de su objetivo. Su agudo olfato e instinto para detectar laxos controles le ayudan a crear las estrategias necesarias para irrumpir en las finanzas y en general en los activos de la empresa y tomar de allí lo que le satisfaga. Un perpetrador no tiene escrúpulos y en muchos casos buscan las empresas con carencias administrativas y financieras; es decir un perpetrador tiene un target y perfila su víctima cuidadosamente. Pero, ¿Cómo puede un empresario proteger su organización desde el departamento de Recursos Humanos o Contratación?

La disuasión de la comisión de fraude empieza por casa y debe ser desde el mismo momento o contacto que tiene el candidato laboral con la empresa; es por ello que un ambiente de total control y la férrea actitud frente al fraude son las herramientas básicas de disuasión.

La importancia de conocer al empleado a contratar comienza con la debida diligencia. El empleado es parte fundamental de empresa; por ende se debe conocer la mayor cantidad de aspectos e información sobre la persona para determinar el nivel de riesgo que implica su contratación o si por el contrario su vinculación debe ser descartada dado la calidad de persona y sus actividades. Por lo tanto, a debida diligencia del cliente (DDC) debe ser un proceso de obligatorio cumplimiento adoptado en las empresas sin importar su tamaño, tipo de negocio, canal y/o productos. Incluso, personas naturales o individuos que requieran contratar personal temporal para determinadas actividades, deberían usar esta herramienta y evitar ser el blanco de la industria criminal. En todo caso, entre más información se obtenga del potencial empleado, menor será el riesgo de comisión de un fraude ocupacional.

El Reglamento Interno de Trabajo (RIT) o el Código disciplinario para los empleados son las herramientas más básicas y conocidas del mundo laboral. Su redacción debe contener aspectos fundamentales sobre faltas graves y menos graves relacionadas con el fraude corporativo y ocupacional o los riesgos a los cuales está expuesta la empresa en este tipo de temas. Es decir, que el RIT, no debe ser la simple y tradicional recopilación de cláusulas o artículos relativos a la forma de laboral, y más bien debe ser el complemento legal y laboral que alineado con el ambiente de control y el buen gobierno corporativo haga parte de la cultura organizacional de cero tolerancia a las actividades delictivas; de modo que desde el inicio de las labores esté claro para el nuevo empleado la inflexible actitud al fraude.

El Código de Ética del buen gobierno corporativo es otra herramienta que protege la Entidad o Corporación por medio de la orientación, supervisión y control de los riesgos; de ahí que los candidatos a suplir las vacantes y los nuevos empleados que pretenden cometer fraude sienten desestimulo al observar que cada una de las personas que laboran en la Organización están comprometidos con la transparencia y la ética a lo largo y ancho de las transacciones de la compañía.

El programa de Administración de Riesgos de delitos económicos es uno de los recursos más avanzado que permite proteger a la empresa de futuros riesgos y por ende consecuencias económicas

que en algunos casos son pérdidas incalculables. El objetivo del programa de administración de riesgo es la promoción de la prevención y detección temprana para evitar procesos costosos de investigación y litigios. Es por ello que el programa se fundamenta en los riesgos que cada proceso pueda generar a la Organización, donde el área de Recursos Humanos o Talento Humano es vital para garantizar éxito en la contratación del nuevo personal.

Por lo tanto, los procesos de reclutamiento, selección y contratación del personal que son desarrollados por el Departamento de Recursos Humanos o de quien haga sus veces deben ser la piedra angular de cualquier programa de administración de riesgo de fraude o lavado de activos. Igualmente, un adecuado ambiente de control debe involucrar herramientas que le permitan al área de recursos humanos fortalecer la percepción de tolerancia cero y actitud férrea frente al fraude desde el primer contacto entre el candidato y la empresa demostrando Congruencia e integridad y tomando la actitud antifraude como estilo de vida laboral.

8.2. Isabel Casares San José-Marti

Economista. Actuaria de seguros. Asesora Actuarial y de Riesgos.

Fundadora y Presidenta de CASARES Asesoría Actuarial y de Riesgos, S.L. http://www.mcasares.es/

Más allá del Fraude Interno: La necesidad del control interno en las empresas

El objetivo fundamental de cualquier principio es tener claro los conceptos que se utilicen para los análisis de los riesgos empresariales y que todos conozcan el alcance del control y el resultado de los mismos, ya que existen muchas metodologías y muchos enfoques distintos para una gestión de riesgos empresariales.

El objetivo de este apartado es ayudar a entender la necesidad de gestionar los riesgos de una empresa y no sólo a reducirlos, por lo que puede generalizarse para todo tipo de riesgos, incluidos los riesgos estratégicos, legales, crediticios, tecnológicos, de mercado, etc. Para una buena gestión de riesgos de una empresa es necesario contemplar todas las etapas fundamentales de identificación, evaluación, respuesta y supervisión, pero es en la etapa de identificación de los riesgos donde podemos detectar además de las amenazas para la empresa, las oportunidades de negocio que pueden ser aprovechadas para la misma y que en un principio puede estar oculta tras las amenazas. Se puede confirmar que tanto la gerencia de los riesgos como un adecuado sistema de control interno pueden contribuir al logro de objetivos empresariales.

