El sistema Financiero y la Seguridad Informática

Amaya Hernández, Janeth Rocio.
jarahdz@gmail.com, jarahdz@hotmail.com
Universidad Piloto de Colombia

Abstract – The implementation of security systems within an organization is vital. Especially when the organization provides financial services and any security breach could lead to million in losses by internal and external fraud. This article aims to explain the impact of new business services in the current security scheme and the challenge that must face the new security implementations.

Resumen— La implementación de la seguridad en sistemas informáticos dentro de una organización es de vital importancia. Sobre todo cuando dicha organización presta servicios financieros y cualquier fallo en la seguridad puede representar millones en pérdidas por fraudes internos y externos. El presente artículo desea exponer el impacto de los nuevos servicios de negocio en el esquema de seguridad actual y el reto al que se deben enfrentar las nuevas implementaciones de seguridad.

Índice de Términos— Cumplimiento Legal, Defensa en profundidad, Sector Financiero, Seguridad Perimetral.

I. INTRODUCCIÓN

El nuevo auge en las operaciones transaccionales vía Internet, los nuevos servicios ofrecidos por las entidades financieras y los nuevos canales a disposición de los usuarios (por ejemplo el uso de dispositivos móviles para realizar transacciones: desde consulta de productos hasta transferencias internacionales), obliga a que los sistemas utilizados para este nuevo esquema de servicios, cuente con un nivel de seguridad importante, no sólo para garantizar la seguridad de la información propia y de usuarios, como uno de los activos más importantes, sino también para dar cumplimiento a las regulaciones vigentes, y es por esto que las entidades financieras se esfuerzan cada vez más en los desarrollos enfocados hacia el aseguramiento de todos los componentes de procesos involucrados.

II. ANTECEDENTES

Las entidades financieras actualmente ofrecen a sus clientes servicios que van desde la consignación de dinero en oficinas hasta la realización de operaciones transaccionales a través de dispositivos móviles. Esto representa un cambio importante en la mentalidad transaccional del usuario, ya que por tiempo y facilidad de operación, las transacciones electrónicas han ganado terreno frente a las transacciones realizadas directamente en una Sucursal.

A. BANCARIZACIÓN

De acuerdo a cifras publicadas por Asobancaria, la bancarización en Colombia también ha tenido un aumento considerable. A corte de diciembre de 2013, en el cuarto trimestre del año, 22.5 millones de personas mayores de edad, contaban con algún producto financiero, lo que representa el 71.5% de la población adulta. El producto más común es la cuenta de ahorros (20.7 millones), seguido por la tarjeta de crédito (6.6 millones). El depósito electrónico (Daviplata[1]) ha logrado posicionarse como un producto innovador que ha vinculado a 1.91 millones de personas en el sector financiero, sin necesidad de abrir cuenta de ahorros con medio transaccional[2].

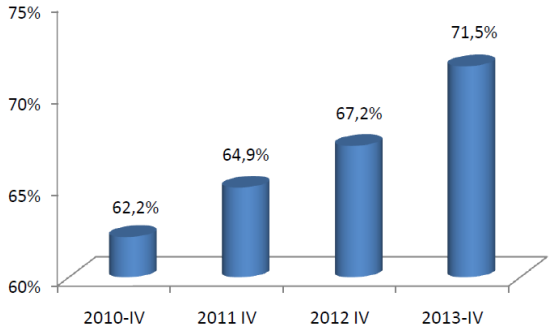

Fig. 1. Evolución de Bancarización en Colombia. Fuente: Asobancaria.

Ante el constante crecimiento en términos de bancarización y desarrollo de nuevos productos de manejo móvil o virtual, los riesgos y amenazas asociados a estas nuevas tecnologías también aumenta, lo que centra la atención en la protección de los sistemas en todos los puntos de procesos, garantizando así fiabilidad al usuario final.

[1] Daviplata: Servicio de monedero electrónico ofrecido por el Banco Davivienda para clientes y para beneficiarios de subsidios y convenios de pago.

