ONE WORLD
ONE PROFESSION
ONE DESTINATION

"Uso de técnicas de contra-inteligencia para que las organizaciones se defiendan de las actividades de quienes cometen fraudes"

Jorge Badillo Ayala

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
ORLANDO, FLORIDA, USA / JULY 14-17, 2013

Jorge Badillo Ayala

Auditor Interno Regional – Sudamérica

Kinross Gold Corporation

- Es ecuatoriano, cuenta con más de 17 años de experiencia en labores de auditoría: interna, financiera, de gestión, forense, informática. Trabaja en la compañía minera canadiense Kinross Gold Corporation como Auditor Interno Regional para Sudamérica, con sede regional en Chile.
- Tiempo atrás trabajó para la Organización de las Naciones Unidas ONU como Contralor Financiero de la Organización Internacional para las Migraciones, Misión en Ecuador; antes se desempeñó como Manager en Ernst & Young y también fue Director de Auditoría Interna del Servicio de Rentas Internas – SRI.
- Es Doctor en Contabilidad y Auditoría - CPA; Magíster en Administración de Empresas - MBA.
- Cuenta con las certificaciones internacionales:
  - CIA – Certified Internal Auditor;
  - CCSA – Certification in Control Self – Assessment
  - CGAP – Certified Government Auditing Professional
  - CRMA – Certification in Risk Management Assurance
  - CISA – Certified Information Systems Auditor
- Es 2do Vicepresidente de la Federación Latinoamericana de Auditores Internos FLAI. Es miembro de Comités Internacionales y de Equipos de Trabajo del IIA Global. Es miembro invitado del Directorio del Instituto de Auditores Internos de Chile. Fue Presidente del Instituto de Auditores Internos del Ecuador.
- A nivel internacional es conferencista, instructor y docente universitario en los temas de su especialidad.

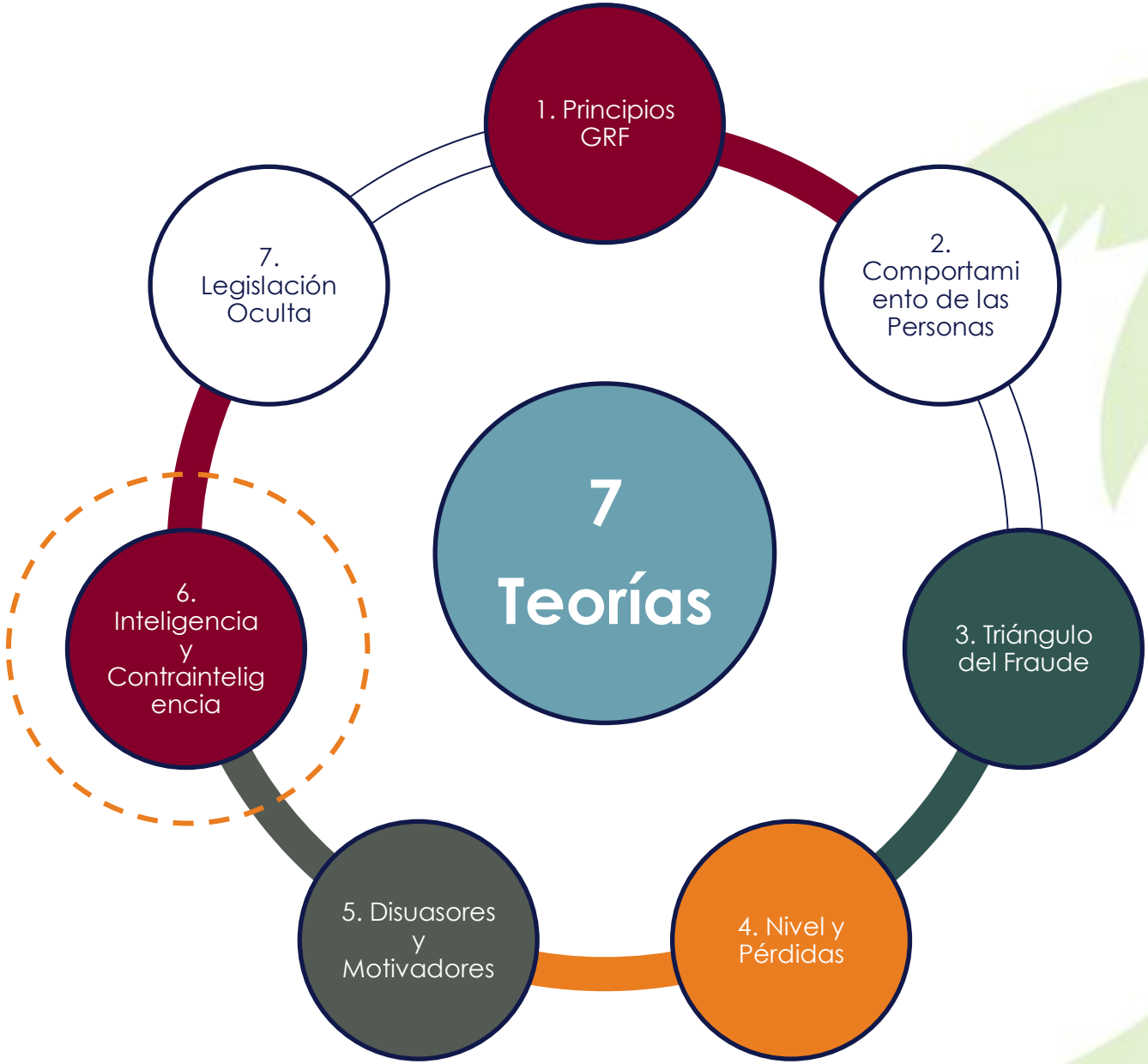
THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
ORLANDO, FLORIDA, USA / JULY 14-17, 2013

Agenda

1. Siete Teorías Clave sobre Fraude
2. Inteligencia y Contrainteligencia
3. Técnicas de Inteligencia
4. Técnicas de Contrainteligencia

1. SIETE TEORÍAS CLAVE SOBRE FRAUDE

1. Siete Teorías Clave sobre Fraude



1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

Ficha técnica

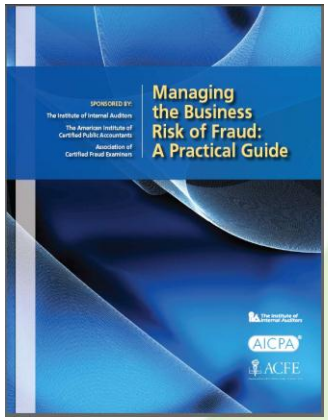
Título: Gestión del Riesgo Organizacional de Fraude: Una Guía Práctica

Emitido por: IIA / AICPA / ACFE

Año: 2008

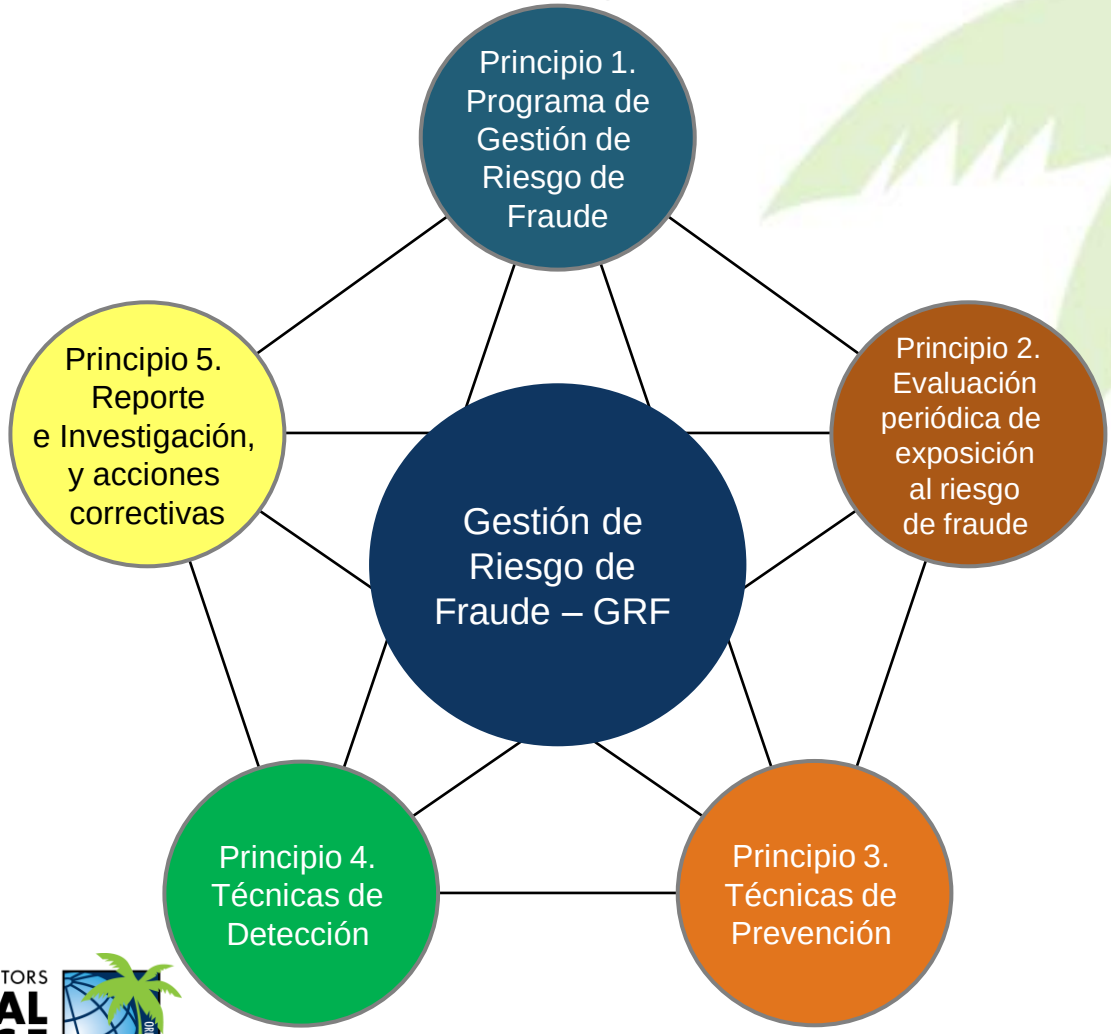
Traducido por: IAI Ecuador

Año: 2011



1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF



1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

1. Programa de gestión de riesgo de fraude

2. Evaluación periódica de exposición al riesgo de fraude

3. Técnicas de Prevención

- **Principio 1:** Como parte de la estructura de gobierno de una organización, un programa de gestión del riesgo de fraude debería estar implementado, incluyendo una política (o políticas) por escrito para transmitir las expectativas de la junta directiva y la alta dirección respecto de la gestión del riesgo de fraude

Principio 2: La exposición al riesgo de fraude debería ser evaluada periódicamente por la organización para identificar posibles esquemas y eventos específicos que la organización necesite mitigar.

