ISSN 2322-8725

# CIBERSEGURIDAD EN EL SECTOR BANCARIO. UNA APROXIMACIÓN A LA INNOVACIÓN EN EL SECTOR FINANCIERO

**Hermann Fuquen, Consultor en Innovación Tecnológica**

**Abstract**— El Sector de servicios financieros enfrenta grandes retos para salvaguardar la integridad y continuidad de sus servicios electrónicos y es en este donde se ha presentado una de las mayores innovaciones a su modelo de negocio en servicios gracias a las tecnologías de la información y la comunicación. El fraude es una de las amenazas a enfrentar el cual solo será posible de mitigar con esquemas innovadores de control y prevención. En este artículo evaluamos el impacto que ha tenido el fraude en el sector financiero e identificamos los métodos para la prevención del fraude que se han desarrollado en el estado del arte.

**Index Terms**— Análisis, CiberSeguridad, Entidad Financiera, Fraude, Mineria de Datos, Monitoreo, Sector Bancario.

## 1. INTRODUCCIÓN

Ciberseguridad, ha sido un término que ha cobrado una fuerte relevancia en las industrias donde la información y el volumen transaccional de sistemas de información hacen parte de la escencia del negocio y su continuidad e integridad aseguran la sostenibilidad del mismo. Diferentes autores han resaltado la revolución que han representado las Tecnologías de la Información y las Comunicaciones a través del desarrollo de Internet, fortaleciendo la generación de conocimiento competitivo en el campo del comercio electrónico (Langari, 2014).

Una de las grandes amenazas para la consolidación de los servicios electrónicos bancarios, es la posibilidad de un eventual fraude en las transacciones realizadas; sin embargo, han surgido grandes corrientes de investigación para mitigar y controlar este riesgo. Actualmente, se utilizan sistemas y métodos inteligentes y técnicas de minería de datos con el fin de detectar el comportamiento sospechoso e inusual y así identificar el fraude y en muchos casos anticiparlo con el fin de proteger al usuario y los intereses de las instituciones bancarias brindando así un servicio eficiente y seguro (Langari, 2014).

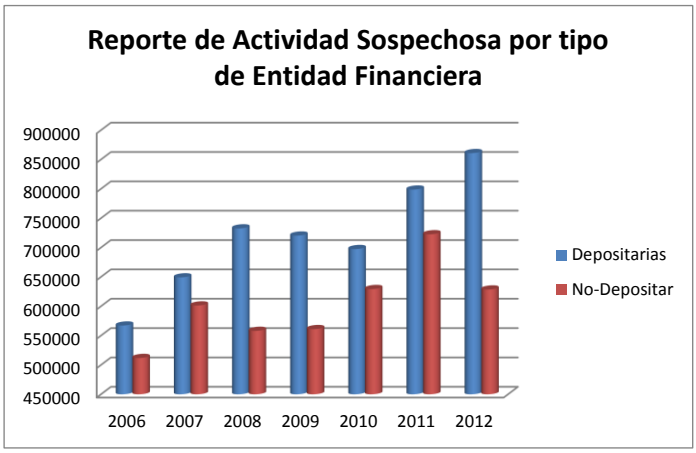


**Figura. 1.** Número de reportes de actividad sospecha al fraude por año en USA.
Fuente: Financial Crimes-Enforcement network (2013)

Según Fraud Watch, los consumidores perdieron aproximadamente 18,82 millones de dólares a través del fraude en 2010, significativamente superior a los USD$ 5.790.000 perdidos en 2004. En promedio, las pérdidas por persona se incrementaron de USD$ 293 en 1999 a USD$ 2,165.15 en 2007. En los laboratorios de uno de los sistemas criptográficos más representativos desarrollados en 1977 el Rivest, Shamir y Adleman (Krantz, S. & Parks, H, 2014), se identificaron 281.000 ataques de Phishing en enero de 2010 dirigidas a las instituciones financieras de todos los tamaños. De otra parte según la oficina gubernamental del gobierno de Estados Unidos "Financial Crimes-Enforcement network" los reportes de actividad sospechosa dentro de entidades financieras en ese país ha presentado una tendencia de crecimiento como se verifica en la Figura 1.

Dentro del análisis por categorías reportadas, doce de las 21 categorías mostraron crecimiento en el año 2012, dentro de estas, las siguientes representaron los cambios más significativos: Robo de identidad (+163%), intrusión a computadoras (+63%), fraude en transferencias electrónicas (+34%), falsificación de tarjetas de crédito y débito (+27%).

