ANALISIS FORENSE PARA CASOS DE FRAUDE EN LOS SISTEMAS DE INFORMACIÓN TRANSACCIONAL DE UNA ENTIDAD FINANCIERA

Cordero, Eusebio.
eusebiocordero@hotmail.com
Universidad Piloto de Colombia

Resumen—El sector financiero colombiano es muy rentable, sin embargo no escapa al flagelo del fraude en todas sus modalidades y aprovechando el dinamismo del sector y de los nuevos avances tecnológicos, es allí donde se requiere que las entidades financiera aprovechen las herramientas como el análisis de riesgos, la correlación de eventos, la clasificación de activos, el control interno y la informática forense para mitigar y minimizar las amenazas y vulnerabilidades que pueden ser explotadas por delincuentes informáticos para la comisión de delitos. La clave para luchar contra el fraude está en aprovechar el conocimiento que ya tienen dichas entidades y fortalecerlo con la normatividad nacional y el cumplimiento de estándares internacionales como PCI y SOX, lo anterior apoyado en un amplio programa de concientización de clientes y empleados para frenar el avance de los fraudes financieros.

Índice de Términos— Riesgo, Fraudes, Informática Forense, PCI, SOX, Circular 052, Circular 038, Circular 022, Circular 042, clasificación de activos, control interno.

I. INTRODUCCIÓN

En este artículo se realiza una descripción de los elementos y pasos que se deben tener en cuenta al momento de investigar un fraude financiero. En primer lugar se hará una pequeña descripción acerca del fraude y se mostrara un ejemplo de cómo un fraude puede acabar con una entidad financiera.

La dinámica actual del mundo y el creciente uso de las transacciones financieras apalancadas en tecnologías como Internet, cajeros automáticos, remesas, pagos por teléfono, banca móvil, etc., ha ampliado el panorama de riesgo en las diferentes entidades. La tecnología no solo ha beneficiado las buenas prácticas y la globalización de mundo financiero sino que también es usada por los defraudadores, incrementando el riesgo en estas organizaciones.

II. FRAUDE

El fraude se puede definir de acuerdo con las normas internacionales de auditoria como: "Un acto intencional por uno a mas individuos dentro de la administración, empleados o terceras partes, el cual da como resultado una representación errónea de los estados financieros".

Algunas de las señales que pueden dar origen a un fraude y que son válidas para cualquier tipo de organización son:

- No existe separación de funciones en los procesos.
- Existencia de controles innecesarios, ser más productivos.
- Empleados sin vacaciones.
- Conflictos de intereses.
- Compartir passwords o contraseñas.
- Liderazgo por miedo.

Los ítems anteriormente relacionados deben ser la base del establecimiento de un plan estratégico de prevención de fraude, dado que los

mismos facilitan el cometimiento de alguno de los siguientes ilícitos:

- Alteración de registros.
- Apropiación indebida de efectivo o de activos de la organización.
- Apropiación de las recaudaciones o retraso en el depósito y contabilización de las mismas.
- Auto préstamos a la alta gerencia.
- Inclusión de transacciones inexistentes.
- Lavado de dinero y de activos.
- Obtener beneficios económicos o personales mediante el uso de recursos tecnológicos para cometer delitos informáticos.
- Omisión de transacciones existentes.
- Suplantación de funcionarios para realizar transacciones ilegales.
- Apropiarse de pagos realizados por clientes.

En la realización de fraudes el mayor porcentaje de pérdidas se da en las esferas más altas de la organización, generalmente por los llamados delitos de cuello blanco y en todos se pueden identificar claramente los siguientes componentes:

- Motivo: Presión o intensión (necesidad, justificación o desafío) para cometer el fraude.
- Oportunidad: Se percibe la existencia de un ambiente favorable para cometer los actos irregulares o ilícitos cuando se cuenta con el conocimiento, tiempo y están plenamente identificadas las debilidades del sistema de control interno.
- Justificación: Es la razón que tiene el defraudador para cometer y justificar el delito, esgrimiendo que se trata de una compensación o bonificación por su trabajo, primero se convence a si mismo de que existen razones válidas para la comisión del fraude.