- **Principio 3:** Técnicas de prevención para evitar potenciales eventos clave de riesgo de fraude deberían estar establecidas, cuando sea posible, para mitigar posibles impactos en la organización.

1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

4. Técnicas de detección

- **Principio 4:** Técnicas de detección deberían estar establecidas para descubrir eventos de fraude cuando las medidas preventivas fallen o los riesgos no mitigados se materialicen.

5. Reporte e Investigación del fraude y acciones correctivas

- **Principio 5:** Un proceso de reporte debería estar implementado para solicitar datos sobre potenciales fraudes y un enfoque coordinado de investigaciones y acciones correctivas debería ser utilizado para ayudar a asegurar que el potencial fraude es afrontado de manera apropiada y oportuna.

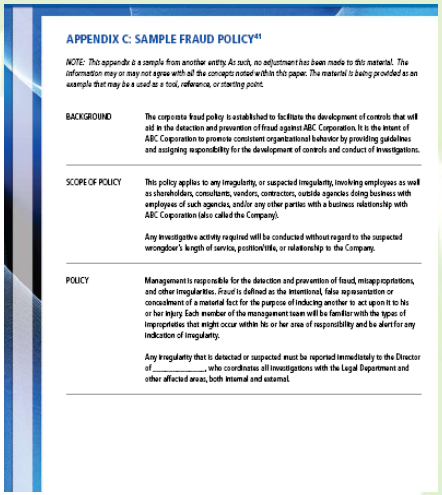
1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

- Contenido sugerido para una Política sobre Fraude:
  - Antecedentes
  - Alcance de la política
  - Política
  - Acciones que constituyen fraude
  - Otras irregularidades
  - Responsabilidades de investigación
  - Confidencialidad
  - Autorización para la investigación de fraude sospechado
  - Procedimientos de reporte
  - Separación de personal
  - Administración de la política
  - Aprobación



APPENDIX C: SAMPLE FRAUD POLICY[41]

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

BACKGROUND — The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against ABC Corporation. It is the intent of ABC Corporation to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

SCOPE OF POLICY — This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with ABC Corporation (also called the Company).

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

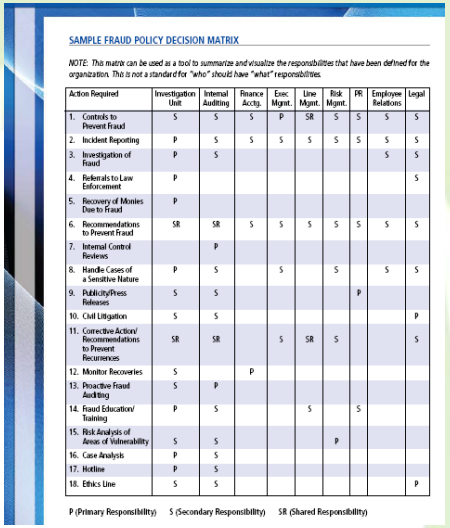
POLICY — Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. *Fraud* is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity.

Any irregularity that is detected or suspected must be reported immediately to the Director of _____, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

- Matriz de Decisión – Política sobre Fraude
- Áreas involucradas
- Identificación de responsabilidades
  - Primaria (P)
  - Secundaria (S)
  - Compartida (RC)
- Acciones requeridas frente al fraude en las organizaciones (18)



SAMPLE FRAUD POLICY DECISION MATRIX

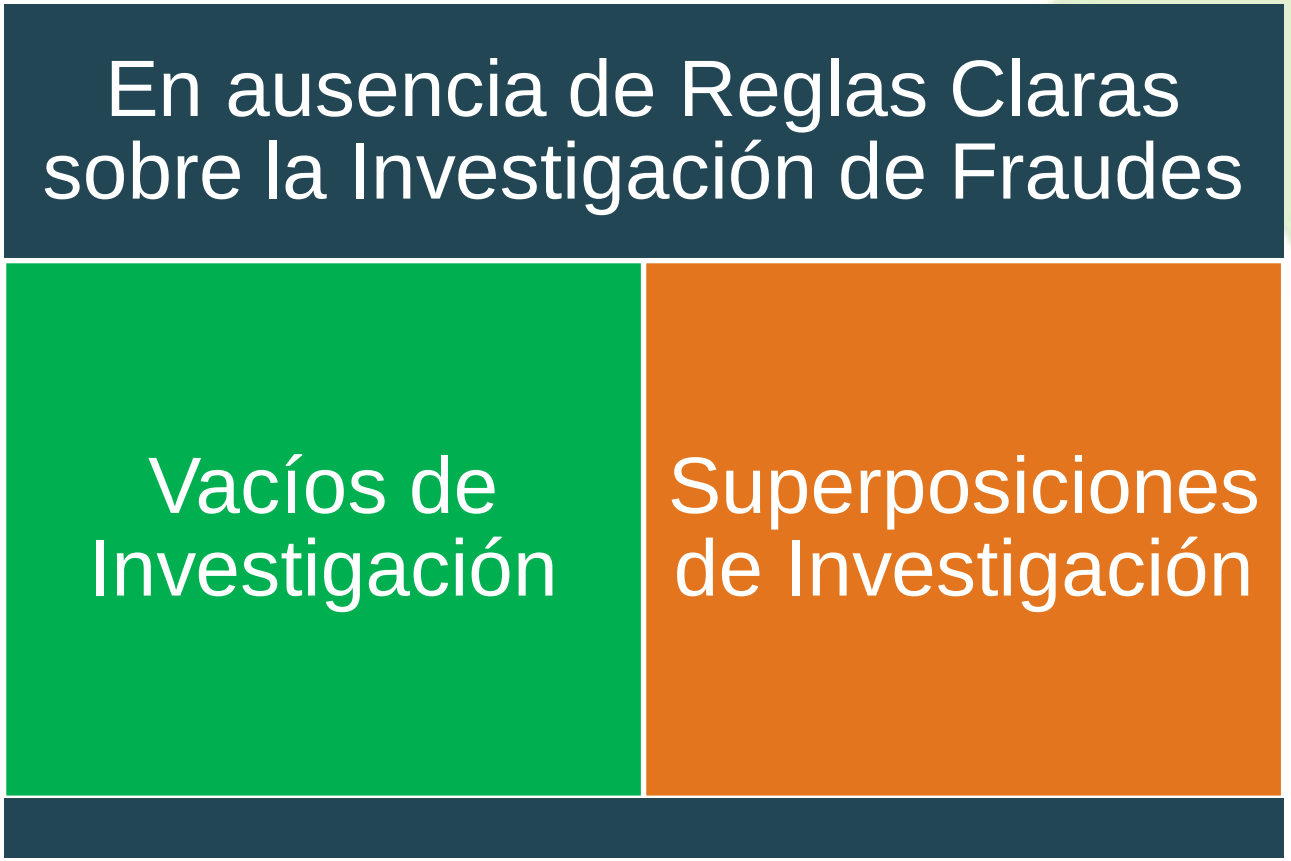
NOTE: This matrix can be used as a tool to summarize and visualize the responsibilities that have been defined for the organization. This is not a standard for "who" should have "what" responsibilities.

Action Required	Investigation Unit	Internal Auditing	Finance Acctg.	Exec Mgmt.	Line Mgmt.	Risk Mgmt.	PR	Employee Relations	Legal
1. Controls to Prevent Fraud	S	S	S	P	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S						S	S
4. Referrals to Law Enforcement	P								S
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Control Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S		S	S
9. Publicity/Press Releases	S	S					P		
10. Civil Litigation	S	S							P
11. Corrective Action/ Recommendations to Prevent Recurrences	SR	SR		S	SR	S			S
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/ Training	P	S			S		S		
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. Ethics Line	S	S							P

P (Primary Responsibility) S (Secondary Responsibility) SR (Shared Responsibility)