Esto demuestra la clara amenaza que representa el fraude para el crecimiento y la generación de confianza que es requerida para el sostenimiento de estos canales electrónicos en el negocio bancario. Lo cual obligua a definir nuevos instrumentos y métodos innovadores para prevenir y anticipar el fraude.

## 2. RIESGO REPUTACIONAL

En general, el riesgo reputacional es el riesgo que potencialmente puede afectar la sostenibilidad o crecimiento de una organización a los ojos de terceros. A menudo, el daño a la reputación de una empresa es intangible y puede emerger gradualmente. Sin embargo, hay fuertes indicios donde los mercados de valores reaccionan inmediatamente a las consecuencias reputacionales de algunos eventos (Perry & Fontnouvelle, 2005).

Según el Basel Committee on Banking Supervision, (2009) se define el riesgo reputacional como aquel derivado de la percepción negativa por parte de los clientes, contrapartes, los accionistas, los inversores, los tenedores de deuda, analistas de mercado, entre otras partes o reguladores pertinentes, que afectan negativamente la

 

capacidad de un banco para mantener medidas existentes o establecer nuevas relaciones de negocios y el acceso continuo a las fuentes de financiación.

El fraude es por tanto una amenaza al riesgo reputacional de las instituciones bancarias, el cual mina la confianza del consumidor final y generará pérdida de clientes y disminución de oportunidades de bancarización de nuevos clientes. Ya que la minimización del riesgo reputacional es fundamental para mantener la credibilidad de la institución bancaria, es importante la aplicación de desarrollos tecnológicos para la prevención del fraude.

## 3. Métodos de Prevención de Fraude

La prevención de fraude se ha convertido en una herramienta de aplicación, en la cual a través de sistemas de monitoreo y control, se evalúa el riesgo de fraude de cada transacción desde la navegación del usuario, lo cual incluye el acceso a las aplicaciones y cualquier actividad que se realice en las mismas. En este proceso, la detección del fraude requiere del uso de políticas basadas en reglas que se fundamentan tanto en la opinión (juicio) o conocimiento humano, como en modelos matemáticos predictivos que permitan puntuar la probabilidad de fraude de una transacción (GARTNER, 2011).

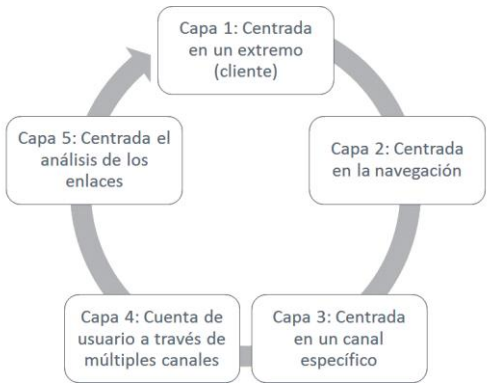


**Figura. 2.** Cinco capas de prevención del fraude.
Fuente: Adaptado de (GARTNER, 2011).

El establecimiento de un sistema que permita la detección y la prevención de fraude, requiere de varias acciones: Por un lado, el establecimiento de un marco de gestión de fraude para la organización. Este marco de gestión debe incluir múltiples capas de monitoreo y análisis (Ver Figura 2), las cuales pueden abarcarse en un plan que avance sobre las prioridades y la complejidad del sistema, para lograr un proceso de monitoreo que permita tanto navegar de manera segura en cualquier tipo de transacción que se realice, como la ejecución de medidas complementarias (por ejemplo a métodos de autenticación existentes). De acuerdo con el informe de GARTNER (2011) la identificación del panorama de amenazas y la conciencia de que este puede cambiar de manera rápida, puede ser previsto si el marco de prevención de fraude y el enfoque de las capas identificado se realizan apuntando a las necesidades de cada empresa.

## 4. Generación de Conocimiento de Datos

La evolución del análisis de los repositorios de datos generados por procesos informáticos a nivel empresarial o académico, permiten la concepción de técnicas refinadas para la generación de nuevo conocimiento para la toma de decisiones con base en metodologías de consolidación, procesamiento y análisis de información.