Los principales riesgos asociados con el fraude financiero son: el riesgo de crédito, de mercado, de liquidez, operacional1, reputacional, legal, estratégico, cambiarios, de los mencionados anteriormente los que guardan relación con los fraudes financieros son:

- Riesgo operacional: es el riesgo de pérdida resultante de la insuficiencia o fallos de los procesos internos, las personas y los sistemas, o de acontecimientos exteriores. Dentro del riesgo operacional, el comité de Basilea II identifica con claridad el fraude, como uno de los elementos relacionados con la gente, el hurto y robo como elementos asociados a eventos externos.
- Riesgo legal: consiste en las consecuencias que pueden derivarse de la violación por parte de las entidades financieras de las normas que regulan el sistema financiero, uno de los hechos más relevantes relacionados con el riesgo legal es el relacionado con el lavado o blanqueo de capitales.
- Riesgo reputacional la reputación en el sector financiero es fundamental, ya que el negocio se basa en buena medida en la confianza que la entidad genera. En el sector financiero no solo se debe ser integro, competente, dedicado, sino que además debe parecerlo, es decir la percepción y la realidad deben ser lo mismo.

El siguiente ejemplo ilustra claramente un fraude financiero que hizo desaparecer una entidad con bastante historia:

"El Barings[2] Bank fue fundado en 1762 en Inglaterra y logro renombre por múltiples operaciones históricas, entre las cuales se destaca el financiamiento de la adquisición de Luisiana por los Estados Unidos. Sin embargo un ejecutivo designado como gerente general de la sucursal de Singapur, pudo más que toda la historia del banco acumulada en más de doscientos años. Su brillante desempeño deslumbro a todos, llegando a genera el 10% de los beneficios de todo el Banco, pero asumiendo riesgos considerables. Cuando las cosas empeoraron, oculto y trato de revertir sus acciones, iniciando la centrifuga que termino en 1995 con perdida acumuladas por 827 millones de libras. El banco fue declarado en quiebra sus operaciones vendidas a otro banco por una libra, cerrando así una larga historia que termino cuando se consumó el típico riesgo operacional de violación a las reglas de la doble supervisión y ocultación de las operaciones perniciosas".

[2] http://baringsbankupc.blogspot.com/2008/05/historia-del-barings-bank.html

En la mayoría de los casos no es fácil investigar y descubrir quién y cómo realizo el fraude por que no se cuenta con una guía o procedimiento adecuado para realizar esta labor, en este orden de ideas es importante desarrollar la actividad de investigación del fraude financiero partiendo de las herramientas que se han implementado en el sector financiero para dar cumplimiento a las circulares emitidas por la Superintendencia Bancaria de Colombia y estándares como las norma de seguridad ISO 27001, PCI o la ley Sarbanes-Oxley de EEUU.

III. HERRAMIENTAS DE APOYO PARALA INVESTIGACION DE FRAUDES

A continuación se mencionan algunas de las herramientas con la cuales cuenta el sector financiero para su lucha contra el fraude, las cuales en ocasiones no son aprovechadas en la investigación de estos delitos.

En primer lugar se debe contar con un sistema de control interno ágil y que comprenda el plan de la organización, los métodos y medidas adoptadas al interior de la misma para salvaguardar sus activos y verificar la confiabilidad de los datos contables y sus recursos tecnológicos, para ello se deben identificar claramente los elementos que se relacionan entre si y que son inherentes al estilo de gestión de la organización, los cuales son:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión y monitoreo.

Otro aspecto a tener en cuenta es la clasificación de los activos informáticos de la organización, el cual se realiza como parte del análisis de riesgos y debe especificar claramente como las personas administran los activos que tienen bajo su responsabilidad, especialmente los activos que almacene, usen algún tipo de información para el desarrollo de sus actividades ya que la seguridad puede estar basada en el impacto o prejuicio de resultar comprometido el activo de información, facilitando la comisión de un delito financiero.

El desconocimiento acerca del futuro genera sentimientos de temor, duda e incertidumbre. El conocimiento de las vulnerabilidades y la implementación de procedimientos para corregirlas es muy importante, actualmente no existe una medida de seguridad que garantice el cien por ciento de protección contra vulnerabilidades, es aquí donde el análisis de riesgos permiten identificar, conocer y medir el impacto de las amenazas y vulnerabilidades.