1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

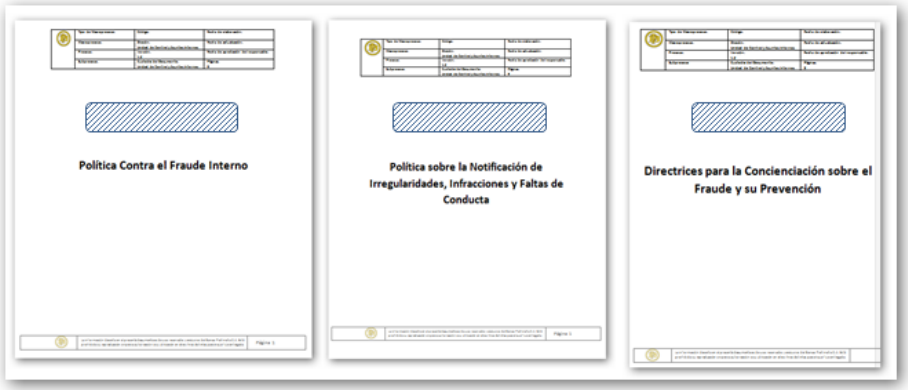


1. Siete Teorías Clave sobre Fraude

1. Los Principios de la Gestión de Riesgos de Fraude – GRF

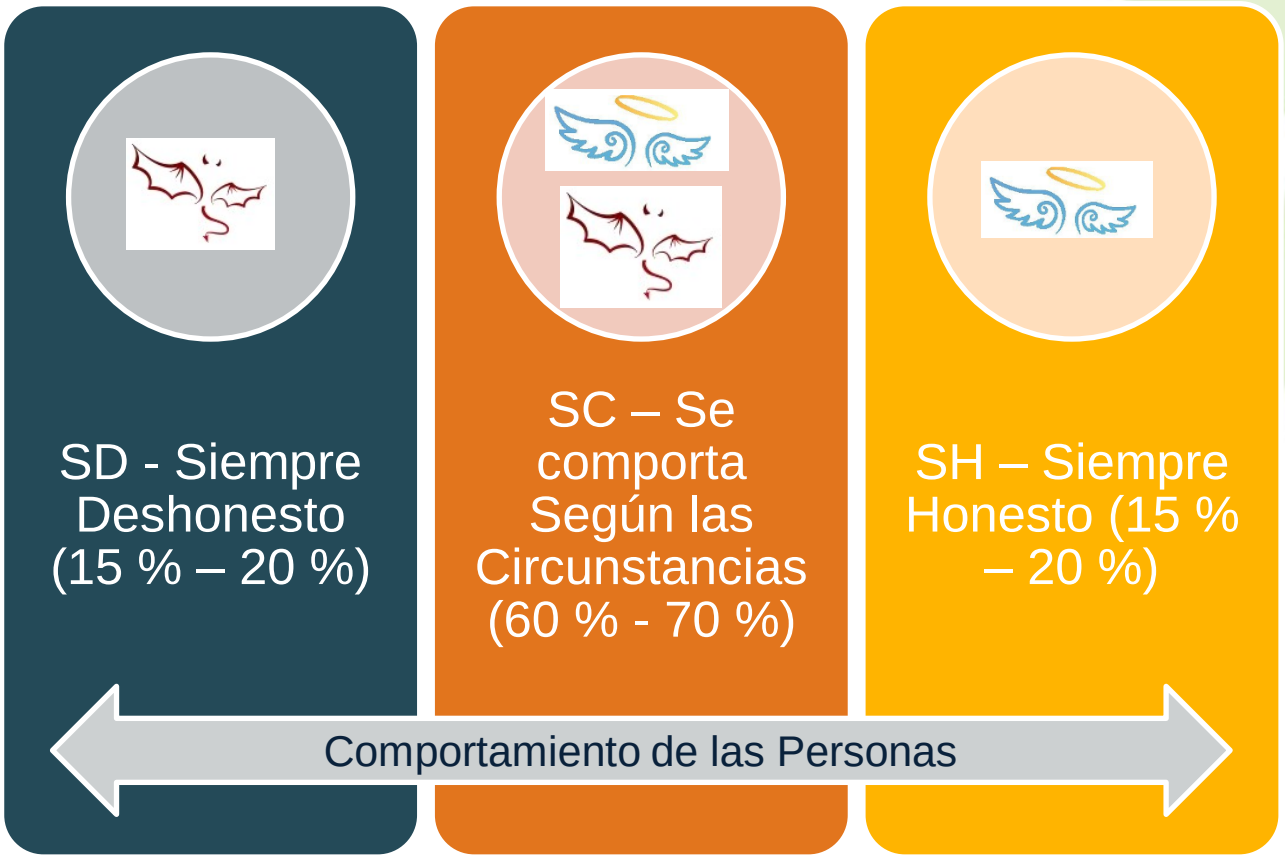
- Con el fin de fortalecer la prevención, detección e investigación de fraude interno, es necesario implementar los siguientes lineamientos:
  - Código de Ética
  - Política Contra el Fraude Interno
  - Política sobre la Notificación de Irregularidades, Infracciones y Faltas de Conducta
  - Directrices para la Concienciación sobre el Fraude y su Prevención

Código de Ética



1. Siete Teorías Clave sobre Fraude

2. Teoría del Comportamiento de las Personas - TCP

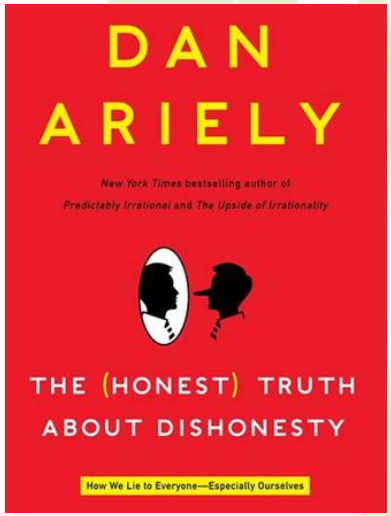


Fuente : ACFE

1. Siete Teorías Clave sobre Fraude

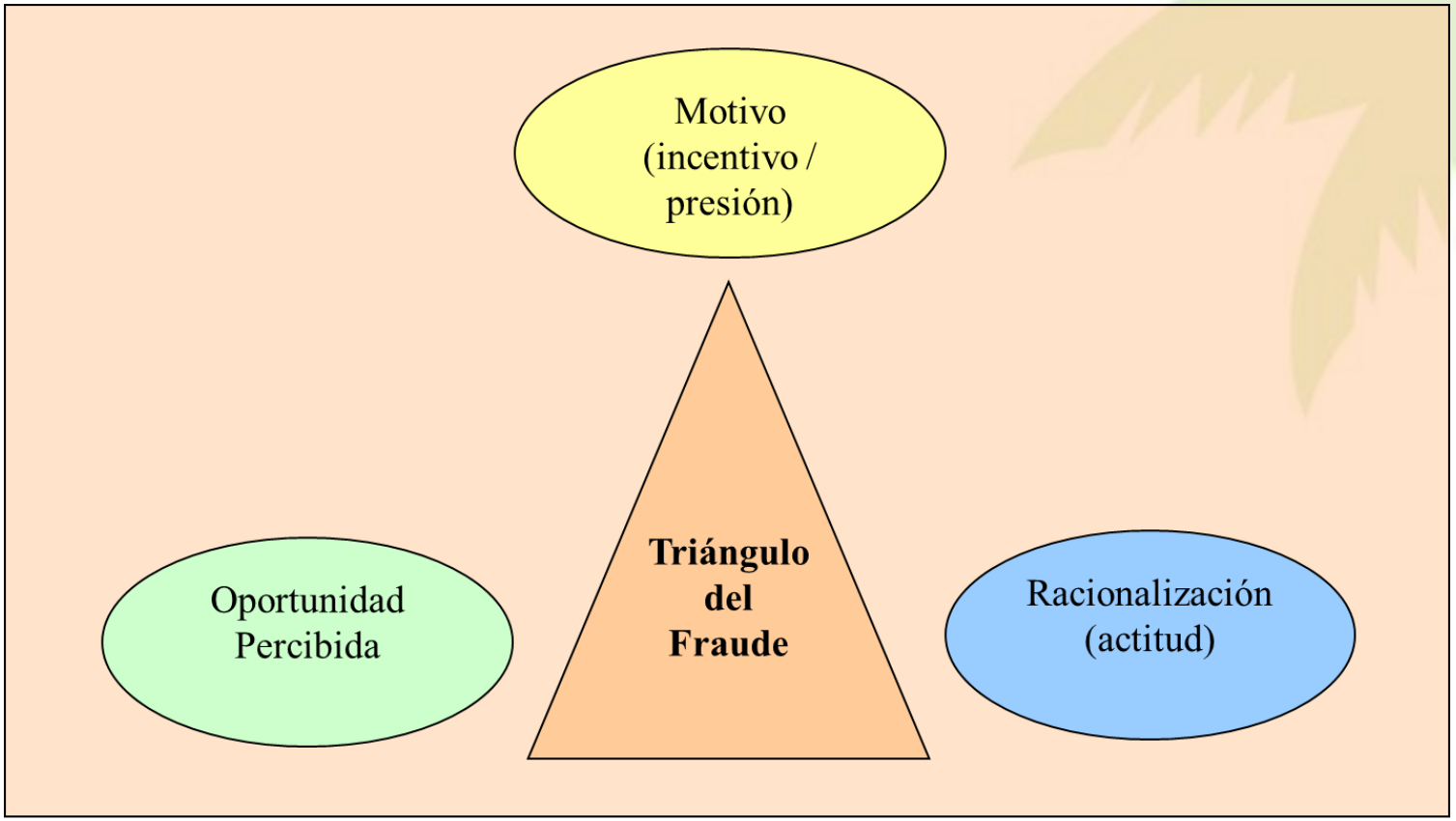
2. Teoría del Comportamiento de las Personas – TCP

- **Experimento base – Dan Ariely**
- Dan Ariely utilizó un experimento base para probar su tesis: les entregó a diversos grupos de personas una hoja con ejercicios numéricos. Cada individuo debía tratar de resolver la mayor cantidad de problemas posible, tarea por la que recibirían dinero dependiendo del éxito que tuvieran. Dos tipos de grupos se sometieron a la tarea. Uno era monitoreado por un investigador, que contaba cada una de las respuestas y les daba dinero dependiendo de la cantidad de ejercicios que lograran hacer. El otro, sin supervisión, debía anotar en una hoja anexa el número de respuestas y luego triturar la hoja con los ejercicios, sin que nadie se enterara del número real de respuestas. Luego cobraban el dinero como si nada.
- En promedio, el primer grupo obtenía cuatro respuestas. El segundo, obviamente ayudado por la mentira al traspasar el número a la segunda hoja, lograba seis respuestas.



1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude - TDF



Fuente: DNA (SAS) 99 - Triángulo del Fraude.

1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude - TDF

- El fraude frecuentemente involucra de manera simultánea los tres elementos antes señalados:

- **Motivo**.- Presión o incentivo (necesidad, justificación, desafío) para cometer el fraude (la causa o razón). Ejemplos de motivos para cometer fraude pueden ser: alcanzar metas de desempeño (como volúmenes de venta), obtener bonos en función de resultados (incremento en las utilidades o rebaja en los costos), mantener el puesto demostrando ficticios buenos resultados, deudas personales.

1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude - TDF

- El fraude frecuentemente involucra de manera simultánea los tres elementos antes señalados:

- **Oportunidad Percibida**.- El o los perpetradores del fraude perciben que existe un entorno favorable para cometer los actos irregulares pretendidos. La oportunidad para cometer fraude se presenta cuando alguien tiene el acceso, conocimiento y tiempo para realizar sus irregulares acciones. Las debilidades del control interno o la posibilidad de ponerse de acuerdo con otros directivos o empleados para cometer fraude (colusión) son ejemplos de oportunidades para comportamientos irregulares.

