# CONSIDERACIONES PARA LA PREVENCIÓN, ANÁLISIS Y DETECCIÓN DE FRAUDE ELECTRÓNICO

## XV CONGRESO LATINOAMERICANO DE AUDITORÍA INTERNA Y EVALUACIÓN DE RIESGOS

Julio R. Jolly Moore, CFE, CGEIT, Internal Audit Quality Assessment
Socio BDO Consulting
BDO Panamá

# Agenda

1. Introducción
2. Aspectos generales de fraudes electrónicos.
3. Técnicas de prevención e identificación.
4. Herramientas de Seguridad para investigaciones de fraude electrónico.
5. Técnicas y procedimientos de investigación durante y después del incidente.
6. Metodología y pasos a seguir.
7. Acciones a incidentes de fraude electrónico que se presenten.
8. Análisis de Riesgos de vulnerabilidades asociadas a fraude electrónico.
9. Preparación de matrices e informes.
10. Conclusiones.

# INTRODUCCIÓN

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# DEFINICIONES

## ¿Qué es el fraude electrónico?

*Cualquier actividad por la cual un ser humano toma acciones mediante equipos o recursos informáticos para obtener una ventaja sobre otra persona o entidad por medio de falsedades, engaños u omisión de la verdad.*

# DEFINICIONES

## ¿Qué es el fraude?

Según las **Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna**, fraude se define como "*Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio*".

# INTRODUCCIÓN - FRAUDE ELECTRÓNICO


En abril del 2005 usuarios maliciosos de Wachovia, Bank of America, PNC Financial Services Group y Commerce Bancorp accesarón datos importantes de más de 676,000 registros de clientes.

Fuente: Privacy Rights Clearinghouse, CSOonline reports.

En enero del 2009 Heartland Payment Systems proveedor de servicios de procesamiento de tarjetas débitos y crédito comunicó que había sido víctima de brechas de seguridad en sus datos. Puede decirse que a sido la mas grande dado que fueron 100 millones de expedientes potencialmente afectados.

Heartland PAYMENT SYSTEMS™

Fuente: Privacy Rights Clearinghouse, CSOonline reports.