El análisis de riesgos busca que la organización cuente con la capacidad de evaluar y manejar adecuadamente los riesgos de seguridad y con base en ello tomar las decisiones de seguridad informática que garanticen la protección de los activos de la organización.

El análisis y administración de logs es uno de los pilares básicos para la gestión de riesgos, de la gestión de identidades y accesos a los sistemas, redes y aplicaciones. Una buena gestión de logs permite conocer casi en tiempo real que está pasando en la infraestructura y sistemas transaccionales de una entidad y que sean relevantes para la seguridad de la misma y a la prevención de fraudes.

La correlación de eventos y de logs es importante ya que el ambiente heterogéneo de las organizaciones emite demasiadas alertas que por sí solas no brindan mucha información, es en este punto donde se requiere de una herramienta de seguridad más práctica, donde varios eventos indican un único problema o riesgo.

Ante la ausencia de una metodología de revisión de logs, la correlación de eventos permite contar con alertas sobre la existencia de problemas o riesgos para la organización, al extraer dichos logs es importante entender que los mismos proviene de diferentes fuentes y entornos con políticas y necesidades diferentes, por lo cual es importante garantizar que no se ha perdido la seguridad e integridad de los datos, por lo tanto se requiere que todos los dispositivos de la organización mantengan sincronizadas sus fechas. Se debe tratar como critico el repositorio donde se almacenan los logs y conservar únicamente al información relevante de los mismos, es importante resaltar que los logs originales de los diferentes dispositivos deben ser respaldados y almacenados de tal manera que se garantice la integridad de los mismos en caso de ser requerido como prueba judicial.

La informática forense es una ciencia sistemática y se basa en hechos premeditados para la recolección de pruebas y su posterior análisis. La

tecnología, juega un papel de suma importancia en la adquisición de información y pruebas necesarias, en este contexto la escena del crimen es el computador, la red y en general todo dispositivo conectado a ella y que sirva como soporte a un sistema de información o sistema transaccional.

Las operaciones que se soportan en la tecnología tienden a reducir costos y ampliar su cobertura través de las redes informáticas, en este escenario es necesario garantizar la integridad y autenticidad de la información. Un seguimiento de los datos que son utilizados por un sistema transaccional financiero puede llevar a identificar un atacante dentro o fuera de la organización llegando a detectar manejos dolosos dentro del sistema transaccional de la organización.

En conclusión, mediante un análisis forense podemos determinar lo ocurrido durante un ataque, una intrusión u otro evento que permita la realización de un fraude en una organización, en este caso una entidad financiera. Básicamente se busca dar respuesta a los siguientes interrogantes: ¿Quién realizo la acción fraudulenta?, ¿Qué activos se vieron afectados o involucrados?, ¿en qué momento se presentó o se materializo el hecho?, ¿Dónde se originó y contra que objetivos? y ¿Cómo fue llevado a cabo y por qué?

Como resultado de un análisis forense se reúne analiza y presenta la información financiera, legal y administrativa de tal manera que pueda ser aceptada por un juez en la imputación de un delito o fraude informático.

En el campo técnico la persona que desee dedicarse al análisis forense debe ser un profesional capacitado, con sólidos conocimientos de informática, técnicas de investigación, legislación penal y una excelente capacidad de análisis y comunicación, además debe ser un profesional equitativo, independiente, honesto, inteligente, astuto, intuitivo, planificador, prudente, cauteloso y con la capacidad de identificar oportunamente cualquier hecho que ayude en el esclarecimiento de fraudes o delitos informáticos.

La informática forense se basa en la evidencia digital que no es otra cosa que información almacenada que puede ser utilizada como prueba en un proceso judicial, para que la misma sea aceptada como prueba se deben seguir ciertos procedimientos en los procesos de recuperación, almacenamiento y análisis de la misma, es acá donde entra en juego el concepto de cadena de custodia, la cual debe ser lo suficientemente robusta para garantizar la inmutabilidad de la evidencia. Es muy importante saber dónde y cómo se obtiene la evidencia en forma eficiente y útil, este punto es muy parecido a la ciencia del mundo forense físico o real, surgiendo como ciencia para aprovechar y garantizar la evidencia electrónica.