1. Siete Teorías Clave sobre Fraude

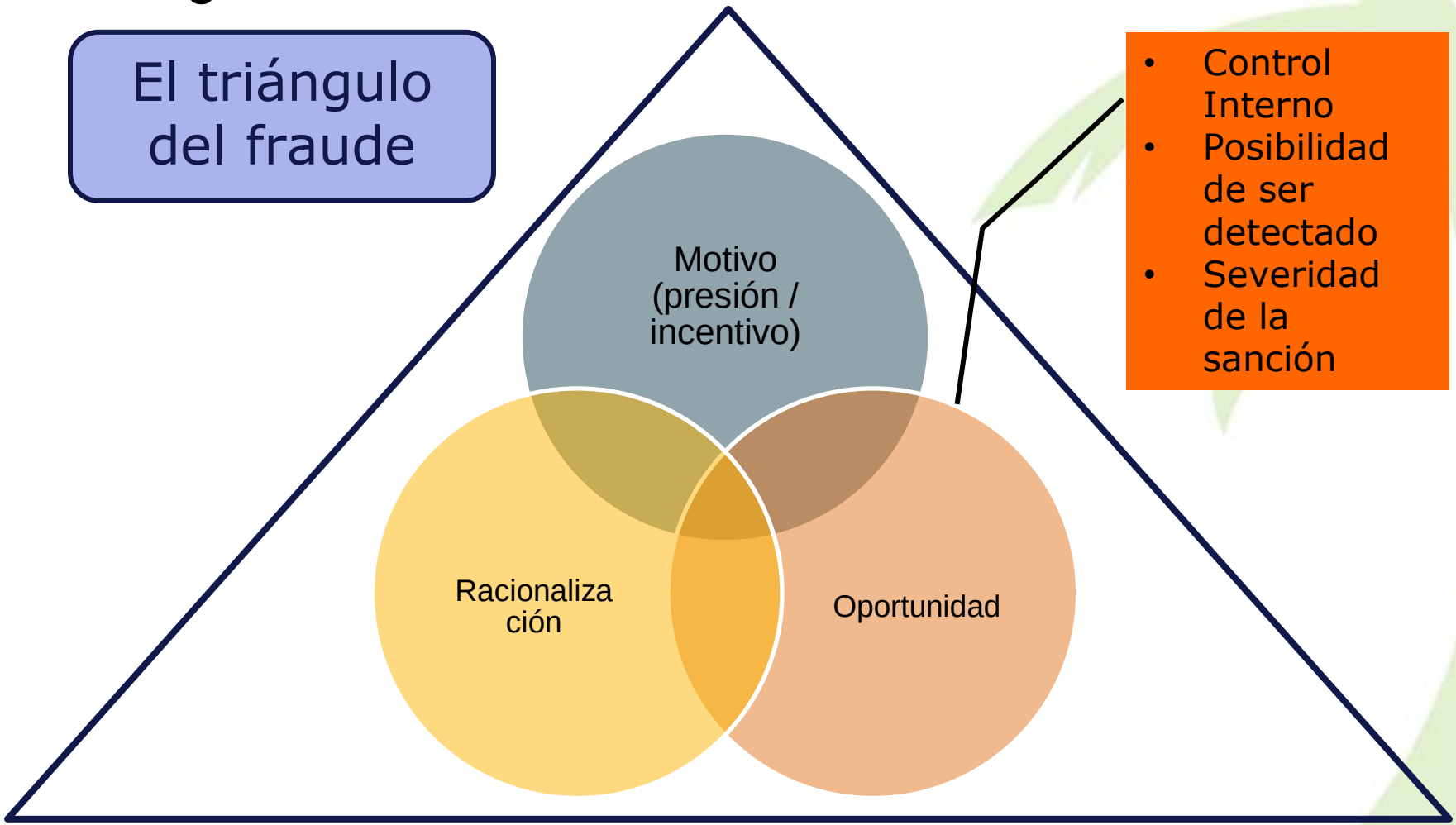
3. Triángulo del Fraude - TDF

- El fraude frecuentemente involucra de manera simultánea los tres elementos antes señalados:
- **Racionalización**.- Es la actitud equivocada de quien comete o planea cometer un fraude tratando de convencerse a si mismo (y a los demás si es descubierto), consiente o inconscientemente, de que existen razones válidas que justifican su comportamiento impropio; es decir, tratar de justificar el fraude cometido. Ejemplos de racionalización para justificar el fraude cometido pueden ser: alegar baja remuneración (convencerse de que no es fraude sino una compensación salarial, un préstamo), falta de reconocimiento en la organización (convencerse de que es una bonificación), fraude cometido por otros empleados y/o directivos (convencerse de que si otros cometen fraudes el fraude propio está justificado).

1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude - TDF

El triángulo del fraude



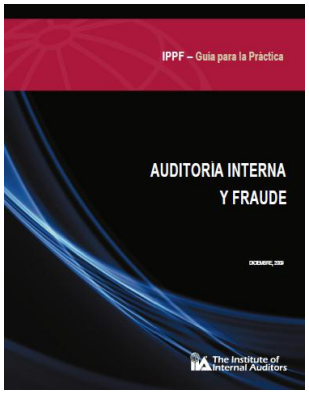
- Control Interno
- Posibilidad de ser detectado
- Severidad de la sanción

1. Siete Teorías Clave sobre Fraude

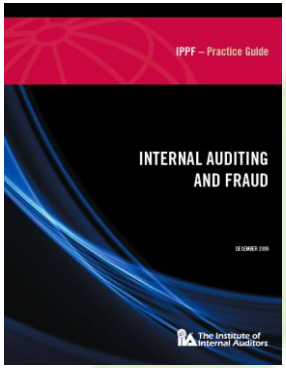
3. Triángulo del Fraude - TDF

Ficha técnica

- Título: Auditoría Interna y Fraude
- Emitido por:IIA Global
- Año: 2009



- Traducido por: IAI Ecuador
- Año: 2011



1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude - TDF

- Motivo
- Oportunidad
- Racionalización

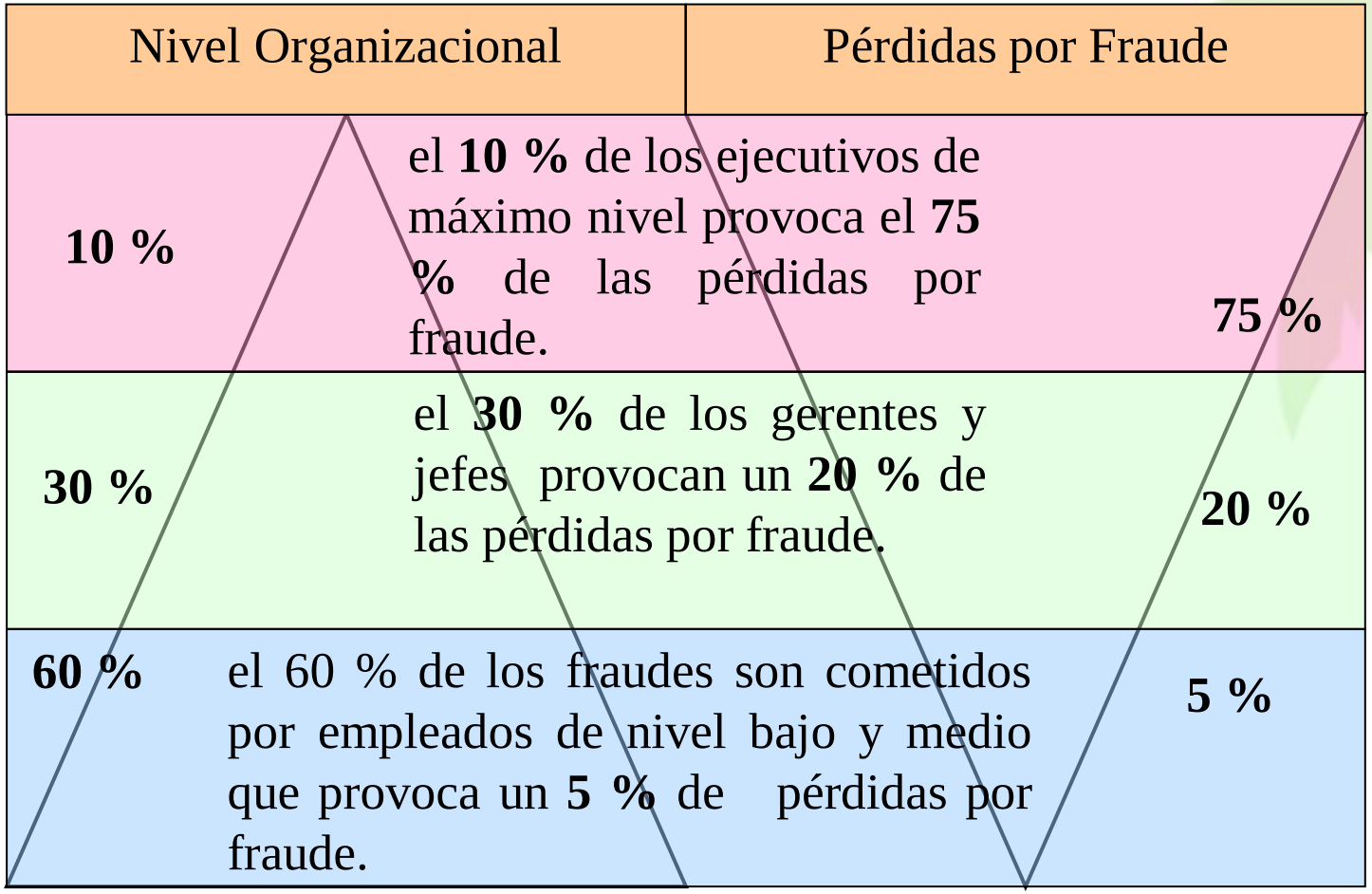
1. Siete Teorías Clave sobre Fraude

3. Triángulo del Fraude – TDF

- **Motivo, Oportunidad, Racionalización**
- "De los tres elementos, la **oportunidad es el factor sobre el que más puede influir una organización**. Las organizaciones necesitan procedimientos y controles internos que eviten poner a empleados en posiciones para cometer fraude y que detecten actividades fraudulentas si estas ocurren."
- "Aunque los auditores internos puedan no conocer el motivo exacto o racionalización conducente al fraude, necesitan identificar las oportunidades de fraude que existan. Los auditores internos también necesitan **comprender cuáles son los esquemas y escenarios de fraude, así como mantenerse al tanto de los indicios que apuntan hacia un fraude y cómo prevenirlo**."