El establecimiento de sistemas de control interno sobre la estabilidad y solvencia, requeridos por las prácticas de buen gobierno, exige la capacidad de las empresas para establecer modelos dinámicos que permitan evaluar la situación de la misma ante la

concreción de determinados riesgos desfavorables que pudieran ser objeto de aseguramiento con terceros.

El buen gobierno de una sociedad en general exige el establecimiento de un control interno adecuado que permita a la dirección de la empresa la toma decisiones, por lo que las empresas deben analizar los riesgos que les son propios de su actividad y mantener unos mecanismos específicos de control interno que aseguren la supervisión continuada de los mismos.

Es necesario que exista transparencia en la información, de forma que pueda ser detectada cualquier amenaza lo antes posible para poder reducir o anular el impacto antes de que este se produzca. Nos encontramos ante una demanda creciente de información por parte de la empresa, a raíz de la aparición de nuevas exigencias que afectan a las empresas cotizadas en materia de responsabilidad social, medio ambiente y sostenibilidad.

La información se necesita en todos los niveles de la organización para, por una parte, identificar, evaluar y responder a los riesgos y por otra, dirigir la entidad y conseguir sus objetivos.

La información operativa de fuentes internas y externas, tanto financiera como no financiera, es relevante para múltiples objetivos de negocio.

Los sistemas de información pueden ser formales o informales. Las conversaciones con clientes, proveedores, reguladores y personal de la entidad a menudo proporcionan información crítica necesaria para identificar riesgos y oportunidades. De igual manera, la asistencia a seminarios profesionales o del sector y la participación en asociaciones mercantiles o de otro tipo puede ser una fuente de información valiosa.

Es importante el establecimiento de una comunicación eficaz en un sentido amplio, que facilite una circulación de la información (formal e informal). La alta dirección debe transmitir un mensaje claro y preciso a todo el personal sobre la importancia de las responsabilidades de cada uno en materia de compartir la información con fines de gestión y control.

Los diferentes niveles de una empresa necesitan diferentes tipos de información del proceso de gestión de riesgos, por lo que a continuación se presenta un cuadro del tipo de información de los distintos niveles o categorías profesionales de la empresa para posibilitar la gestión eficaz de la gestión de los riesgos de la empresa y reunir los siguientes atributos:

- Cantidad suficiente para la toma de decisiones.
- Información disponible en tiempo oportuno.
- Datos actualizados recientes.
- Datos incluidos correctos.
- Información obtenida fácilmente por las personas autorizadas.

Como consecuencia de las nuevas exigencias, la empresa debe analizar los riesgos propios de su actividad, mantener unos mecanismos específicos de control interno que aseguren la medición continuada de los mismos, establecer sistemas de información que garanticen la transparencia y proporcionen seguridad.

El fin último de todas las empresas es la de generar valor. Sin embargo, en la consecución de ese fin siempre está presente la incertidumbre o el riesgo. La gestión de riesgos por parte de la dirección le permite tratar eficazmente la incertidumbre, mejorando así la capacidad de generar valor. La gestión de riesgos aporta ventajas a la empresa, aunque presenta limitaciones que impiden que el consejo o la dirección tengan seguridad absoluta de la consecución de los objetivos, derivadas de factores como que el juicio humano en la toma de decisiones, las decisiones sobre la respuesta al riesgo y el establecimiento de controles necesitan tener en cuenta los costes y beneficios relativos.

Todas las personas que integran una empresa, tienen alguna responsabilidad en la gestión de riesgos corporativos. El consejero delegado es el responsable último y deberá asumir su titularidad, pero el director de riesgos, director financiero, auditor interno u otros, desempeñan responsabilidades claves de apoyo, mientras que el restante personal de la empresa, es responsable de ejecutar la gestión de riesgos corporativos de acuerdo con las directrices y modelos establecidos.

La evaluación de riesgos es el proceso orientado a identificar los riesgos que conlleva el desarrollo de la actividad de la empresa para poder establecer unas conclusiones y recomendaciones justificadas para mejorar las condiciones de la aceptación del riesgo por parte de la empresa. Tras la identificación y evaluación de los riesgos se debe gestionar y controlar el riesgo, para ello, se pueden realizar distintas acciones alternativas para la adecuada gestión y control de los riesgos como son la eliminación, reducción, asunción financiera y transferencia de los riesgos a una tercero a través de fórmulas del sector asegurador o financiero.