Se podría definir la generación de conocimiento como un proceso de extracción no trivial, que obtiene patrones que bajo ciertas condiciones establecidas por el usuario (válido, novedoso, potencialmente, útil y entendible) representan conocimiento requerido (Valencia, 2006). El proceso de generación de conocimiento se fundamenta en etapas sistemáticas que se traducen comúnmente del proceso KDD (Knowledge Discovery in Databases), el cual tiene una estructura general distribuida en fases como el procesamiento previo de la información, identificación de patrones y procesamiento final. (Graham Williams, 1996)

## 5. Aplicación de Técnicas de Minería de Datos

Todas las empresas acumulan a lo largo de su historia grandes cantidades de datos, los cuales por lo general son utilizados parcialmente, o no son usados. Actualmente, la cantidad de datos que se manejan, puede impedir una visión completa y clara de la situación de la empresa. La necesidad de información relevante y en tiempo real, ha generado la necesidad de desarrollar sistemas de información que le dén apoyo a los procesos de toma de decisiones. Sin embargo, los sistemas no siempre son suficientes, por no estar al alcance de los requerimientos de la empresa en términos de eficacia. (ÁNGELES LARRIETA & SANTILLÁN GÓMEZ, 1998)

El descubrimiento de conocimiento a través de información dispersa en varios repositorios de información, debe estar compuesto por varias etapas que permiten consolidar, seleccionar, evaluar y presentar información relevante para la toma de decisiones entorno al nuevo conocimiento extraído de forma sistemática.

Para obtener este nuevo conocimiento, es necesario seleccionar las técnicas de minería de datos adecuadas para los sistemas antifraude que permitirán la mitigación de los riesgos de fraude. A partir de las características y ventajas principales de cada técnica de minería de datos se deberán realizar pruebas técnicas con variables tales como eficiencia de la técnica de minería de datos seleccionada, tiempo de respuesta, hardware necesario para el procesamiento, calidad de la información suministrada según las políticas de seguridad de la entidad a la que se aplica, entre otras. (Liao & Chu, 2012).

Para la selección del método o técnica para la migración de y análisis de datos, es necesaria la selección efectiva, teniendo en cuenta las características de cada una de las técnicas existentes y su aprovechamiento según el caso de estudio. Como ejemplo, entre las distintas técnicas de minería de datos contamos con las siguientes:

1. Redes Bayesianas
2. Clasificación por Regresión
3. Máquinas de Vector Soporte
4. Clasificación usando Patrones Frecuentes
5. Vecindad
6. Algoritmos Genéticos
7. Aproximación Fuzzy

Estas son solo agunas de las técnicas más representativas que podrían ser usadas como Fuente de investigación y generación de conocimiento para la mitigación del fraude; sin embargo, existen otras más que en cada caso será necesario evaluar para la correcta gestión del riesgo y mitigación del fraude.

## 6. Tendencias de investigación en el sector bancario

El uso de la tecnología en el sector bancario es esencial para mejorar indicadores de eficiencia y seguridad por medio de mejoras significativas en la experiencia del usuario, sin desestimar los constantes lineamientos regulatorios, cada vez más rigurosos.

Las tecnologías de la información y las comunicaciones asociadas con el sector bancario han crecido desde el año 2013 a una tasa del 3.4% lo equivalente a USD $179.2 Billones y se espera un crecimiento constante, estimando una inversión de USD $192 Billones para el año 2015 (CAPGEMINI 2013). Las mayores inversiones por parte de la banca provienen de la región de Asia Pacifico, las cuales están en el orden de USD $62.2 Billones (CELENT 2013). El sector de la banca de consumo o retail cuenta con la mayor inversión en tecnologías de información y comunicación estimadas en USD $104.5 Billones para el año 2015 mientras que por parte de la banca corporativa se estima una inversión de USD $51.4 Billones para el año 2015.

Las siguientes son las grandes tendencias en materia de desarrollo tecnológico en donde se localizarán las mayores inversiones (ibis).

1. Los bancos deberán mejorar la administración tecnológica de gran cantidad de datos (big data) de tal manera que pueda aprovechar con éxito su extensa base de datos de clientes.
2. Los bancos están invirtiendo cada vez más en herramientas tecnológicas para el análisis de información que permita comprender, cada vez mejor, las necesidades de los clientes, mejorar la gestión de riesgos y cumplimiento, aumentando de esta manera la eficiencia en las operaciones bancarias.
3. Los bancos aumentarán las inversiones en tecnología en los canales digitales (Internet, equipos móviles y los medios como redes sociales) buscando la convergencia digital.
4. Los bancos buscan ofrecer cada vez mejores servicios y productos en un entorno cada vez más competitivo, para esto se hacen inversiones tecnológicas que flexibilicen el core bancario, dinamizando el negocio mediante la oferta de productos innovadores.