Para la realización de una investigación la informática forense requiere que se tengan en cuenta los siguientes aspectos:

- Normas existentes para la obtención de pruebas o resultados.
- Tener conocimiento del procedimiento para llevar a cabo la investigación y en especial las consideraciones legales.
- Identificar las condiciones bajo las cuales, la evidencia será considerada como: admisible, autentica, completa, confiable y creíble.

Lo anterior se encuentra enmarcado dentro del RFC3227, que es el documento que describe los pasos para la recolección de evidencia y almacenamiento de la misma

IV. GUIA PROPUESTA PARA EL DESARROLLO DE UNA INVESTIGACION DE UN FRAUDE FINANCIERO

Para la investigación de un incidente de fraude financiero se propone la siguiente guía la cual se basa en el uso de las herramientas mencionadas anteriormente. Las actividades propuestas son las siguientes, no necesariamente se requieren todas ni en el estricto orden en el cual se presentan.

Requisición o solicitud de investigación: La requisición de una investigación por un posible fraude bancario puede tener su origen en uno de los siguientes hechos:

- Como resultado de una auditoria de revisión del estado actual de los diferentes procesos de la entidad bancaria.
- Por información proveniente de un empleado u otra persona acerca de la sospecha del cometimiento del fraude, o
- Por materialización de un evento de fraude.

En la solicitud es importante relacionar toda la información que permita dar inicio al proceso de

análisis la cual debe contener como mínimo la siguiente información:

- Descripción del fraude o posible fraude, indicando la fecha y los detalles del mismo.
- Información general de quien reporta el fraude.
- Información de los posibles equipos involucrados.

Una vez presentada la solicitud de investigación de un caso de fraude bancario se debe proceder con la conformación de un equipo multidisciplinario que investigara este hecho.

La primera tarea del equipo investigador será iniciar revisando la documentación del caso y validar la que sea relevante para la investigación como: normatividad existente, políticas de seguridad, privilegios de los usuarios, políticas de acceso, diagramas de red, topología de red, inventarios de activos, clasificación de activos, logs, identificación de los equipos y administradores o dueños de los dispositivos involucrados en el ilícito.

Acto seguido se elabora el plan inicial de investigación el cual debe contemplar los dispositivos a analizar y la forma de obtener la información de los mismos, en este punto es importante recalcar que debido a la dinámica de las entidades financieras no es posible en todos los casos retener el equipo para el desarrollo de la investigación sino que el mismo continua soportándolos procesos que requiere la entidad financiera. Para la obtención de la información de estos equipos es importante identificar y realizar una entrevista con el administrador de los mismos para indagar si los logs o la información requerida se puede obtener de un repositorio central de eventos o si es factible el uso del ultimo backup o copia de seguridad realizada y que coincida con la fecha de la realización del fraude.

Entrevista aclaratoria para entender los hechos: Para el mejor entendimiento y desarrollo de la investigación se debe realizar una reunión con la persona o personas que reportaron el fraude con el objetivo de entender de primera mano la situación y extraer la mayor cantidad de información posible, como se mencionó anteriormente se debe realizar la misma reunión con los administradores o dueños de los equipos involucrados en el incidente, lo mismo que con, los posibles sospechosos o involucrados en el incidente.

Como resultado de estas entrevistas debe quedar bien claro el tipo de información requerida y el método de obtención de la misma con el fin de dar inicio al proceso de cadena de custodia de la información obtenida que permita que la misma sea válida como un elemento material probatorio en caso de requerir imputar cargos por el delito cometido.

La entrevista tiene un enorme potencial como instrumento de investigación es importante para la realización del proceso investigativo y en muchos casos su uso es forzado y frecuentemente obligatorio, más aún tiene gran importancia como complementación en relación a los hechos a investigar, en donde su aporte consiste en el entendimiento de los hechos y las obtención de información que permita identificar y analizar los equipos, normas de seguridad, cronogramas de actividades, distribución de las funciones y sistemas informáticos involucrados, lo que facilita la planificación de las acciones necesarias para esclarecer los hechos relacionados con el fraude cometido.

Desarrollar un plan de investigación: La investigación y manejo de cada caso de fraude es distinta una de otra, y es necesario manejar cada caso de manera diferente, dependiendo de las circunstancias del incidente.