	Consejo de administración	Unidades de negocio	Personal
A NIVEL INTERNO	• Conocer los riesgos más importantes a los que se enfrenta la empresa. • Conocer los posibles efectos en el valor de la empresa para los accionistas de las desviaciones con respecto a los márgenes de rendimiento previstos. • Asegurar niveles apropiados de toma de conciencia en toda la empresa. • Saber cómo la empresa gestionará una crisis. • Ser consciente de la importancia de la confianza de los interesados en la empresa. • Tener claro cómo gestionar las comunicaciones con los inversores. • Estar seguro de que el proceso de gestión de riesgos funciona de forma efectiva. • Divulgar una clara política de gestión de riesgos que abarque las responsabilidades y la filosofía de gestión de riesgos. • Asegurarse que todos los responsables de cada área o de la totalidad de trabajadores conocen y llevan a cabo la política de gestión de riesgos.	• Ser conscientes de los riesgos que comprenden sus áreas de responsabilidad, los impactos posibles que estos pueden ejercer en otras áreas y las consecuencias que otras áreas pueden provocar en ellas. • Disponer de indicadores de rendimiento que les permitan supervisar las actividades de negocio y financieras clave, el progreso hacia la consecución de los objetivos e identificar los desarrollos que requieren las intervenciones (ej. Previsiones y presupuestos). • Disponer de sistemas que adviertan de las variaciones en las previsiones y en los presupuestos con la debida frecuencia para que sea posible tomar las medidas apropiadas. • Informar rápida y sistemáticamente a la alta dirección de cualquier nuevo riesgo o fallo en las medidas de control existentes que perciban. • Informar y mantener relaciones con las otras unidades de negocio para aunar los esfuerzos en cuanto a medición y gestión de riesgos.	• Comprender su responsabilidad respecto a riesgos individuales. • Ser conscientes de cómo pueden mejorar continuamente la respuesta de la gestión de riesgos. • Entender que la gestión y la conciencia de riesgos son una parte fundamental de la cultura de la empresa. • Informar rápida y sistemáticamente a la alta dirección de cualquier nuevo riesgo o cualquier fallo en las medidas de control existentes que perciban.

COMUNICACIÓN EXTERNA	Las empresas tienen que informar regularmente a sus interesados explicando sus políticas de gestión de riesgos y la efectividad con la que está consiguiendo sus objetivos. Un buen gobierno corporativo requiere que las empresas adopten un enfoque metódico respecto a la gestión de riesgos que: – Proteja los intereses de sus interesados. – Asegure que el consejo de administración desempeña sus deberes de dirigir la estrategia, crear valor y supervisar el rendimiento de la empresa. – Asegure que los controles de gestión existen y que funcionan bien. Las medidas relativas a los informes a cumplimentar sobre la gestión de riesgos deben quedar establecidas claramente y ser puestas a disposición de los interesados. Los informes deben tratar: – Los métodos de control, especialmente de las responsabilidades de la dirección sobre la gestión de riesgos. – Los procesos para identificación de riesgos y cómo son conducidos por los sistemas de gestión de riesgos. – Los sistemas de control primarios implantados para gestionar riesgos importantes. – El resultado de los métodos de control y los procesos de identificación, deficiencias, aspectos a mejorar… – La supervisión y revisión del sistema implantado. Cualquier deficiencia importante que no esté cubierta por el sistema, o que se dé en el propio sistema, debe ser notificada junto con las medidas que se han tomado para tratarla.

9. Acerca del autor:

Albert Salvador Lafuente

Economista y Auditor Interno certificado por el IIA (The Institute of Internal Auditors)

Socio de Grupo Paradell Compliance S.L., liderando un proyecto en el diseño y comercialización de programas de prevención de delitos y gestión del fraude. http://www.grupoparadell.com/gestion-del-fraude/.

Miembro de SEC, Salud, ética y Compliance

Fundador y Vicepresidente de World Compliance Association.

Propietario y administrador de los blogs:

- Fraude Interno: www.fraudeinterno.wordpress.com
- Compliance: www.prevenciondedelitos.wordpress.com

Especialista en Fraude Interno y Compliance ha participado como conferenciante o ponente en Congresos. Participa en seminarios sobre la materia y es tutor de cursos presenciales y online en materia de fraude Interno y Compliance

Ha escrito numerosos artículos sobre Fraude Interno y Compliance en las principales revistas técnicas y jurídicas.

Tiene 24 años de experiencia en empresas líderes del sector bancario. Ha trabajado como auditor de la red comercial y como auditor de procesos en trabajos transversales, implantando el modelo de Corporate Assurance y mejores prácticas bancarias propuestas por el IAE (Instituto de Auditores Interno). Ha liderado proyectos en la última integración bancaria, así como desarrollado iniciativas propias de valor en el ámbito del fraude interno, forensic y prevención de blanqueo de capitales, así como la creación y implantación de modelos de auditorías normativas (CNMV, Ley de transparencia, SEPBLAC...) y comerciales.


creatividad
innovación
imaginación
formación
ágora del conocimiento
https://fraudeinterno.wordpress.com/