1. Siete Teorías Clave sobre Fraude

4. Nivel Organizacional y Pérdidas por Fraude - NOPF



Fuente : ACFE

1. Siete Teorías Clave sobre Fraude

5. Teoría de Disuasores y Motivadores de Fraude - DMF

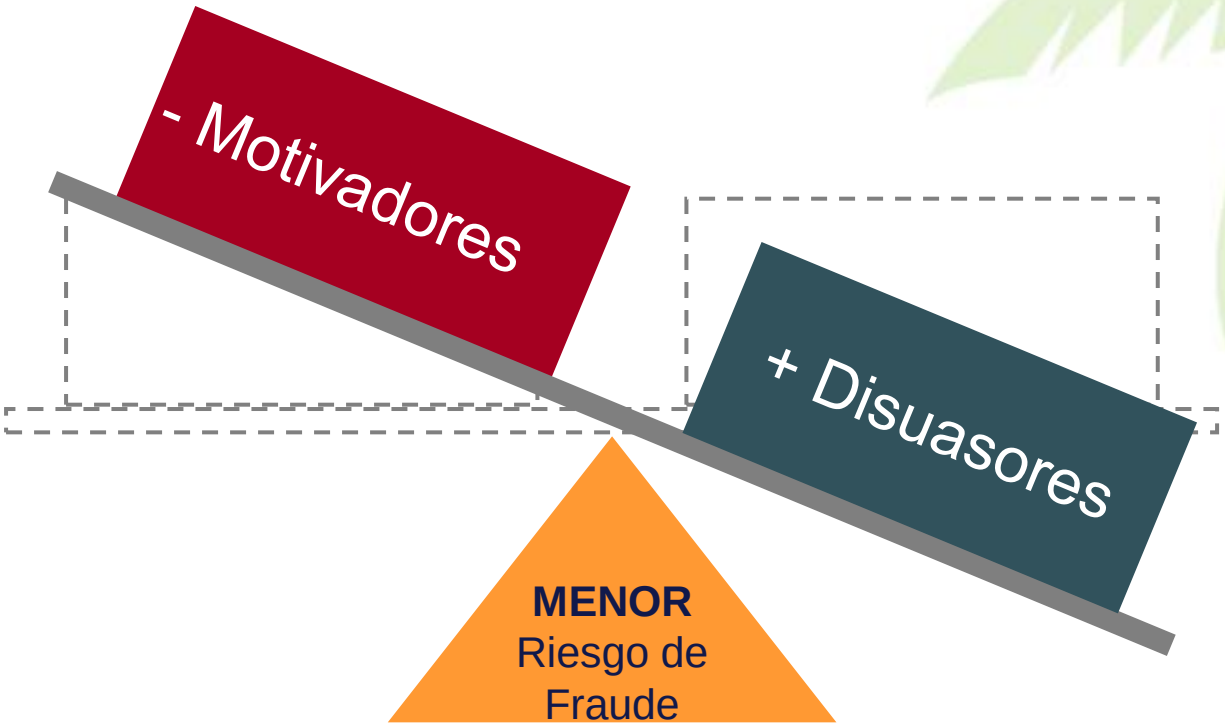
- Los disuasores mantienen una relación inversa con el riesgo de fraude
  - A + disuasores – riesgo de fraude
  - A – disuasores + riesgo de fraude

- Los motivadores mantienen una relación directa con el riesgo de fraude
  - A + motivadores + riesgo de fraude
  - A – motivadores - riesgo de fraude

- Cuando está ausente un disuasor usualmente esto se convierte en un motivador, más que en una situación neutra

1. Siete Teorías Clave sobre Fraude

5. Teoría de Disuasores y Motivadores de Fraude - DMF



1. Siete Teorías Clave sobre Fraude

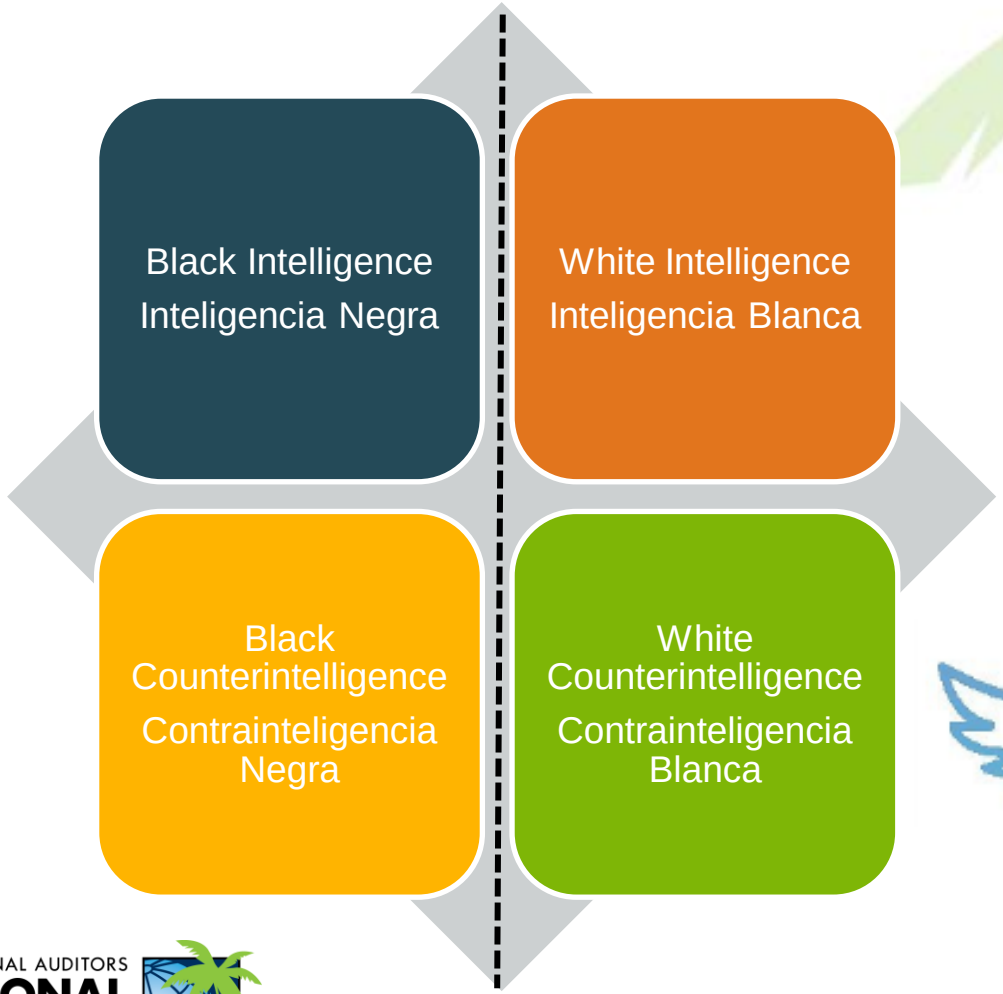
6. Teoría de Inteligencia y Contrainteligencia – TIC

- **Inteligencia**.- Obtener información del enemigo. En gestión de riesgos de fraude esto corresponde a tener implementados mecanismos para detectar e investigar fraudes.

- **Contrainteligencia**.- Evitar que el enemigo obtenga información de uno. En gestión de riesgos de fraude esto corresponde a evitar que quienes planean cometer o están cometiendo fraudes accedan a información que les permita lograr con éxito el fraude sin ser descubiertos y sancionados. Hay que tener en cuenta que quienes cometen fraudes en ocasiones recurren a prácticas de espionaje e infiltración.

1. Siete Teorías Clave sobre Fraude

6. Teoría de Inteligencia y Contrainteligencia – TIC



1. Siete Teorías Clave sobre Fraude

6. Teoría de Inteligencia y Contrainteligencia – TIC

Black Intelligence: Deshonesto obtiene información de honesto (quien es o será víctima de fraude)	**White Intelligence**: Honesto obtiene información de deshonesto (quien comete o cometerá fraude)
Black Counterintelligence: Deshonesto evita que honesto obtenga información de él y sus actividades	**White Counterintelligence**: Honesto evita que deshonesto obtenga información de él y sus actividades