# ANTECEDENTES

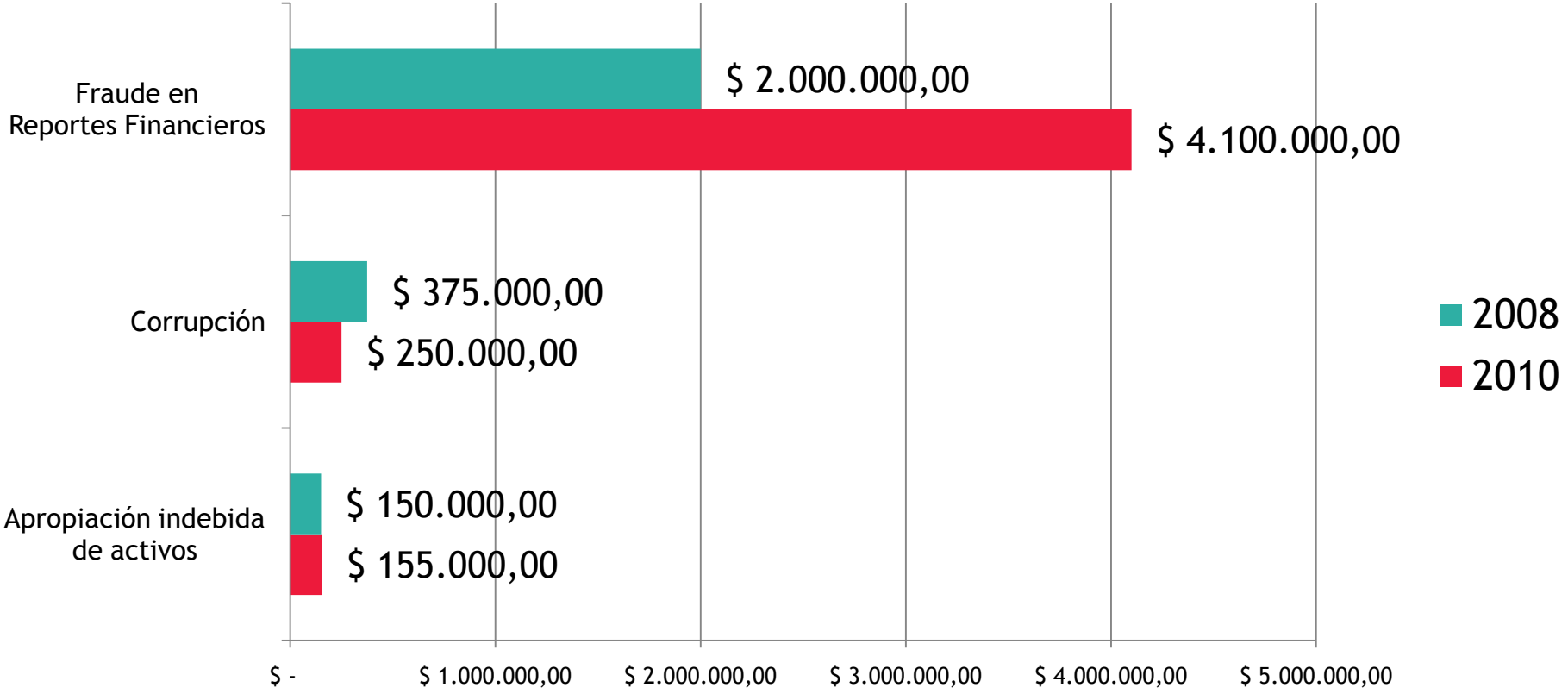
## Tipos de Crimen

| Tipo de Crimen | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|
| Fraude Telecomunicaciones | 10% | 8% | 5% | 5% |
| Fraude Financiero | 7% | 9% | 12% | 12% |
| Abuso interno | 48% | 42% | 59% | 44% |
| Sabotaje | 2% | 3% | 4% | 2% |
| Robo de información confidencial | N/A | N/A | 17% | 17% |