[2] http://www.asobancaria.com/portal/pls/portal/docs/1/4070047.PDF

B. EL USO DE CANALES

Dentro de las estadísticas expuestas por la Superintendencia Financiera de Colombia, se encuentra que en el caso de las transacciones presenciales versus las virtuales, de las operaciones realizadas en 2012, el 32 por ciento se realizaron por internet. De acuerdo a la información presentada en medios financieros, el monto de recursos movilizados por internet ha llegado al 27.8%, frente a un 20% que tenía tres años antes[3].

Fig. 2. Operaciones por Canal. Fuente: www.portafolio.co

Si bien ésta información corresponde a estadísticas verificadas en 2013, con esta pequeña muestra se puede evidenciar el crecimiento que puede alcanzar la operación a través de dispositivos móviles e internet a medida que las entidades financieras ofrecen más productos y servicios que permitan realizar transacciones desde la comodidad de la casa. Adicionalmente, conociendo que algunos de los recursos que el gobierno destina para planes como subsidios están siendo entregados a sus beneficiarios a través de medios electrónicos, - contando como uno de los casos, las entregas del subsidio Familias en Acción que se han venido realizando a través de un servicio ofrecido en el celular (DaviPlata)- el mercado de servicios móviles apenas está iniciando una larga trayectoria en la inclusión del portafolio de canales que las entidades financieras ofrecen a sus clientes.

C. REGULACIONES – NORMATIVIDAD PARA PRESTACIÓN DE SERVICIOS FINANCIEROS

Para que se pueda llevar a cabo la prestación de servicios financieros a sus clientes por medio de canales físicos y virtuales, se deben implementar ciertas normas y estándares de acuerdo a la reglamentación estipulada por los entes de control. Entre los estándares requeridos y mejores prácticas de seguridad se encuentran:

- Norma PCI-DSS[4]: Esta norma corresponde a los estándares de seguridad aplicables a todas las plataformas y procesos que intervienen en las operaciones que se realizan con tarjeta de crédito o débito. Contiene 12 requerimientos de seguridad agrupados en los siguientes puntos: Construir y Mantener un red segura, Proteger los datos de las tarjetas, Mantener un programa de administración de vulnerabilidad, Implementar medidas sólidas de control de acceso, supervisar y evaluar las redes con regularidad, Mantener una política de seguridad de la información.
- Implementación Tecnología EMV: Corresponde a un estándar de seguridad que busca reemplazar las llamadas bandas magnéticas de las tarjetas por el chip que contendrá la información del usuario y su producto. Esta implementación en Colombia es obligatoria desde 2013, sin embargo, la tecnología chip si bien dificulta la clonación de tarjetas por banda magnética, no puede evitar el robo de la información por otros medios, especialmente cuando se realizan compras en línea. Adicional a que algunos establecimientos en el mundo aún utilizan la banda magnética, por lo que sigue presentando esta vulnerabilidad.
- Ley de protección de Datos Personales Ley 1581/2012: Esta ley busca proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones, como la recolección, uso y tratamiento por parte de las entidades sean públicas o privadas. Incluye el derecho al habeas data como una garantía al derecho a la intimidad.
- Circular 052 / 042: a) 052/25 oct. 2007: Comprende los requerimientos mínimos de seguridad y calidad en el manejo de la información a través de medios y canales de distribución de productos y servicios. El objetivo principal de la circular corresponde a la implementación de elementos que permita garantizar la seguridad desde los canales a partir de autenticación fuerte, manejo adecuado de información confidencial de usuarios, envío de notificaciones, entre otros. Define como canales de distribución los siguientes: Oficinas, ATM, Receptores de cheques, receptores de dinero en efectivo, POS (pin pad), IVR, Call Center, Accesos Remotos (RAS), Internet, Dispositivos móviles. b) 042 /4 oct. 2012: Imparte nuevas instrucciones relacionadas con los requerimientos de seguridad de la 052.
- Manejo de Autenticación Segura: Si bien, el tema de autenticación viene incluido en los requerimientos de seguridad de la norma 052, es indispensable que las entidades aseguren y certifiquen el acceso de los usuarios a los canales con un adecuado método de autenticación (autenticación fuerte – Autenticación de doble factor).
- Norma ISO27001: Define los requisitos necesarios para la implementación de un Sistema de Gestión de la Seguridad de la Información. También describe los

[3] http://www.portafolio.co/economia/operaciones-bancarias-ganan-terreno-internet.