1. Siete Teorías Clave sobre Fraude

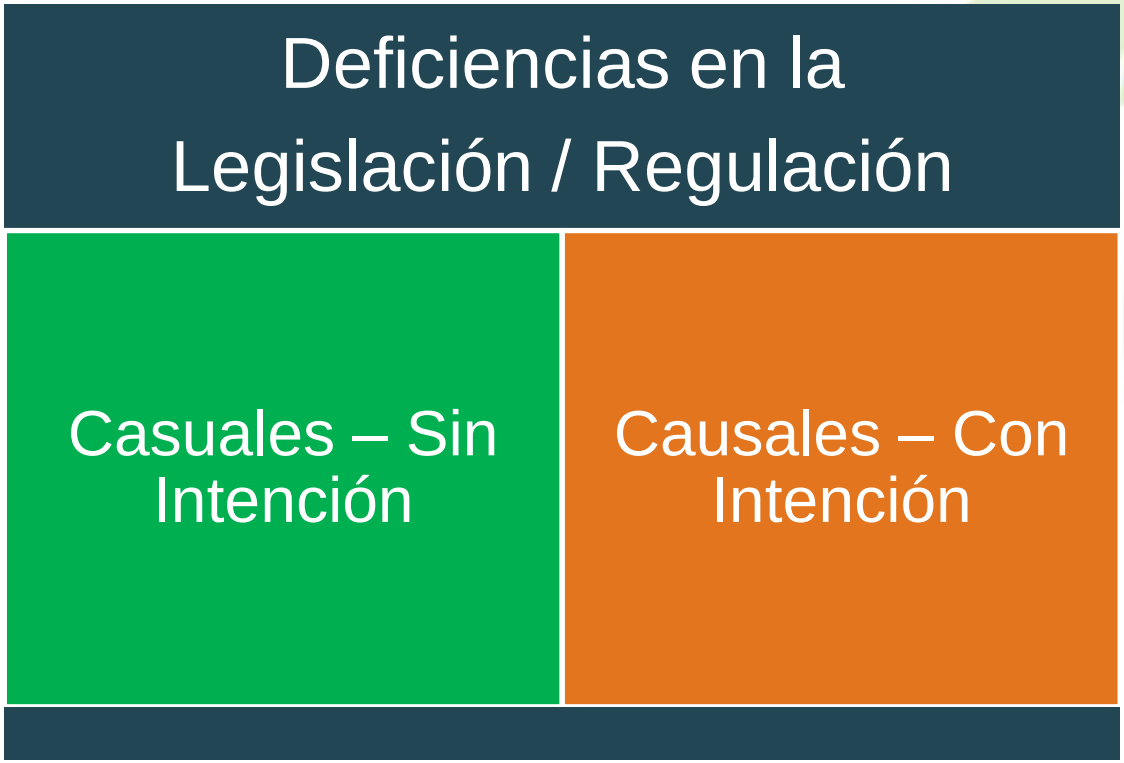
7. Teoría de la Legislación Oculta – TLO

- En muchos casos las deficiencias para combatir fraude presentes en las legislaciones / regulaciones (externas o internas) **no son CASUALES sino CAUSALES**, pues grupos de interés inciden directa o indirectamente para que la legislación / regulación tenga / mantenga las indicadas deficiencias.

- La legislación oculta puede presentarse a nivel corporativo o nivel de país

1. Siete Teorías Clave sobre Fraude

7. Teoría de la Legislación Oculta – TLO



1. Siete Teorías Clave sobre Fraude

7. Teoría de la Legislación Oculta – TLO

Aspecto tributario	Antes Reforma	Después Reforma
Interés por mora tributaria	1,1 tasa máxima activa	1,5 tasa máxima activa
Recargo en monto de evasión	No existente	20 %
Acción penal	Pago evita acción penal	Pago no evita acción penal
Caución para reclamo	No existe	20 %
Acción social para denuncia	No existe	Si existe
	Al no ser disuasores se convierten en MOTIVADORES	DISUASORES

2. INTELIGENCIA & CONTRAINTELIGENCIA

2. Inteligencia & Contrainteligencia

Inteligencia / Contrainteligencia	"Enemigo"	Actividades de Inteligencia "**Obtener** información clave para"	Actividades de Contrainteligencia "**Evitar** que el enemigo obtenga información clave para"
Militar 	Enemigo militar	• Tomar ventaja militar en un conflicto (defensa & ataque)	• Tomar ventaja militar en un conflicto (defensa & ataque)
Comercial 	La competencia	• Tomar ventaja comercial	• Tomar ventaja comercial
En Fraude 	Quienes cometen Fraude	• Prevenir, detectar e investigar fraudes	• Cometer / seguir cometiendo fraudes

- **Inteligencia**.- Obtener información del enemigo
- **Contrainteligencia**.- Evitar que el enemigo obtenga información de uno

2. Inteligencia & Contrainteligencia

ALERTA.
Los deshonestos también realizan actividades de **inteligencia** (para poder cometer sus fraudes) y **contrainteligencia** (para evitar ser descubiertos)

Black Intelligence: Deshonesto obtiene información de honesto (quien es o será víctima de fraude)	White Intelligence: Honesto obtiene información de deshonesto (quien comete o cometerá fraude)
Black Counterintelligence: Deshonesto evita que honesto obtenga información de él y sus actividades	White Counterintelligence: Honesto evita que deshonesto obtenga información de él y sus actividades

2. Inteligencia & Contrainteligencia

- Técnicas y herramientas para afrontar el fraude
  - Por su objetivo y momento de acción
    - Prevención
    - Detección
    - Investigación
  - Desde la perspectiva de la **obtención / protección** de información relacionada con fraude
    - Inteligencia
    - Contrainteligencia

2. Inteligencia & Contrainteligencia

INFORMACIÓN

Inteligencia – **Obtener** Información

Contrainteligencia – **Proteger** Información

Nuestra asignación es hacer nuestro sistema contable menos transparente.

¿Qué?

Nosotros no queremos que los inversionistas conozcan lo que nosotros estamos haciendo.

¿Nosotros somos malas personas?

Nosotros somos buenas personas que han sido influenciadas por una cultura corporativa corrupta.

Ah, bien, seguiré adelante

2. Inteligencia & Contrainteligencia

3. TÉCNICAS DE INTELIGENCIA

3. Técnicas de Inteligencia

Inteligencia Blanca

- Sistemas de gestión de denuncias y protección a denunciantes
- Monitoreo de actividades en mundo real y mundo virtual (actividades, accesos, comunicaciones, alertas "red flags")
- Análisis de datos (comportamientos, tendencias, relaciones, concordancias esperadas / diferencias esperadas no están)
- Monitoreo continuo / auditoría continua
- Revisión periódica de logs/pistas de auditoría (acceso, transaccionales)
- Controles ocultos (confidencialidad)
- Revisiones / auditorías sorpresa
- Confirmación de adhesión al Código de Ética
- Análisis y confirmación de antecedentes para fines de contratación/promoción
- Entrevistas de salida
- Comportamiento crediticio
- Períodos de vacación obligatorios
- Rotación de funciones
- Declaraciones juramentadas de bienes de empleados solicitada periódicamente
- Inclusión en la evaluación de desempeño de aspectos de ética y valores
- Calificación de proveedores
- Cláusula de auditabilidad de contratos
- Política de revelación de conflictos de intereses
- Análisis de relaciones
- Listas negras (empleados, proveedores, otros)
- Guía de casos de fraude (esquema, prevención, detección)
- Sistemas de detección de intrusos – IDS
- Emboscada
- Técnicas de prevención, **detección e investigación** de fraudes

3. Técnicas de Inteligencia

Inteligencia Negra

- Monitoreo de actividades en mundo real y mundo virtual
- Ingeniería social (obtener información en base a engaños)
- Colusión
- Presión / tentación para obtener información / "ayuda"
- Infiltrar personas en áreas/organizaciones
  - Regulados infiltrados en reguladores (Superintendencias, Ministerios, Administraciones Tributarias, Aduanas)
  - Infiltrar áreas de control
  - Infiltrar área a ser atacada
- Obtener información para identificar/construir la "oportunidad"
  - Acceso, conocimiento, tiempo
  - Control interno
  - Posibilidad de detección
  - Sanción

4. TÉCNICAS DE CONTRAINTELIGENCIA

4. Técnicas de Contrainteligencia

Contrainteligencia Blanca

- Evaluación de control interno
- Evaluación de riesgos de fraude
- Seguridad de la información
  - **Confidencialidad**
  - Integridad
  - Disponibilidad
- Seguridad física
  - Seguridad, monitoreo y restricción de accesos a bienes / instalaciones
- Seguridad lógica
  - Identificación & autenticación (simple, doble o triple factor; algo que sé, algo que tengo, algo que soy)
  - Controles biométricos
  - Perfiles/Roles y usuarios
    - Necesidad de saber
    - Menor privilegio
    - Segregación de funciones
- Seguridad lógica (continuación)
  - Cierre automático de sesión (período de inactividad)
  - Impedir inicio de sesiones simultáneas con un mismo usuario desde distintos equipos
  - Bloqueo del usuario ante un número determinado de intentos de acceso fallidos (usualmente tres)
  - Asociar el usuario y clave con el número IP del equipo
  - Encriptación de información
  - Control de entrada / salida de información (mail, dispositivos, etc.)
  - Firewalls
- Capacitación & concientización
- Señuelos & distractores
- Técnicas de **prevención**, detección e investigación de fraudes

4. Técnicas de Contrainteligencia

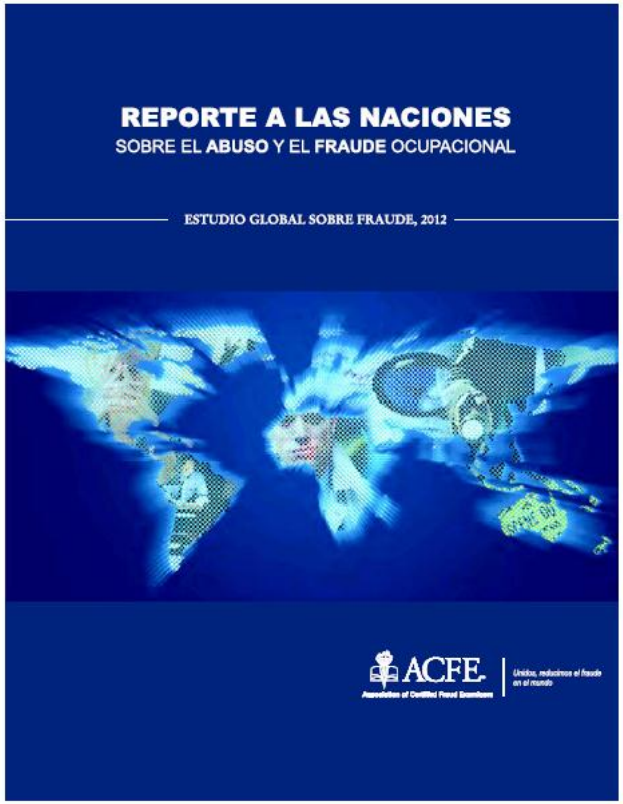
Contrainteligencia Negra

- Distorsión de la información
- Asimetría de la información
- Suplantación de identidad real o virtual
- Alteración de sistemas
- Aprovechar/construir brechas de control
- Evadir / eludir controles
- Falsos controles
- Legislación oculta
- Creación de una falsa imagen (persona honesta, trabajador ejemplar)
- Falsificación, engaño, mentira
- Técnicas de ocultamiento del fraude
- Monopolio
- Discrecionalidad
- Falta de transparencia
- Desorden / confusión
- Diluir responsabilidad & autoridad

INFORMACIÓN ADICIONAL

Información Adicional

- Reporte a las Naciones – ACFE (2012)
  http://www.acfe-mexico.com.mx/index2.html#
- Menú: Base de conocimiento / reporte a las naciones



Información Adicional

- Reporte a las Naciones – ACFE (2012)

Resumen de resultados

• Los participantes de la encuesta estiman que la organización típica pierde un 5% de sus ingresos anuales ante el fraude. Aplicado al Producto Bruto Mundial de 2011, esta cifra se traduce en una pérdida potencial proyectada superior a los 3.5 billones (millones de millones) de dólares (USD 3.5 trillones).