FUENTE: CSI / Computer Crime & Security Survey 2008

# ANTECEDENTES

## Pérdida promedio en casos de fraude




*Fuente: ACFE - Association of Certified Fraud Examiners - www.acfe.org*

# ANTECEDENTES

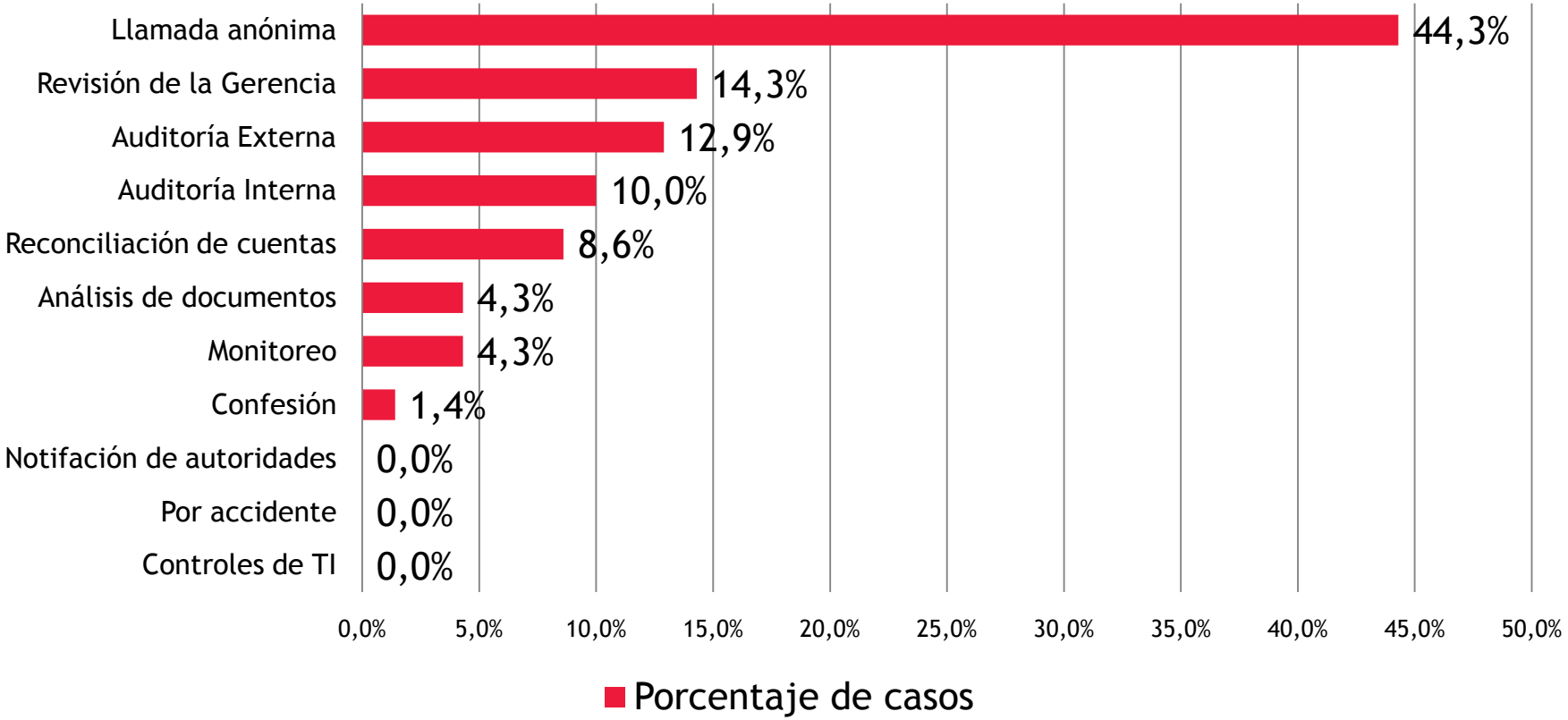
## Tipos de crímenes en Centro y Sur América

| Respuesta | Porcentaje de casos |
|---|---|
| Corrupción | 47.1% |
| Facturación | 28.6% |
| Bienes (No involucra efectivo) | 18.6% |
| Robo de Efectivo | 14.3% |
| Fraude | 12.9% |
| Dinero en mano | 11.4% |
| Reembolso de gastos | 11.4% |
| Fraude de estados financieros | 10.0% |
| Modificación de cheques | 8.6% |
| Planilla | 4.3% |
| Registro de desembolsos | 1.4% |

*Fuente: ACFE - Association of Certified Fraud Examiners - www.acfe.org*

# ANTECEDENTES

## Método de detección del fraude




*Fuente: ACFE - Association of Certified Fraud Examiners - www.acfe.org*

# ORIGEN DEL FRAUDE

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# ORIGEN DEL FRAUDE

## 3 Condiciones principales

**PRESIÓN**

- La clientela baja constantemente
- Quiebra inminente del negocio
- Expectativas y ganancias irreales
- La compensación depende de resultados


**JUSTIFICACIÓN**

- La actividad no es criminal
- Las metas se están cumpliendo
- La competencia lo hace

**OPORTUNIDAD**

- Transacciones significativas relacionadas
- Transacciones altamente complejas
- Uso significativo de estimados y no número exactos