[5] http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

controles aplicables, las consideraciones de monitoreo, revisión y gestión del sistema SGSI

D. AMENAZAS A SISTEMAS ELECTRÓNICOS

Dentro de las muchas amenazas que se encuentran presentes en los sistemas informáticos, en relación a los canales disponibles para los nuevos servicios, se pueden definir nuevos criterios para su clasificación encontrando presentes entre otros los siguientes:

- Terroristas
- Crimen Organizado
- Hackers
- Competencia Desleal
- Empleados Descontentos

Los hackers hacen parte de las amenazas conocidas como externas a los sistemas de información. Estos se clasifican así:

- Hackers: Individuos que irrumpen en sistemas informáticos para aprender más acerca de ellos.
- Crackers: Hackers con intenciones criminales para afectar o dañar sistemas informáticos con intenciones de ganancias económicas.
- Phreakers: Conocidos por intervenir comprometiendo los sistemas telefónicos.
- Script Kiddies: Hackers con menor nivel de habilidad.
- Hacktivist: Individuos que tienen motivaciones políticas.

Esto nos muestra como el uso de nuevos medios para la entrega de servicios también debe presentar un cambio en la concepción inicial para la clasificación y análisis de amenazas.

E. FRAUDES ELECTRÓNICOS FINANCIEROS

Los intentos de fraudes electrónicos en empresas financieras son comunes debido a la actividad económica de dichas organizaciones y a la información que en sus sistemas contienen (contando con el resultado económico para el atacante en caso de que éstos intentos logren cumplir su finalidad bien sea el hurto de información o de dinero de cuentahabientes).

Según un estudio realizado por la empresa KPMG[5], los datos de ataques cibernéticos tiene origen desde la deslealtad de empleados internos, fallas tecnológicas, hasta la seguridad física y de terceros. Estos factores se pueden validar en el siguiente gráfico:

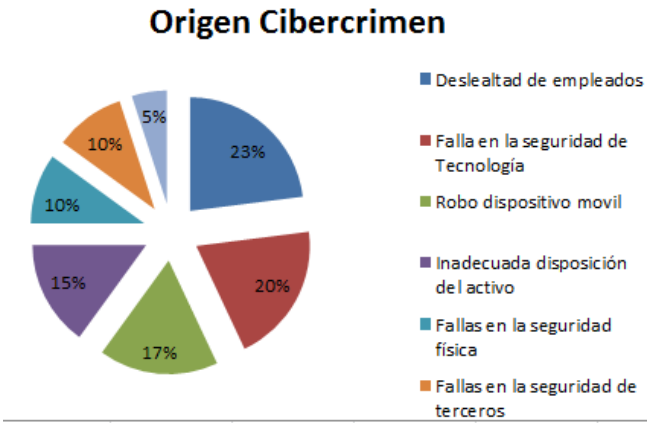

Figura 3. Origen Cibercrimen. Fuente: KPMG

Dentro de lo fraudes electrónicos más conocidos se encuentran:

- Phising: Corresponde al envío de correos electrónicos a usuarios donde se solicita ingresar a una URL e ingresar datos y claves a manera de actualización. Los delincuentes buscan usar dichos datos para un fraude posterior.
- KeyLogger: El término de keylogger realmente corresponde a una definición de una función que permite registrar las pulsaciones de teclado en un computador. Sin embargo, ésta función complementada con malware (virus o incluso dispositivos físicos de rastreo), puede generar que se rastree y monitoree lo que un usuario está digitando y en caso de estar realizando transacciones electrónicas, se puede obtener las credenciales con las que éste accesa a su cuenta bancaria.
- Spoofing: Hace referencia a las diferentes técnicas de suplantación de identidad para usos maliciosos. Se puede presentar spoofing en diferentes características (en correos, en IP, en MAC). Algunos tipos de ataques relacionados con spoofing son: Denegación de Servicio (DOS), realizado a través de IP spoofing, suplantando equipos de la misma red de manera que sea más difícil hallar el origen del ataque y éste sea más efectivo; Man in the Middle: Interceptando la comunicación entre dos servidores y utilizando IP spoofing para que no se sospeche de la interceptación, se puede obtener y modificar la información del canal.
- Fuerza bruta: Intentos de acceso a un sistema o a cuentas de usuario a través de la prueba de diferentes combinaciones de contraseña. Para esto ya existen algunos mecanismos que permiten realizar dicha actividad automáticamente (John the ripper, Caín, Medusa, entre otros) y si bien parece algo anticuado, ésta sigue siendo un métodos muy utilizado por los delincuentes.
- Ataques de Diccionario: Complementa el ataque de fuerza bruta, ya que el diccionario como su palabra lo indica ya tiene palabras y claves frecuentes, que

[5] https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf

utilizadas en un ataque de fuerza bruta pueden ser un poco más efectivo.