La primera parte del plan es la preparación y definición de todos los elementos requeridos para el adecuado desarrollo de la investigación entre las tareas a desarrollar tenemos:

- Identificar plenamente los equipos involucrados en el incidente.
- Definir y elaborar los formatos requeridos para documentar toda interacción que se realice con los equipos involucrados en el fraude.
- Definir cómo se va a adquirir y preservar la información base de la investigación.
- Definir los roles y responsabilidades de cada uno de los miembros del equipo investigador.
- Determinar el tipo de herramientas requeridas para realizar la investigación,
- Iniciar con el debido proceso de cadena de custodia de los equipos y la información obtenida (es importante recalcar que todo el proceso se debe documentar, especialmente

si se va a trabajar con equipos que no se pueden apagar o que son de misión crítica, en este caso es importante identificar plenamente si se lleva un adecuado respaldo de los mismos y si registran los eventos del mismo en un repositorio central con el objetivo de tomar de allí la información y no afectar el desarrollo normal de las actividades de la entidad).

- Priorizar las fuentes de obtención de datos.
- Definir criterio para verificar la integridad de la información obtenida.
- Documentar, documentar y documentar toda acción que se realice.

Para que la información obtenida o el proceso realizado pueda tener algún tipo de validez jurídica se requiere garantizar los requisitos de admisibilidad fijados por la Ley 527 de la Legislación Colombiana: Para valorar la fuerza probatoria de la información digital "… se tendrá en cuenta la confiabilidad en la forma en la que se haya conservado la integridad de la información y la forma en la que se identifique a su iniciador". Los responsables de esta actividad son los denominados "custodios de la evidencia", quienes se harán cargo de validar que la evidencia se encuentre correctamente identificada además de mantener una estricta cadena de custodia. En esta actividad se debe:

- Inventariar los dispositivos o elementos de almacenamiento de evidencia digital removibles como CD's, DVD's, pen drives, memorias USB, discos duros externos, cintas.
- Si se encuentran dispositivos magnéticos involucrados utilizar bolsas antiestáticas.
- Registrar detalladamente los elementos a custodiar, su ubicación y los posibles propietarios o usuarios.
- Proteger la integridad de la evidencia, para ello se debe poder describir claramente la manera como se encontró la evidencia, como se manejó y todo lo que sucedió con ella.

Al final de la investigación debe ser posible responder a las siguientes preguntas:

- ¿Quiénes realizaron la adquisición de la evidencia?
- ¿Cuándo y dónde se realizó?
- ¿Quién protegió y transportó la evidencia?
- ¿Quiénes tienen la custodia de la evidencia?
- ¿Durante cuánto tiempo tendrán la custodia?
- ¿Cómo se almacenan? ¿Qué métodos de protección fueron utilizados?
- ¿Quiénes y porque razón tuvieron contacto con la evidencia?

Es necesario rotular y registrar en el formato de incautación todos los números de serie de los elementos custodiados, para todas las actividades de esta fase de recolección de evidencia es necesario tener las debidas consideraciones, con el fin de minimizar el riesgo de pérdida de su calidad de admisibilidad.

Desarrollar la investigación: Para dar inicio al proceso de atención del incidente se procede a obtener, con las herramientas definidas para este propósito, la información y definir cuál es la más relevante para la investigación, es importante que la misma sea adquirida, almacenada y archivada sin realizar ningún tipo de cambio sobre la misma, se debe actualizar el documento de cadena de custodia para reflejar esta situación.

El siguiente paso es analizar, esta fase es efectuada por los investigadores, en general, se identifican los datos tanto físicos como lógicos para construir una línea de tiempo en donde se correlacionen todos los hechos y se pueda obtener la mayor cantidad de detalles del incidente ocurrido, las personas que intervienen en esta fase deben estar altamente capacitadas.

Para examinar la evidencia, se recomienda los siguientes:

- Preparación: En este paso se debe planear cual va a ser el directorio de trabajo, es decir, donde se va a almacenar la información que se extraerá de lo entregado por los técnicos forenses.
- Extracción: Importante proceso, se recomienda conocer los tipos de extracción de evidencia.
- Análisis de los datos extraídos: En este paso se busca interpretar los datos extraídos y determinar su significado en el caso de estudio.
- Conclusión: Se describe la información significativa, producto del análisis sobre los

dispositivos de almacenamiento y datos suministrados por la fase de recolección.