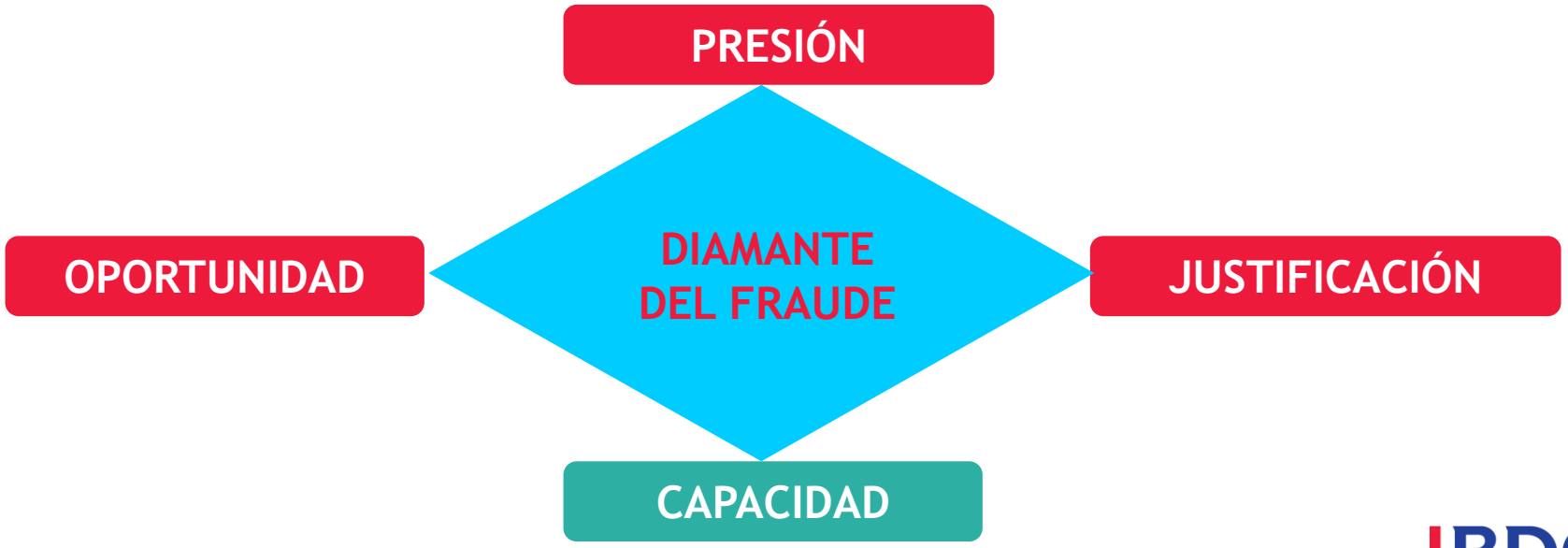
# ORIGEN DEL FRAUDE

## Factor humano

Incorporación del factor humano: **CAPACIDAD**

La oportunidad abre la puerta al fraude, la presión y justificación llevan a una persona a cometer fraude; pero la persona debe tener la capacidad de reconocer la puerta abierta y tomar ventaja de ella una y otra vez.

*Fuente: David Wolfe and Dana Hermanson*



# TIPOS DE FRAUDE
## El árbol del fraude

- Los fraudes pueden ser categorizados en tres grandes tipos:
  - Corrupción
  - Apropiación de activos
  - Fraude de estados financieros

# NORMAS Y ESTÁNDARES

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# NORMAS APLICABLES A AUDITORÍA INTERNA

## Normas para la práctica profesional de Auditoría Interna

- NORMA 1210.A2 – APTITUD PROFESIONAL REQUERIDA POR EL AUDITOR
  - Los auditores internos deben tener conocimientos suficientes para evaluar el **riesgo de fraude** y la forma en que se gestiona por parte de la organización, pero **no** es de esperar que tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude.

# NORMAS APLICABLES A AUDITORÍA INTERNA

## Normas para la práctica profesional de Auditoría Interna

- NORMA 2120.A2 – GESTIÓN DE RIESGOS
  - La actividad de auditoría interna debe **evaluar** la posibilidad de ocurrencia de fraude y cómo la organización maneja gestiona el riesgo de fraude.