- Skimming: Consiste en el robo de información de Tarjetas de Crédito, utilizando mecanismos de lectura ilegales, instalados en cajeros automáticos o en datafonos, que realizan la copia de la banda magnética y posteriormente la utilizan en actividades fraudulentas.
- En los ataques internos, si bien no tiene una definición puntual, cabe resaltar que los funcionarios atacantes aprovechan los accesos a la red de su organización y en algunos casos los conocimientos que poseen de sistemas para vulnerar desde dentro las aplicaciones y sistemas.

Estas actividades delictivas finalmente conllevan entre otras a las siguientes consecuencias:

- Accesos no autorizados: Acceso abusivo a un sistema de información, Robo de identidad, Interceptación de información.
- Vandalismo: Negación de Servicios, Destrucción de información, Suplantación de sitio Web, Utilización de Software Malicioso.
- Cibercrimen: Actividades ilícitas que tienen como objetivo el robo, manipulación, alteración o destrucción de activos o información de clientes u organizaciones utilizando para tal fin medios informáticos o componentes electrónicos
- Amenazas Persistentes Avanzadas: Corresponden a grupos organizados, que cuentan con los recursos y la tecnología necesarios para acceder a sistemas informáticos con un objetivo específico. Pueden pasar desapercibidos por cierto tiempo y pueden evadir la detección. Adicional, pueden generar otros accesos a los sistemas.

A nivel de seguridad uno de los principales inconvenientes de estos ataques, es que generalmente los criminales pueden ocultar su ubicación geográfica y es muy difícil poder rastrear dichos ataques. Se valen de la clandestinidad de la red para ejecutar sus crímenes y adicional, éstos no en todos los casos se identifican instantáneamente sino tiempo después de cometido el crimen.

III. IMPLEMENTACIONES SEGURAS PARA SERVICIOS ELECTRÓNICOS

En la actualidad las implementaciones de los sistemas de gestión de seguridad, se han enmarcado en metodologías bien conocidas, dentro de los cuales, se destacan:

Framework	Objetivo
Cobit	Gobierno IT y Auditoria
ISO 27000	Information Security Management system.
ITIL	IT service Manager
NIST	Sistemas de información.

Tabla 1. Metodologías de gestión de seguridad. Fuente: Implementing Cisco IOS Network Security

Para el desarrollo de estas implementaciones se parte de principios de arquitecturas de diseño de seguridad como lo son la Defensa en profundidad, Menor privilegio, el eslabón más débil, desagregación de roles y responsabilidades, etc.

Para el caso particular del articulo y por ser el más difundido e implementado se propone observar a detalle el correspondiente a Defensa en profundidad, ya que éste cubre en su mayoría las guías definidas por los otros principios y es definido por una arquitectura extremo a extremo de seguridad basado en la definición de capas que componen el servicio.

El objetivo de este es crear dominios de seguridad y separarlos por diferentes tipos de controles de seguridad; el funcionamiento se basa en la redundancia de controles donde en caso de la falla de uno de ellos en alguna capa este es mitigado por el de las otras capas.

Las capas comúnmente implementadas se encuentran:

A. CAPA FÍSICA

Contempla el entorno físico de los componentes del servicio (ubicación, condiciones medio-ambientales, acceso, etc.).

Dentro de los controles implementados se cuenta con sistemas de vigilancia y seguridad física perimetral, Controles de acceso (Tarjetas de aproximación, Biométricos), Circuitos cerrados de monitoreo, etc. Se consideran adicionalmente sistemas de respaldo de energía, aire acondicionado los cuales aseguran las condiciones para la funcionalidad de la infraestructura sobre la cual funcionan los servicios.