Teniendo en cuenta lo anterior, se puede decir que la tarea de recuperación y reconstrucción de la evidencia digital, requiere una búsqueda eficiente sobre el contenido de diferentes medios de almacenamiento, con el fin de identificar evidencia relevante, además, el analista siempre debe suponer que puede existir información no visible dentro del medio.

La evidencia digital puede ser clasificada, comparada e individualizada de diferentes maneras, las cuales deben ser utilizadas a criterio del investigador basado en la evidencia que se haya recolectado hasta el momento.

Demostración lógica y tecnológica de las conclusiones: Con base en los análisis realizados se procede a sacar las conclusiones y se describe la forma en la que se realizó el fraude, se valida la hipótesis y con este resultado se procede a la elaboración del documento final.

Generar reporte : Consiste en documentar todas las acciones, eventos y hallazgos obtenidos durante el proceso. Todo el personal está involucrado en ésta fase y es vital para asegurar la cadena de custodia de la evidencia.

V. CONCLUSIONES

Las nuevas tendencias tecnológicas y la lucha contra el fraude requieren una mayor cooperación entre las entidades financieras, los organismos de supervisión y las auditorías externas, a nivel internacional también se requieren de mayor cooperación entre los organismos de supervisión.

A pesar de las medidas de seguridad implementadas por la diferentes entidades financieras, que buscan dar cumplimiento a la normatividad nacional e internacional, y proteger a los clientes y a la misma entidad, no hay nada seguro frente al fraude, que es un problema muy costoso que debe ser atacado en conjunto por las entidades financieras y los clientes, capacitando a las usuarios y demás personal relacionado con el sistemas financiero, enfatizando su responsabilidad y riesgos a los que se encuentra expuesto.

Se deben implementar las recomendaciones emitidas por los entes de control y las definidas en los estándares de la industria con el fin de minimizar la ocurrencia de fraudes financieros.

Estimular la suspicacia en cada uno de los clientes y empleados de las entidades financieras como forma de generación de alertas tempranas ante cualquier riesgo de fraude bancario.

Las autoridades de regulación y supervisión requieren el fortalecimiento de indicadores de alertas tendientes a prevenir la comisión de fraudes, apoyándose en un estricto control interno y aprovechamiento de las nuevas tecnologías.

Una buena estrategia para minimizar la ocurrencia de fraudes es apoyarse en las herramientas de control interno, clasificación de activos, correlación de logs y análisis de riesgo ya que permiten conocer en cualquier momento el real estado de la entidad.

La tendencia de fraude financiero probablemente continuara presentándose, pero no es posible evaluar los futuros escenarios sin tener en cuenta un buen modelo de control interno apoyado en un esquema de generación de alertas mediante el análisis y tendencias, basados en la información almacenada en los logs de los sistemas transaccionales de las entidades financieras y una adecuada clasificación de los activos informáticos.

El uso de la informática forense se convierte en una herramienta ideal para combatir e investigar los fraudes que se presenten en los sistemas transaccionales de las entidades financieras.

VI. BIBLIOGRAFÍA

[1] PCI Security Standars Councill LLC, Requisitos y procedimientos de evaluación de seguridad Versión 2.0, Octubre, 2010; p. 5 – 20. [En línea] 2010 Disponible en Internet: https://www.pcisecuritystandards.org/documents/pci_dss_es-la_v2.pdf.

- ACIS. “UNA INTRODUCCION AL ANALISIS DE RIESGOS”. [En línea]. [15 de julio de 2012] disponible en: (http://www.acis.org.co/fileadmin/Conferencias/ACIS-Riesgos.pdf).
- ALVAREZ VALDEZ, Francisco. “Fraudes Bancarios. Impacto en el resto de las Entidades del Sistema Financiero. Mitigación del Riesgo y Sanciones Aplicadas.”. [En línea]. [15 de

julio de 2012] disponible en: (http://www.felaban.com/archivos_actividades_congresos/11.pdf).

