EL ANÁLISIS FORENSE COMO HERRAMIENTA DE LA INVESTIGACIÓN

Juan Sebastián Grijalva

El Fraude

- Hablamos de Análisis Forense únicamente cuando la pretensión de la organización es la judicialización de la evidencia recolectada.

Situación Actual

ATAQUES EXTERNOS

las organizaciones sufren frecuentemente ataques de diversos tipos a sus sistemas de información por ejemplo: los portales web Secuelist ofrecen información actualizada y completa sobre aquellas amenazas de Internet que están activas, una de sus publicaciones “Desarrollo de las amenazas informáticas” expone los programas maliciosos en Internet y los principales ataques mediante la web.

ATAQUES INTERNOS

Según El Comercio 67% de las instituciones financieras en Perú han experimentado incidentes de seguridad o privacidad en el último año, afirmó un estudio realizado por Deloitte. Con este resultado, Perú tiene el segundo más alto porcentaje en la región, ubicándose solo después de Colombia (100%).

Algunos Casos (robosbancarios.com)

- Banco: BBVA Bancomer
- Cliente: Alejandro Sanchez
- Cantidad Defraudada 2.9 Millones de pesos,
- Cel: 04455-5413-1662
- Email:

- Banco: BBVA Bancomer
- Cliente: Hugo Guerra
- Cantidad defraudada 10.5 Millones de Pesos (Fraude mixto, por **banca en línea**, robo directo de los funcionarios del banco, falsificación de firmas, etc.)

- Banco: Santander Serfin
- Cliente: María Ramírez
- Cantidad Defraudada: 1 Millón de pesos

Sistematización del Problema

La falta de evidencia con validez probatoria impide la judicialización de la misma para que se pueda sancionar a los autores de la mayoría de los fraudes.

POR ESTO!
Quintana Roo
Dignidad, Identidad y Soberanía

Cancún, Quintana Roo, México, jueves 4 de mayo del 2017 | Director General: Mario R. Menéndez Rodríguez | Año 25 No. 8823

Negociazo

Mario Di Costanzo, presidente de la CONDUSEF, informó que sólo los ingresos por comisiones dejaron a los Bancos en el 2016 un total de 143 mil millones de pesos / El cobro de cargos NO reconocidos ascendió a mil 219 millones de pesos, de los cuales únicamente 254 fueron devueltos a los clientes

La República 2-3

Bancos, por las nubes

- Registran 143 mil millones de pesos de ganancias sólo por comisiones
- Tarjetas de crédito, las que más generaron utilidades con 52 mil millones
- Mientras, caen las reservas internacionales de Banxico
- Los gasolinazos disparan los ingresos de Pemex en 43.1%

Fraudes Bancarios en la Impunidad

Las pérdidas económicas anuales por fraudes a usuarios de tarjetas de débido y crédito superan los mil millones de pesos en México y más de 200 mil personas reportan anomalías en sus tarjetas ante la CONDUSEF

La República 3-4

Judicialización Inteligente (Sistematización)

- ¿Los procesos de seguridad ligada a los recursos humanos, es efectivo en la organización?
- ¿Le conviene a la institución financiera judicializar un fraude detectado, poniendo en evidencia que los controles internos fallaron?
- ¿La institución cuenta con especialistas en Seguridad de la Información y Seguridad Tecnológica?
- ¿Cuál es la relación entre la institución financiera y el sistema judicial?