B. CAPA RED

El aseguramiento de las plataformas internas de una organización es vital para garantizar la disponibilidad e integridad de los servicios. Implementación del zonas desmilitarizadas por medio de elementos de seguridad perimetral de red, estos son los mayormente difundidos del concepto de seguridad, como Firewalls, IDS, IPS, Proxies; a estos se han sumado nuevos conceptos como Firewall de aplicación.

Al interior de perímetro en la capa interna de red se cuentan con protocolos de red y configuraciones como VLAN´s, ACL´s, WIPS para redes inalámbricas, NAC e

implementación de protocolos seguros como Kerberos, SSH, SSL para la comunicación de aplicaciones y gestión de equipos entre otros.

C. CAPA DE HOST - SERVIDORES E INFRAESTRUCTURA

Se dispone desde la implementación de procesos de *Hardening*, controles de contraseñas seguras, controles en el manejo de usuarios, gestión de parches de seguridad, sistemas de antivirus y antimalware, escaneos de vulnerabilidades, etc.

D. CAPA APLICACIÓN

Se busca que las aplicaciones cumplan con estándares de desarrollo y criterios de seguridad definidos. Uso de métodos de autenticación y protocolos seguros para el intercambio de información, manejo de logs, manejo de privilegios de administración, operación, pruebas de vulnerabilidad sobre servidores de aplicación, auditorías a la gestión de administración y desarrollo, entre otras. También aplica el uso de appliances de seguridad que permiten la creación y administración de accesos desde servidores cliente y los request propios de aplicación hacia el servidor que atiende dichas peticiones, incluyendo el aseguramiento físico de los equipos que atienden todas las peticiones y que contienen las bases de datos . La seguridad se complementa con la aplicación de plantillas de seguridad creadas para diferentes tipos de Servidores de Aplicación.

E. CONCIENCIACIÓN

Parte del respaldo y compromiso de la alta Gerencia consignado en la Política de Seguridad definida. Se desarrollan procesos, procedimientos y se implementan programas de capacitación internos, campañas de comunicación, donde se muestre y se consigne la importancia de la seguridad informática dentro de las actividades diarias y como compromiso de todos.

Generalmente se desarrollan campañas en las páginas oficiales de la organización para que los clientes se encuentren informados de los riesgos.

IV. EL NUEVO RETO DE LA IMLEMENTACIÓN DE SEGURIDAD PARA SERVICIOS ELECTRÓNICOS

Como se vio en el artículo, las implementaciones de seguridad tradicionales contemplan el aseguramiento de los servicios hasta donde se consideraba el perímetro interno de la compañía. Pero el desarrollo de nuevos servicios con más canales disponibles para entregarlos para uso de los usuarios finales, ha abierto un abanico de posibilidades los cual lleva a la frontera de los servicios prácticamente hasta el usuario, extendiendo el perímetro de la compañía fuera de esta.

Dentro de lo que corresponde a ofrecer un sitio seguro para la realización de transacciones a partir de un producto financiero, hay una variedad de actores dentro y algunas veces fuera de la organización que deben estar al día con respecto a los lineamientos de seguridad que deben aplicarse dentro del proceso, donde se debe garantizar un aseguramiento desde los operadores y entes externos hasta el punto final de cada operación.

Adicional a esto, las nuevas y cada vez más exigentes regulaciones hacen considerar la necesidad de buscar día a día la innovación en la implementación de nuevas plataformas de seguridad, donde el resultado final sea generar actividades proactivas en vez de reactivas, y dónde sea mayor el monitoreo y evidencias de anomalías antes de que éstas generen algún efecto negativo.

Estas innovaciones no sólo deben considerarse como aplicación de normas vigentes, deben tenerse en cuenta para crear optimizaciones a las políticas de seguridad internas, que refuercen los campos en los que los aseguramientos físicos no pueden llegar: las intenciones y/o necesidades de las personas. Si bien son un activo importante de las organizaciones, también son un punto de falla a considerar. Es por esto que se deben implementar medios de comunicación internos que garanticen el flujo de la información con respecto a las políticas de seguridad a todos los funcionarios.

Así mismo, generar nuevos planes de concientización a usuarios finales dónde conozca no sólo las ventajas del uso de las nuevas tecnologías, sino también los riesgos expuestos en ella. Involucrarlos en el aseguramiento propio de su información y realizar el acompañamiento en el momento que lo requiera a través de los canales de servicio.