• La pérdida media causada por los casos de fraude ocupacional en nuestro estudio fue de USD 140,000. Más de una quinta parte de estos casos provocaron pérdidas de al menos USD 1 millón.

Más de una quinta parte de los fraudes en nuestro estudio causaron pérdidas por al menos 1 millón de dólares

• Los fraudes reportados duraron en promedio 18 meses antes de ser detectados.

• Al igual que en Reportes anteriores, **los esquemas de apropiación indebida de activos fueron por mucho el tipo más común de fraude ocupacional, constituyendo el 87% de los casos reportados;** también fueron la forma menos costosa de fraude, con una pérdida media de USD 120,000. **Los esquemas de fraude en estados financieros constituyeron sólo el 8% de los casos en nuestro estudio, pero causaron la mayor pérdida media (USD 1 millón).** Los esquemas de corrupción quedaron en el medio, ya que constituyen poco más de un tercio de todos los casos reportados y generaron una pérdida media de USD 250,000.

• Hay mayores probabilidades de detectar un fraude ocupacional a través de un aviso (tip) que por cualquier otro método. La mayoría de los avisos alertando sobre fraudes proviene de los empleados de la organización víctima.

• La corrupción y los esquemas de facturación fraudulenta presentan los mayores riesgos para las organizaciones del mundo. Para todas las regiones geográficas, estos dos tipos de esquemas constituyeron más del 50% de los fraudes reportados en el estudio.

• El fraude ocupacional es una amenaza importante para las pequeñas empresas. Las organizaciones más pequeñas de nuestro estudio sufrieron las mayores pérdidas medias. Estas organizaciones suelen utilizar un menor número de controles anti-fraude que sus contrapartes más grandes, lo que aumenta su vulnerabilidad ante el fraude.

• Al igual que en Reportes anteriores, **las industrias que con mayor frecuencia son víctimas del fraude ocupacional son las de servicios bancarios y financieros, el sector gubernamental y la administración pública, así como los sectores de la manufactura.**

• La presencia de controles anti-fraude se correlaciona de manera evidente con una disminución significativa en el costo y la duración de los esquemas de fraude ocupacional. Las organizaciones víctima que implementaron cualquiera de los 16 controles anti-fraude habituales sufrieron pérdidas considerablemente más bajas y reportaron menores tiempos de detección del fraude, en contraste con las organizaciones que carecen de estos controles.

• **Los defraudadores con mayores niveles de autoridad tienden a causar pérdidas mucho más grandes.** La pérdida media de los fraudes cometidos por el propietario/ejecutivos fue de USD 573,000, la pérdida media generada por el nivel gerencial fue de USD 180,000 y la pérdida media causada por los empleados fue de USD 60,000.

• **Cuanto más tiempo ha trabajado un defraudador para una organización, mayores tienden a ser las pérdidas por fraude que provoca.** Los defraudadores con más de diez años de antigüedad en la organización víctima causaron una pérdida media de USD 229,000. En comparación, la pérdida media causada por los defraudadores que cometieron el fraude en su primer año de trabajo fue de sólo USD 25,000.

• La gran mayoría (77%) de todos los fraudes en nuestro estudio fueron cometidos por personas que trabajan en uno de estas seis áreas laborales: contabilidad, operaciones, ventas, alta dirección, servicio al cliente y compras. Esta distribución es muy similar a la que hallamos en nuestro estudio de 2010.

• La mayoría de los defraudadores ocupacionales son infractores por primera vez, con historiales de empleo limpios. Aproximadamente 87% de los defraudadores ocupacionales nunca había sido acusado o condenado por un delito relacionado con el fraude, y el 84% nunca había sido sancionado o despedido por una conducta relacionada con fraude.

Información Adicional

- Reporte a las Naciones – ACFE (2012)

• **En 81% de los casos, el defraudador mostró uno o más indicadores conductuales que a menudo se asocian con un comportamiento fraudulento.** Vivir más allá de los propios medios (36% de los casos), dificultades financieras (27%), relación inusualmente cercana con proveedores o clientes (19%) y problemas de control excesivos (18%) fueron las señales de advertencia más comúnmente observadas.

• **Casi la mitad de las organizaciones víctima no recuperan nada de las pérdidas sufridas por fraude.** Al momento de nuestra encuesta, el 49% de las víctimas no había recuperado ninguna de las ganancias ilícitas obtenidas por el defraudador. Este hallazgo es consistente con nuestras investigaciones anteriores, que indican que 40-50% de las organizaciones víctima no recuperan ninguna de sus pérdidas relacionadas con el fraude.

Conclusiones y Recomendaciones

• La naturaleza y amenaza del fraude ocupacional son verdaderamente universales. Aunque nuestra investigación observó algunas diferencias regionales en los métodos utilizados para cometer fraude, así como enfoques distintos de las organizaciones para prevenirlo y detectarlo, muchas tendencias y características son similares sin importar el lugar en donde se produjo el fraude.

• Proporcionar medios para informar sobre actividades sospechosas es una parte fundamental de un programa de lucha contra el fraude. Se deben implementar mecanismos para reportar fraudes, tales como líneas de denuncia, con objeto de recibir avisos tanto de fuentes internas y externas, y dichos mecanismos deben permitir el anonimato y la confidencialidad. La dirección debería exhortar activamente a los empleados a reportar cualquier actividad sospechosa, así como publicar y hacer hincapié en una política anti-represalias.

• No se debe considerar a las auditorías externas como el método principal de detección de fraudes en una organización. Estas auditorías fueron el control mayormente implementado en nuestro estudio. Sin embargo, sólo detectaron el 3% de los fraudes del Reporte y se posicionaron mal como medio para limitar las pérdidas por fraude. Si bien las auditorías externas sirven a un propósito importante y pueden tener un enérgico efecto preventivo sobre posibles fraudes, su utilidad como medio para descubrir el fraude es limitada.

• La capacitación anti-fraude focalizada a los empleados y a los niveles gerenciales es un componente crítico de un buen programa para prevenir y detectar el fraude. Los avisos de los empleados no sólo son la forma más común de detectar el fraude ocupacional, nuestra investigación muestra también que las organizaciones que tienen programas de capacitación anti-fraude para empleados, gerentes y ejecutivos experimentan pérdidas menores y fraudes más cortos que las organizaciones sin estos programas. Como mínimo, el personal debe ser capacitado sobre las acciones que constituyen fraude, la manera en que éste perjudica a todos en la organización y el modo de informar sobre actividades cuestionables.

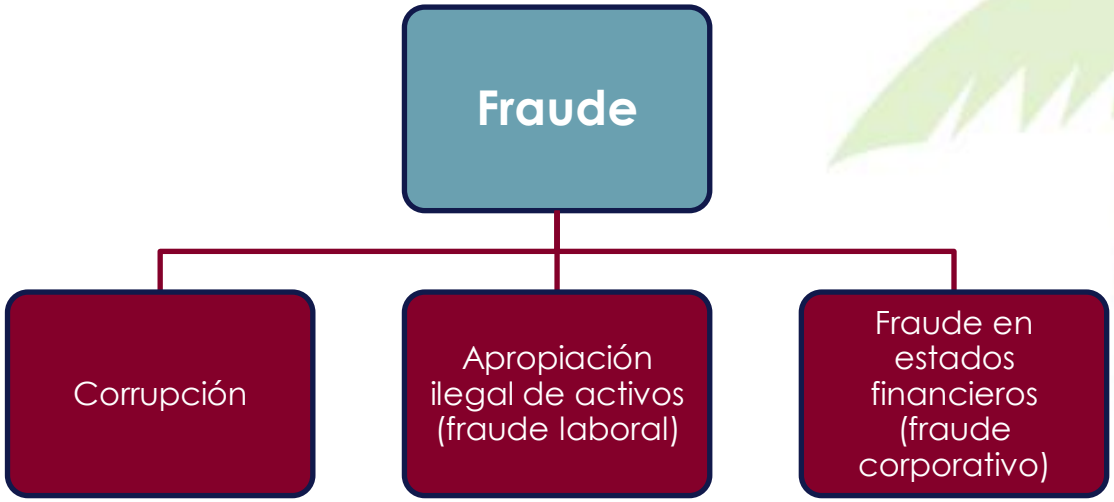
• Nuestro análisis siguen mostrando que las pequeñas empresas son especialmente vulnerables al fraude. Estas organizaciones suelen tener menos recursos que sus contrapartes más grandes, lo que a menudo se traduce en limitados y menos eficaces controles anti-fraude. Además, debido a que tienen menos recursos, las pérdidas sufridas por las pequeñas empresas suelen ser de mayor impacto que las que provocaría en organizaciones más grandes. Los niveles gerenciales y los propietarios de pequeñas empresas deben centrar sus esfuerzos de lucha contra el fraude en los mecanismos de control más rentables en términos de costo-beneficio, tales como líneas de denuncia, capacitación a los empleados y el establecimiento de un ambiente ético adecuado dentro de la organización. Además, una evaluación de los esquemas de fraude que representan las mayores amenazas para el negocio puede ayudar a identificar aquellas áreas que ameritan una inversión adicional en cuanto a la implementación de controles anti-fraude focalizados.