- NORMA 2210.A2 – OBJETIVOS DEL TRABAJO
  - El auditor interno **debe** considerar la probabilidad de errores, fraude, incumplimientos y otras exposiciones significativas al elaborar los objetivos del trabajo.

# TÉCNICAS DE PREVENCIÓN E IDENTIFICACIÓN

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# TÉCNICAS DE PREVENCIÓN E IDENTIFICACIÓN

- La posibilidad del fraude es inherente en todo negocio y su mejor defensa es la preparación y monitoreo periódico.
- Técnicas principales para la prevención e identificación del fraude:
  - Establecer una cultura corporativa de control.
  - Establecer una políticas para la denuncia confidencial de posibles fraudes.
  - Identificar los riesgos de manera oportuna y establecer los planes para administrarlos.
  - Monitorear y probar la eficiencia de los controles.

# TÉCNICAS DE PREVENCIÓN E IDENTIFICACIÓN

## Técnicas principales para la prevención e identificación del fraude (continuación):

- Reforzar el proceso de selección y reclutamiento.
- Implementar el uso de herramientas y sistemas para la identificación de actividades sospechosas o no autorizadas.
- Realizar charlas o entrenamientos de concientización al personal sobre el buen uso de los recursos tecnológicos.
- Establecer políticas claras sobre el manejo de incidentes y las sanciones por incumplimiento de las políticas de seguridad.
- Entrenar y certificar a personal de TI para poder prevenir e investigar incidentes de fraude.

# TÉCNICAS DE PREVENCIÓN E IDENTIFICACIÓN HERRAMIENTAS

## Sistemas de detección de intrusos o IDS (Intrusion Detection Systems)

- Detectar escaneo maliciosos o no autorizados y alertar a la administración o gerencia.
- Crear bitácoras detalladas para habilitar un análisis y forense y asistir en las posibles acciones legales.
- Detectar explotación de vulnerabilidades (Network IDS) o archivos o bitácoras que se están borrando (Host IDS) y alertar a la gerencia.

# TÉCNICAS DE PREVENCIÓN E IDENTIFICACIÓN HERRAMIENTAS

Herramientas más comúnmente utilizadas para la prevención e identificación de crímenes y fraudes electrónicos. (fuente: CSI Computer Crime & Security 2008)

| | |
|---|---|
| Anti-virus | **97%** |
| Firewalls | **94%** |
| VPN | **85%** |
| Anti-spyware | **80%** |
| Encriptación de datos | **71%** |
| IDS | **69%** |
| Administración de "logs" | **51%** |
| Herramientas forenses | **41%** |

# HERRAMIENTA DE SEGURIDAD PARA EVALUACIONES DE FRAUDE ELECTRÓNICO

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# HERRAMIENTAS DE SEGURIDAD PARA EVALUACIONES DE FRAUDE ELECTRÓNICO

## *Realizar imágenes de discos (Disk Imaging )*

**EnCase** es una herramienta certificada por NSA (National Security Agency) y NIST (National Institute of Standards and Technology).

**FastBlock** (una herramienta de hardware para prevenir la escritura sobre el disco original). **EnCase** debe ser considerada como la mejor solución para realizar copias imágenes de un disco duro.

# HERRAMIENTAS DE SEGURIDAD PARA EVALUACIONES DE FRAUDE ELECTRÓNICO

## *Recuperación de datos*

**Recover MyFile**, desarrollada por GetData, es utilizada para la recuperación de archivos simples.  Busca en un sector del disco y recupera archivos borrados a través del análisis de los contenidos.

**GetDataBack**, Herramienta para recuperar información cuando una tabla de partición del disco duro, una tabla maestro, o un directorio está corrupto.