- ARDITA, Julio C. "Experiencias en Análisis Forense Informático". [En línea]. [15 de julio de 2012] disponible en: (http://www.cybsec.com/upload/Ardita_Analisis_Forense_v2.pdf).
- ASOBANCARIA. "Congreso de Prevención de Fraude". [En línea]. [22 de septiembre de 2012] disponible en: (http://www.asobancaria.com/portal/page/portal/Eventos/eventos/congreso_prevencion_fraude/Tab5).
- CAMBRUN BARRERE, Martín. "Análisis Forense Informático". [En línea]. [05 de agosto de 2012] disponible en: (http://www.criptored.upm.es/cibsi/cibsi2009/docs/5mintalk-barrere.pdf).
- FARIAS-ELINOS, M. "La seguridad inicia con el análisis de Riesgo". [En línea]. [17 de julio de 2012] disponible en: (http://seguridad.cudi.edu.mx/congresos/2003/esime/ariesgo.pdf).
- FERNANDEZ BARCELL, Manuel. "ESTUDIO DE UNA ESTRATEGIA PARA LA IMPLANTACIÓN DE LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN". [En línea]. [15 de julio de 2012] disponible en: (http://www.mfbarcell.es/conferencias/Metodolog%C3%ADas%20de%20seguridad_2.pdf).
- FERNANDEZ FDEZ-SANGUINO, Julio. "FRAUDES E IRREGULARIDADES EN LA ACTIVIDAD FINANCIERA". [En línea]. [05 de agosto de 2012] disponible en: (http://www.eben-spain.org/docs/Papeles/X/fdz-sanguino.pdf).
- FERRER, Rodrigo. "METODOLOGIA DE ANALISIS DE RIESGO". [En línea]. [17 de julio de 2012] disponible en: (http://www.sisteseg.com/files/Microsoft_Word_METODOLOGIA_DE_ANALISIS_DE_RIESGO.pdf).
- FISCALÍA GENERAL DE LA NACIÓN. "MANUAL DE PROCEDIMIENTOS DEL SISTEMA DE CADENA DE CUSTODIA". [En línea]. [15 de julio de 2012] disponible en: (http://richardgorky.com/normatividad/resolucion06394.pdf).
- FUND & ASSET MANAGER RATING GROUP. "Metodología de Clasificación de Administradores de Activos". [En línea]. [15 de julio de 2012] disponible en: (http://www.fitchratings.cl/Upload/Metodologia%20Clasificacion%20de%20Adm%20Activos.pdf).
- GOBIERNO EN LINEA - FONDO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. "ANEXO_1_Metodologia_de_clasificacion_de_Activos". [En línea]. [15 de julio de 2012] disponible en: (http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ANEXO_1_Metodologia_de_clasificacion_de_Activos.pdf).
- LOPEZ DELGADO, Miguel. "análisis forense digital". [En línea]. [15 de julio de 2012] disponible en: (http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf).
- MATALOBOS VEIGA, Juan Manuel. "ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN". [En línea]. [15 de julio de 2012] disponible en: (http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf).
- NOREÑA, Ricardo y ESPEJO, David. "Cómo detectar el fraude financiero". [En línea]. [15 de julio de 2012] disponible en: (http://www.cincodias.com/articulo/opinion/detectar-fraude-financiero/20060613cdscdiopi_3/).
- Payment Card Industry Data Security Standard. "PCI – DSS: Data Security Standard". [En línea]. [15 de julio de 2012] disponible en: (https://www.pcisecuritystandards.org/).
- RODRIGUEZ, Marcelo. "Automatización de Procesos de Análisis Forense Informático". [En línea]. [15 de julio de 2012] disponible en: (http://www.cert.uy/historico/pdf/autoForensic.pdf).
- SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Externa 052 de 2007".

[En línea]. [15 de julio de 2012] disponible en: (http://www.superfinanciera.gov.co).

- SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Externa 038 de 2009". [En línea]. [15 de julio de 2012] disponible en: (http://www.superfinanciera.gov.co).
- SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Externa 022 de 2010". [En línea]. [15 de julio de 2012] disponible en: (http://www.superfinanciera.gov.co).
- SUPERINTENDENCIA FINANCIERA DE COLOMBIA. "Circular Externa 042 de 2012". [En línea]. [15 de julio de 2012] disponible en: (http://www.superfinanciera.gov.co).

Autor

Eusebio Cordero O.
Ingeniero de Sistemas
Universidad Nacional de Colombia
2002
Especialista en Seguridad Informática
Universidad Piloto de Colombia
2013