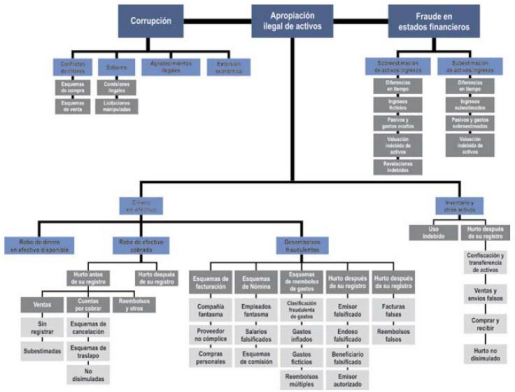
• La mayoría de los defraudadores muestran rasgos de comportamiento que pueden servir como señales de advertencia. Por lo general, los controles internos tradicionales no identifican estas banderas rojas conductuales (como el hecho de vivir más allá de los propios medios o exhibir una necesidad de control excesiva). Los gerentes, empleados y auditores requieren capacitación respecto de estos patrones de conducta comunes y deben poder identificarlos (en particular cuando se presentan junto con otras anomalías) para ayudar a identificar patrones indicativos de actividades fraudulentas.

• El costo del fraude ocupacional (tanto a nivel financiero como de reputación para una organización) puede ser sumamente perjudicial. Con casi la mitad de las organizaciones víctimas incapaces de recuperar sus pérdidas, las medidas proactivas para prevenir el fraude son esenciales. La dirección debe evaluar continuamente los riesgos específicos de fraude de la organización y revisar sus programas de prevención de fraude a la luz de esos riesgos. Una lista de verificación como la que se presenta en la página 70 puede ayudar a las organizaciones a prevenir eficazmente el fraude antes de que ocurra.

Información Adicional

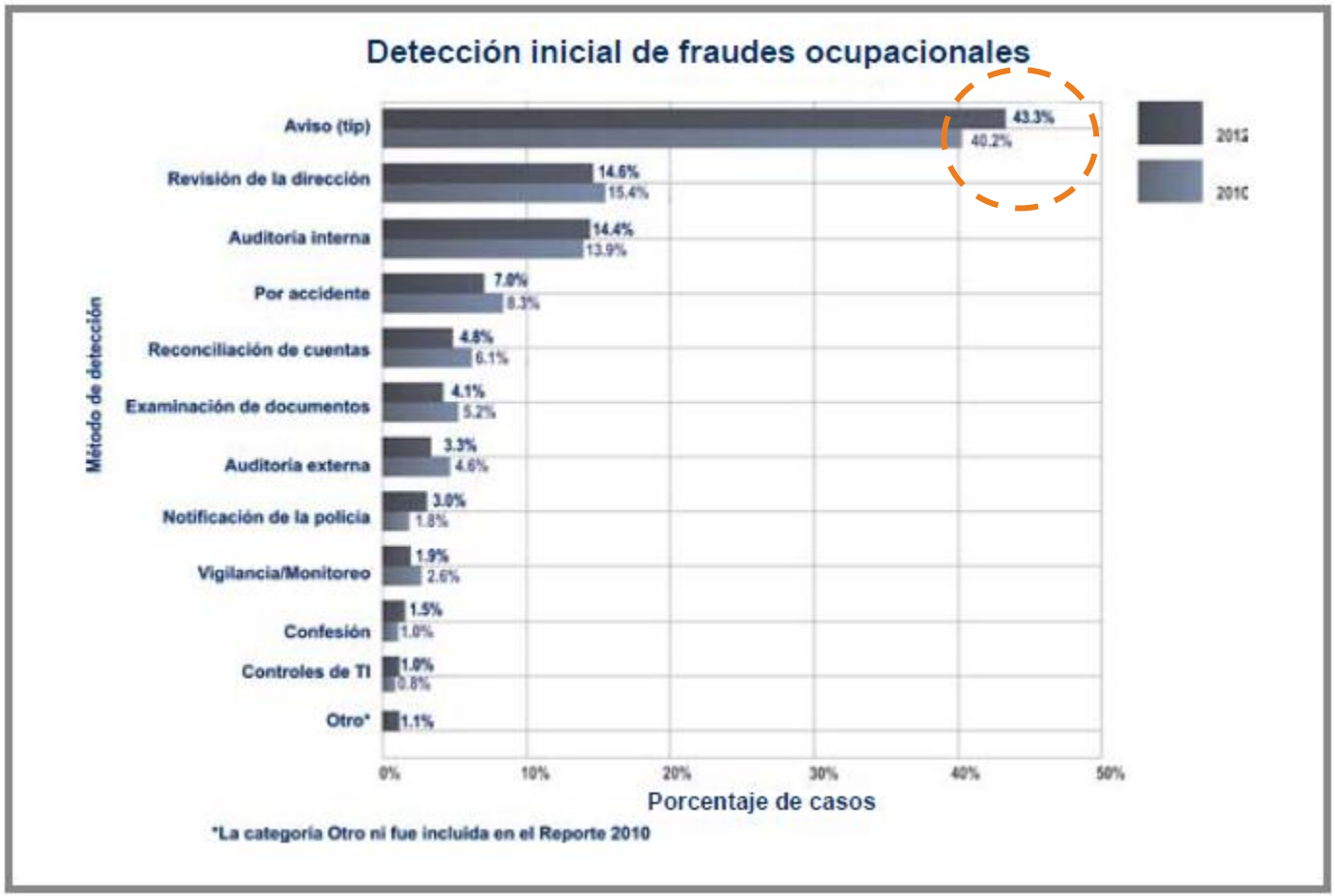
- Reporte a las Naciones – ACFE (2012)





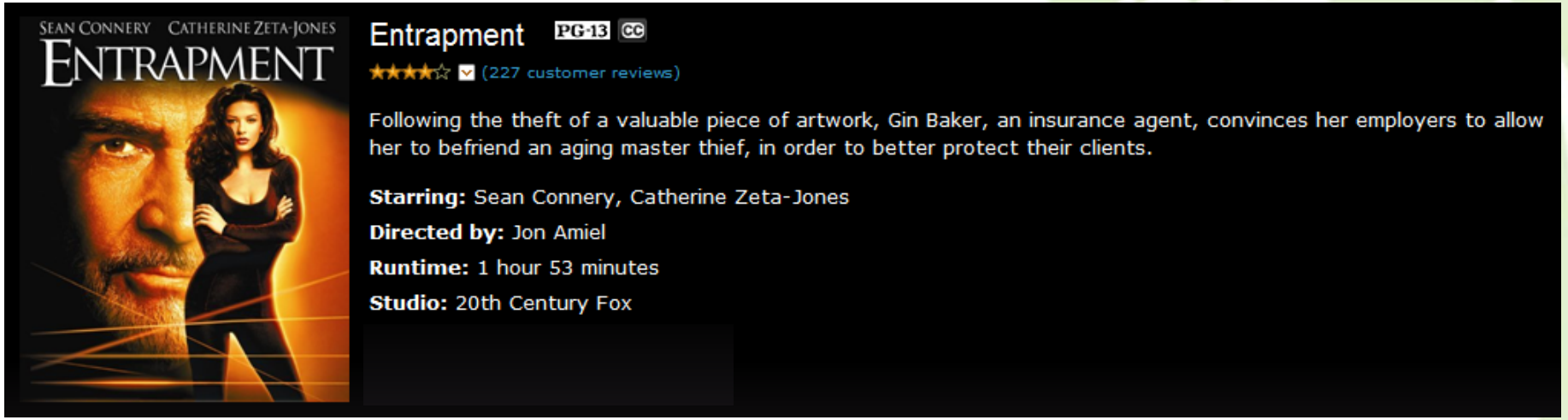
Información Adicional

- Reporte a las Naciones – ACFE (2012)



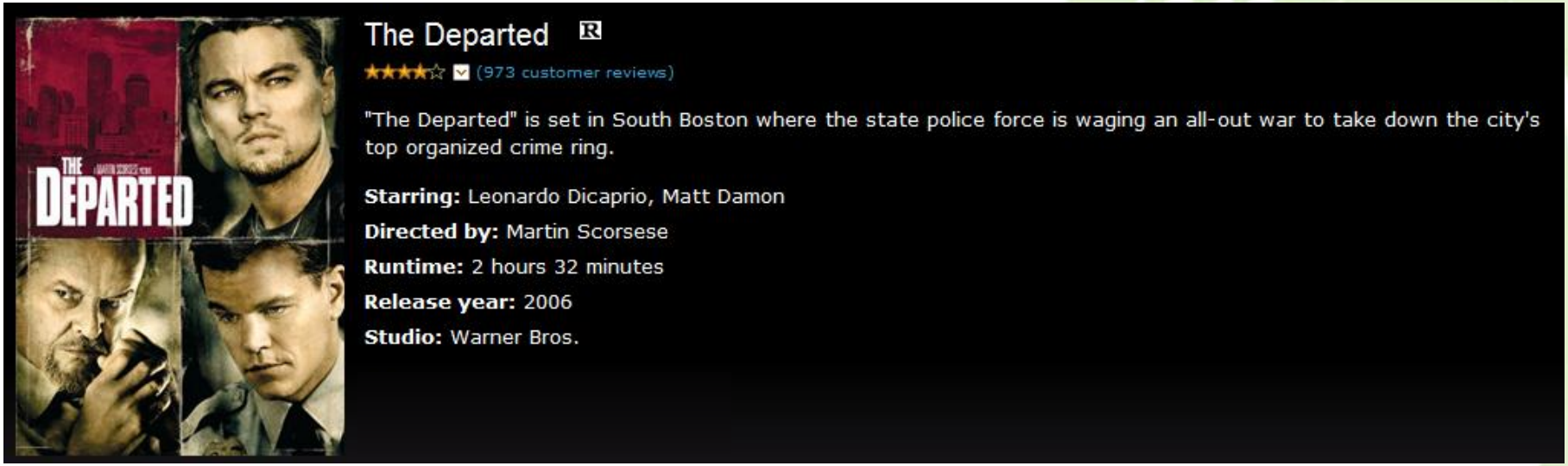
Información Adicional

- La Emboscada (La Trampa) - 1999



Información Adicional

- Los Infiltrados - 2006



Información de Contacto

Jorge Badillo Ayala

jgba1975@hotmail.com

¡Muchas gracias
por su atención!

Preguntas