# HERRAMIENTAS DE SEGURIDAD PARA EVALUACIONES DE FRAUDE ELECTRÓNICO

## *Recuperación de datos (E-mail)*

**Recover MyEmail**, desarrollado por GetData, analiza los archivos de correo electrónico y busca correos borrados. Recupera mensajes y pueden ser exportados a archivos EML o hacia un nuevo PST y es compatible con Microsoft Outlook y Outlook Express.

## *Análisis de datos*

**dtSearch** es una herramienta para búsquedas simples que genera un índice de todos los archivos almacenados en el disco y permite realizar búsquedas de texto.

# HERRAMIENTAS DE SEGURIDAD PARA EVALUACIONES DE FRAUDE ELECTRÓNICO

## *Recuperación de contraseñas*

**Passware Kit Enterprise** recupera todo tipo de contraseñas en aplicaciones simples como Excel, Word, Windows, Lotus Notes ID, RAR, WinZip, Access, Outlook, Acrobat, Quicken, QuickBooks, entre otros.

# TÉCNICAS Y PROCEDIMIENTOS DE INVESTIGACIÓN DURANTE Y DESPUES DEL INCIDENTE

## Consideraciones para la prevención, análisis y detección de fraude electrónico

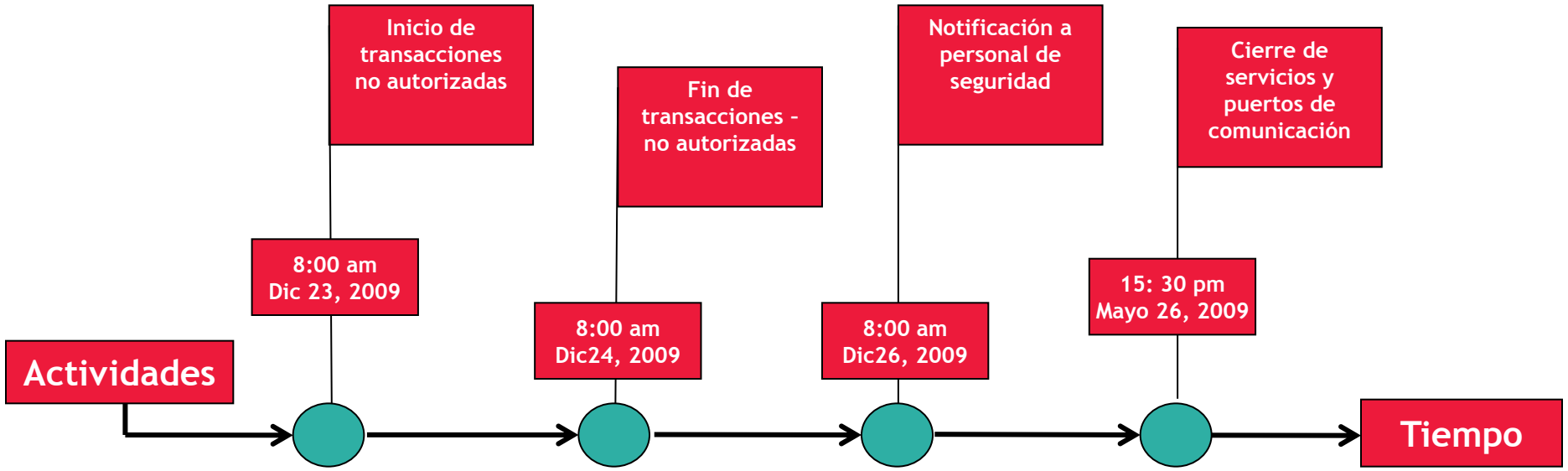
# TÉCNICAS Y PROCEDIMIENTOS DE INVESTIGACIÓN DURANTE Y DESPUES DEL INCIDENTE

## Obtener un entendimiento del entorno donde ocurrió el incidente

- Revisar información histórica de la organización.
- Identificar los ambientes y entornos de tecnología que se utilizan.
- Identificar al personal que mantiene y da soporte a los ambientes de tecnología.
- Identificar los procesos del negocio principales.
- Identificar cualquier cambio significativo que se haya dado recientemente.