V. CONCLUSIONES Y RECOMENDACIONES

- La seguridad bancaria no depende exclusivamente de la entidad financiera. Si bien tienen la obligación de ofrecer aseguramiento en los procesos correspondientes a los nuevos productos y servicios, también es responsabilidad de los clientes concientizarse sobre el buen manejo que se deben dar a éstos. Conocer los lineamientos básicos de seguridad y aplicarlos en su día a día sin importar la complejidad de la operación a realizar.
- Al cumplir con la implementación de las plantillas y con la normatividad exigida para la seguridad Bancaria, si bien se pueden disminuir los fraudes presentados y los intentos de intrusión en un porcentaje considerable, se debe mantener el seguimiento a los procedimientos de seguridad establecidos a través de las pruebas de vulnerabilidad, ethical hacking y auditorías, así como a las remediaciones correspondientes a los eventos presentados.
- El recurso humano es un activo importante de la organización y se debe cuidar como tal. Sin embargo,

también representa un riesgo considerable si no es capacitado, concientizado de su labor y evaluado en su desempeño. Así como tiene privilegios a los accesos de los sistemas, se deben regular las limitaciones de ejecución sobre los aplicativos en base al cargo. Un individuo interno es susceptible de ser el mismo intruso o el canal de acceso a uno, sin darse cuenta.

- Se deben garantizar las actualizaciones en herramientas, procesos y a los recursos de acuerdo a como se presente la necesidad y se evalúen sus riesgos, de forma que se pueda garantizar el cumplimiento de los requerimientos de seguridad de los nuevos servicios desde su desarrollo y optimizar los ya existentes.
- Para poder identificar, controlar y hacer seguimiento a los riesgos y amenazas, se debe contar con un grupo interdisciplinario que evalúe a nivel de los servicios, de la criticidad de éstos en el negocio y en base a nuevos proyectos y optimizaciones en canales transaccionales, sean virtuales o móviles, los riesgos que dichos proyectos o servicios conllevan. Se deben programar y supervisar las debidas labores de prevención, detección, evaluación y reacción en el caso de la materialización de un riesgo, analizando su causa raíz y realizando el seguimiento respectivo a su solución.
- La gestión integral del riesgo es fundamental para la correcta detección de irregularidades que presenten amenazas para las entidades y clientes, y para evitar la materialización de riesgos que puedan afectar la operación, debe existir una implementación adecuada de normas y estándares de seguridad asociados con la industria, siempre contando con el seguimiento de las actividades ejecutadas.

  La innovación es un factor importante en la arquitectura de seguridad. La búsqueda constante de nuevos componentes que permitan el aseguramiento de servidores permitirá definir una implementación robusta de los sistemas de seguridad, un control adecuado a riesgos y amenazas y un mejoramiento continuo de los procesos involucrados.

REFERENCIAS

[1] http://www.socinfo.es/art-socinfo/1623-reportaje-sobre-qseguridad-informatica-en-banca-y-empresasq

[2] http://www.portafolio.co/economia/operaciones-bancarias-ganan-terreno-internet

[3] http://www.asobancaria.com/portal/page/portal/Asobancaria/publicaciones/economica_financiera/reporte_bancarizacion/2013

[4] http://www.asobancaria.com/portal/pls/portal/docs/1/3796048.PDF

[5] http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[6] http://www.colombia.com/tecnologia/actualidad/sdi/80540/tarjetas-con-tecnologia-chip-un-mecanismo-suficiente-de-seguridad

[7] http://colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

[8] http://colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

[9] http://www.certicamara.com/download/eventos/2012/1120_SeguridadparaServiciosFinancieros/Presentacion_novedades_Circular_042_nov_20_de_2012.pdf

[10] http://www.certicamara.com/download/eventos/2012/1120_SeguridadparaServiciosFinancieros/Presentacion_mecanismos_autenticacion_sector_financiero_nov_20_2012.pdf

[11] https://www.kpmg.com/CO/es/IssuesAndInsights/ArticlesPublications/Documents/Encuesta%20de%20Fraude%20en%20Colombia%202013.pdf

[12] Implementing Cisco IOS Network Security – Volume 1. Cisco.