Eventos Internos más Comunes

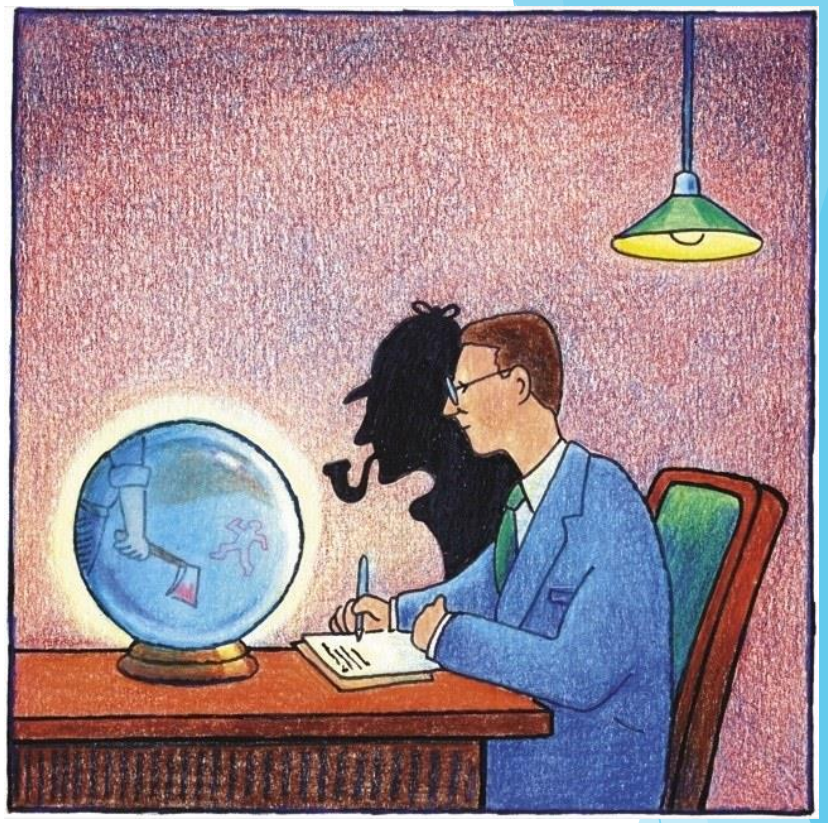
- Fuga de Información
- Suplantación
- Modificación
- Acoso (Pasquines, difamaciones)
- Backdoors

Fuente Deloitte

Método IFPT (Investigación del Fraude Personal y Tecnológico)

- Identificación
  - Perfilamiento
  - Reconocimiento de los medios
- Preservación
  - Levantamiento de la Imagen por parte del Perito
  - Almacenamiento de los equipos y cadena de custodia
- Análisis
  - Búsqueda de información Útil
- Presentación
  - Informe Pericial

Identificación



PERFILAMENTO

El perfilamiento nos permite reducir el ámbito de la investigación, características propias del infractor permitirán obtener información que conduzca a la determinación del mismo.

RECONOCIMIENTO DE LOS MEDIOS

¿Qué información se necesita?

¿Cómo aprovechar la información presentada?

¿En qué orden ubico la información?

¿Acciones necesarias a seguir para el análisis?

HERRAMIENTAS

- Análisis Psicofisiológico
- Análisis del contexto
- Análisis de Equipos y Comunicaciones

Preservación

LEVANTAMIENTO

Se deberá tipificar el levantamiento de la información misma que dependerá de los medios, se podrá obtener imágenes forenses o copias espejo de la información, este proceso debe ser correctamente documentado y se debe contar con la autoridad para hacerlo.

CADENA DE CUSTODIA

Manejo del lugar de los hechos

Fijación del lugar de los hechos

Recolección de la evidencia

Embalaje y rotulado de la evidencias

Transporte de la evidencia

Análisis

- Recuperación de archivos eliminados
- Firmas características
- Documentos
- Archivos gráficos
- Multimedia
- Archivos ejecutables
- Data carving
- Análisis de sistema operativo
- Fecha y hora del sistema

- Conexiones de red abiertas
- Puertos TCP o UDP abiertos
- Usuarios conectados al sistema
- Tabla de enrutamiento interna
- Procesos en ejecución
- Archivos abiertos
- Papelera de reciclaje
- Historial de Internet
- Correo electrónico
- Búsqueda de caracteres
- Metadatos
- Registro de SO