# TÉCNICAS Y PROCEDIMIENTOS DE INVESTIGACIÓN DURANTE Y DESPUES DEL INCIDENTE

## Crear una línea de tiempo con los eventos ocurridos y acciones tomadas



# PRINCIPALES PASOS DE EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# METODOLOGÍA EN EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## ETAPA PRINCIPAL

# METODOLOGÍA EN EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## 1 Respuesta y planeación

Definición del alcance (*¿Qué sucedió?*)

Preparación del equipo de trabajo

Definición de procedimientos y herramientas para la administración de datos y evidencia

Definición de estrategia (*directo o "undercover"*)

# METODOLOGÍA EN EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## 2 Remediar e Investigar

- Tomar acciones correctivas de ser necesario (cerrar puertos, activar “logs”).
- Extracción y almacenamiento de datos y evidencia.
- Análisis de datos y evidencias.

# METODOLOGÍA EN EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## 3 Reportes

- Completar investigación
- Preparar recomendaciones
- Preparar y presentar informe

# METODOLOGÍA EN EVALUACIONES Y AUDITORÍAS SOBRE INCIDENTES DE FRAUDE ELECTRÓNICO

## Consideraciones Claves

- La administración de la cadena y custodia de la evidencia es crucial.
- Siempre deben existir copias originales de la información analizadas.
- Se debe almacenar la información por un periodo prudente luego de concluir este proceso de investigación.

# ACCIONES ANTE INCIDENTES DE FRAUDE ELECTRÓNICO QUE SE PRESENTEN

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# ACCIONES ANTE INCIDENTES DE FRAUDE ELECTRÓNICO QUE SE PRESENTEN

- Identificar por lo menos lo siguientes puntos para evaluar el objetivo y alcance:
  - ¿qué sucedió? ¿dónde sucedió? ¿cuándo sucedió o si continúa el caso? ¿está bajo control al situación?
- Determinar la necesidad de involucrar a las autoridades o buscar asesoría legal.
- **No tocar los equipos** – apagar o reiniciar sistemas puede borrar evidencias, como por ejemplo registros y pistas de auditoría.

# ACCIONES ANTE INCIDENTES DE FRAUDE ELECTRÓNICO QUE SE PRESENTEN

| Categoría | Acciones |
|---|---|
| ***REMEDIACIÓN***<br>Tomar acciones para corregir las fallas o deficiencias que conllevaron al problema o incidente. | • Cesar temporalmente las actividades afectadas.<br>• Dirigir comunicaciones o actividades a un ambiente seguro<br>• Suspender trabajos o reasignar al personal<br>• Cambiar contraseñas, accesos, o listas de control<br>• Cambios a seguridad física |
| ***DETECCIÓN***<br>Acciones destinadas a maximizar la cantidad de datos que se pueden recuperar para asistir en la identificación de los responsables y las acciones tomadas. | • Uso de herramientas y técnicas para el diagnóstico<br>• Aumentar el registro y monitoreo de actividades<br>• Revisar las pistas de auditoría en los ambientes de TI<br>• Tomar control de equipos y sistemas<br>• Entrevistas al personal |

# ACCIONES ANTE INCIDENTES DE FRAUDE ELECTRÓNICO QUE SE PRESENTEN

| Categoría | Acción |
|---|---|
| ***Retención de evidencia***<br>Acciones para asegurar que cualquier evidencia está protegida contra cambios y evite dudas sobre su integridad | • Asegurar los medios y copias de respaldo existentes<br>• Completar las rutinas de respaldo de información<br>• Completar la preparación de “imágenes” de los medios de almacenamiento<br>• Recuperar o copiar las bitácoras de operaciones, redes, seguridad, teléfono, fax, voz y video.<br>• Recuperar información y registro de accesos al sitio<br>• Registrar evidencia utilizando cámaras de foto y video.<br>• Prevenir el acceso a todos los equipos involucrados. |
| ***Prevención***<br>Acciones que atienden sistemáticamente las debilidades que dieron paso al incidente | • Hacer recomendaciones que apoyen en el diseño e implementación de medidas preventivas para evitar la recurrencia de este tipo de incidentes. |

# ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

El análisis de riesgo de un sistema debe estar basado en su vulnerabilidad al fraude, abuso interno o externo, mal uso o administración y/o control interno.