## 7. Conclusión

La evolución de los servicios bancarios presenta grandes retos debido a las ventajas y vulnerabilidades que ha traído el uso intensivo de los sistemas de información y comunicación en esta industria.

Como se muestra en la sección anterior las tendencias de investigación en cuanto a la expectativa de desarrollo de nuevos niveles de servicio dirigidos al usuario bancarizado es una variable de importante consideración para el posicionamiento futuro de los bancos dominantes alrededor del mundo. El manejo de la información se convierte en un factor clave ya que una vez los bancos identifiquen sus deficiencias en el manejo de sus datos, se darán cuenta de las grandes posibilidades que tienen para prevenir fraudes, analizar el comportamiento de los clientes en tiempo real y satisfacer las necesidades de los clientes con productos y servicios dirigidos a segmentos específicos.

Por tanto, existen grandes retos relacionados con la implementación de herramientas de análisis de datos. Ante todo, se requiere un cambio en el manejo de las bases de datos y la arquitectura de las herramientas que permiten el análisis de gran cantidad de datos, lo que es conocido como Big Data, los cuales deben ser tenidos en cuenta por el banco con el fin de mejorar su operación.

De otra parte, es importante considerar las tendencias de los usuarios por ejemplo, los clientes bancarios en la actualidad usan la tecnología para personalizar su experiencia en diferentes plataformas como las redes sociales, su música, aplicaciones de interés entre otras. De la misma manera el usuario, en especial los jóvenes esperan que su institución financiera permita la personalización de herramientas, productos y servicios de acuerdo a sus necesidades. Lo anterior representa un gran reto tecnológico para el sector. Tener la capacidad de flexibilizar el core bancario sin dejar atrás las necesidades de los clientes, los cuales, tendrán la oportunidad de tener productos diseñados para satisfacer sus necesidades específicas será un gran reto a solventar intensificando el uso de aplicaciones móviles que exigirán el desempeño de sistemas ubicuos que mantengan altos niveles de seguridad.

La flexibilidad requerida en los sistemas, junto a la demanda de nuevos servicios y el continuo aprendizaje de los métodos cibercriminales que crean nuevos y más sofisticados métodos para concretar el fraude, serán los pilares que delinearan el negocio bancario en los próximos años.

Colombia ya ha ingresado a esta tendencia y se está preparando para afrontar los retos que el servicio bancario exige, la investigación y el desarrollo de nuevas innovaciones promoverán la solidez futura del sistema financiero colombiano que apalancará el desarrollo económico de la nación.

## Bibliografía:

ÁNGELES LARRIETA, M. I., & SANTILLÁN GÓMEZ, A. M. (1998). Minería de Datos: Concepto, características, estructura y aplicaciones. Contaduría y Administración, 79-84.

CAPGEMINI. (2013). Trends in the Global Banking Industry 2013. Paris: Global Financial Services Market Intelligence.

CELENT. (2013). IT Spending in Banking: A Global Perspective. Boston: Celent Global Financial Services.

GARTNER. (2011). Documentos Gartner Inc. Obtenido de Sitio Web Gartner Inc.: https://www.gartner.com/doc/1646115/layers-fraud-prevention-using-beat

Graham Williams, Z. H. (1996). Modelling the KDD Process. A Four Stage Process and Four Element Model. Boston: CSIRO.

Krantz, S. G., & Parks, H. R. (2014). RSA Encryption. In A Mathematical Odyssey (pp. 197-215). Springer US.

Langari, R. M. (2014). Introducing a model for suspicious behavior

 

detection in electronic banking by using decision tree algorithms. Journal of Information Processing and Management, 681-700.

Liao, S.-H., & Chu, P.-H. (2012). Data mining techniques and applications – A decade review from 2000 to 2011. Taiwan: Elsevier Ltd.

Perry & Fontnouvelle, P. (2005). Measuring Reputational Risk: The Market Reaction to. Federal Reserve Bank of Boston.

Valencia, E. (2006). Aplicación de las Redes Neuronales a la Mineria de Datos. México D.F.: UNAM.