Presentación y Defensa

Finalmente el sistema jurídico basado en la oralidad pretende que se pueda sustentar el informe pericial sobre los hallazgos

Casos de Relevancia

Ecuador, lunes, 2 octubre 2017 | 18:40:23

EL TELÉGRAFO

Política | Economía | Ecuador | Sociedad | Justicia | Fanático | Cultura | Mundo | Opinión

Lunes, 31 Julio 2017 00:00 JUSTICIA Visitas: 2939

Odebrecht compró banco para pagar los sobornos

Foto: Internet

Casos de Relevancia

EL COMERCIO

ACTUALIDAD TENDENCIAS DEPORTES DATA OPINIÓN MULTIMEDIA BLOGS


Abogado de Jorge Glas pedirá se revoque la orden de...


Así fueron las últimas horas de Jorge Glas antes de...


Simpatizantes de Jorge Glas lamentan prisión para


Jorge Glas dice que acata 'bajo protesta' orden

Actualidad · SEGURIDAD

25 de agosto de 2017 00:00

Fiscalía allanó un banco por pago de coimas de Odebrecht

8535

ÚLTIMA HORA

18:34 Neymar deja antes el entrenamiento de la selección de Brasil

18:30 Abogado de Jorge Glas pedirá se revoque la orden de prisión preventiva

18:23 Así fueron las últimas horas de Jorge Glas antes de conocer su orden de captura

18:20 Simpatizantes de Jorge Glas lamentan prisión para Vicepresidente y opositores dicen que se hizo 'justicia'

VER MÁS

LO ÚLTIMO EN VIDEOS

Casos de Relevancia

LA VANGUARDIA | Política

Al Minuto Internacional Política Opinión Vida Deportes Economía Local Gente Cultura Sucesos Temas

Política Elecciones

AVANCE "La UE insta por primera vez al diálogo sobre Catalunya", en la portada de este martes

BRASIL CORRUPCIÓN

Fiscalía inspecciona oficinas de Odebrecht y tres bancos en Panamá

Comparte en Facebook Comparte en Twitter 0

29/12/2016 00:42 | Actualizado a 29/12/2016 00:42

Panamá, 28 dic (EFECOM).- El Ministerio Público (MP) panameño inspeccionó hoy las oficinas de Odebrecht en Panamá y de tres bancos, en el marco de sus investigaciones sobre la constructora brasileña, informaron fuentes judiciales y medios locales.

La inspección ocular fue realizada por la Fiscalía Especial Anticorrupción (FEA), creada este mismo miércoles para que de manera exclusiva investigue los casos de supuesta corrupción que involucran a Odebrecht, como el pago de 59 millones de dólares en sobornos a funcionarios, dijo a Efe una fuente judicial.

El MP no ha precisado el resultado de estas diligencias ni dado detalles sobre las mismas.

El canal de televisión local TVN informó de que la revisión efectuada a las tres entidades bancarias, no identificadas, se realizó para verificar el estatus de las cuentas de Odebrecht.

Más noticias

"Me han roto los dedos uno en uno y me han tocado las tetas mientras se reían"

Al menos 59 muertos y más de 527 heridos en un tiroteo en Las Vegas

Los 8 hábitos que según la ciencia nos ayudan a adelgazar fácilmente

Conclusiones

- El análisis forense, permite a las instituciones investigar de una manera útil y efectiva, cualquier tipo de evento, garantizando la gestión adecuada de la evidencia obtenida de dicha investigación con el objeto de su posterior judicialización.
- Las instituciones bancarias en el año 2017 han sido el principal objetivo de los ataques informáticos así cómo de infiltración, muchos de los casos siguen sin resolverse.
- Las empresas bancarias no solo gestionan efectivo, el dinero no solo está en las bóvedas, el dinero está en los sistemas tecnológicos que apoyan la operación y por tal la alteración de la información es tan valiosa como el mismo dinero.