Debe considerar por lo menos:

- Factores de riesgo (como por ejemplo, propósito del sistema, documentación existente, frecuencia de las auditorías, etc.)
- Categorizar cada factor de riesgo (alto, medio o bajo) para asignar un valor (3, 2 ó 1).
- Asignar un peso o valor de importancia para cada factor identificado, por ejemplo muy importante, importante, etc.

# ANÁLISIS DE RIESGOS DE VULNERABILIDADES ASOCIADAS A FRAUDE ELECTRÓNICO

- El análisis de riesgo permite identificar que sistemas son de mayor riesgo, es decir alta probabilidad a propiciar un fraude.
- Conlleva a determinar donde se deben enfocar los esfuerzos e inversiones para mantener la seguridad y prevenir fraudes.
- Indica la frecuencia de la revisiones que se deben realizar.

# PREPARACIÓN DE INFORMES Y MATRICES

| Sistema 1 | | | R x I |
|---|---|---|---|
| **Factor** | **Riesgo** | **Importancia** | **Total** |
| **Objetivo**: El sistema se utiliza para registrar transacciones | Alto (3) | Muy importante (3) | 9 |
| **Documentación**: Existe documentación y manuales del sistema | Bajo (1) | Muy importante (3) | 3 |
| | | TOTAL | **12** |

| Sistema 2 | | | R x I |
|---|---|---|---|
| **Factor** | **Riesgo** | **Importancia** | **Total** |
| **Objetivo**: … | Medio (2) | Importante (3) | 6 |
| **Documentación**: … | Bajo (1) | Muy importante (3) | 3 |
| | | TOTAL | **9** |

# PREPARACIÓN DE INFORMES Y MATRICES

| Tabla de Evaluación de Fraudes Electrónicos - Riesgos y Controles | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sistema | | | | | Personal con acceso | | Historial de eventos | | Riesgos/ Fraudes | Controles | | | | | Recomendaciones |
| Nombre | Nivel de Riesgo | | | Valor | Usuario | Perfil | Cantidad | Descripción | | Detalle/Objetivo | Tipo de control | | Efectividad del control | | |
| | Alto | Medio | Bajo | | | | | | | | Automático | Manual | Alta | Media | Baja | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |

# CONCLUSIONES

## Consideraciones para la prevención, análisis y detección de fraude electrónico

# CONCLUSIONES

## Consideraciones para la prevención, análisis y detección de fraude electrónico

- Un análisis de riesgos es necesario para saber que sistemas son más susceptibles al fraude.
- Toda empresa debe mantener y propiciar un ambiente de control interno adecuado para ayudar a prevenir el fraude.
- Se requiere de una metodología y pasos definidos para aplicar técnicas y herramientas de prevención y detección de fraude de manera correcta.
- La empresa debe apoyarse en personal especializado para investigar situaciones donde se ha suscitado un fraude o crimen informático.
- Debe poder identificar responsables e implementar medidas que ayuden a evitar reincidencia de este tipo de eventos.

# GRACIAS

## CONSIDERACIONES PARA LA PREVENCIÓN, ANÁLISIS Y DETECCIÓN DE FRAUDE ELECTRÓNICO

XV CONGRESO LATINOAMERICANO DE AUDITORÍA INTERNA Y EVALUACIÓN DE RIESGOS

Julio R. Jolly Moore, CGEIT, CFE, Internal Audit Quality Assessment

Socio de BDO Consulting

BDO Panamá

jjolly@bdo.com.pa