Entre Ciencia e Ingeniería, vol.13, no. 26, julio-diciembre de 2019, páginas 36-42. DOI: https://doi.org/10.31908/19098367.1154.
ISSN 1909-8367 (Impreso), ISSN 2539-4169 (En línea)

Soluciones Tecnológicas para la Prevención de Fraude y diseño de un Modelo de Prevención del Riesgo Transaccional para el Botón de Pago[1]

Technological Solutions for Fraud Prevention and design of a Transactional Risk Prevention Model for the Payment Button

J. C. Moreno, C. S. Sánchez, J. C. Salavarrieta y L.M. Vargas

Recibido: noviembre 2018 – Aceptado: septiembre 30 de 2019

***Resumen*— El sector de servicios financieros enfrenta desafíos en el desarrollo de actividades que requieren la utilización de tecnologías de la información y las comunicaciones, debido a que están expuestas a una serie de riesgos como cibercrímen, que pueden afectar la confianza en la marca de la empresa y en el servicio. Con el fin de hacer frente a estos desafíos, ACH Colombia desarrolló un proyecto para anticipar y prevenir los riesgos relacionados con los crímenes informáticos, utilizando herramientas que faciliten el análisis de información para la toma de decisiones. Adicionalmente, ha diseñado e implementado un modelo de prevención especial para el botón de pagos, que es uno de los servicios que esta compañía presta a las entidades financieras, personas jurídicas y naturales y entidades públicas. El presente artículo pretende presentar algunos resultados del proyecto.**

***Palabras clave*— Botón de pagos, ciberseguridad, prevención del cibercrimen, pago electrónico, Prevención fraude, servicios financieros.**

***Abstract* — The financial services sector faces challenges in the development of activities that require the use of information and communication technologies because these are activities exposed to risks such as cybercrimes, which can affect trust in the company's brand and the confidence in the service. In order to face these challenges, ACH Colombia developed a project in order to anticipate and prevent the risks related to computer crimes, using tools that facilitate the analysis of information for decision-making. It also designed and implemented a particular prevention model for the payment button, which is one of the services that the company provides to banks, legal and natural persons and public entities. This article aims to present some results of the project.**

***Descriptors*— Payment button, cybersecurity, cybercrime prevention, electronic payment, fraud prevention, financial services.**

I. NOMENCLATURA

TIC: Tecnologías de Información y comunicaciones.
TI: Tecnologías de Información

II. INTRODUCCIÓN

CON el fin de mejorar su interacción con los clientes y ofrecerles servicios a través de diferentes canales, el sector financiero se encuentra desarrollando una serie de soluciones, con base en tecnologías de información y comunicaciones, las cuales demandan un grado de confiabilidad, de tal forma que le faciliten al cliente final la toma de decisión con respecto a la adopción de las nuevas alternativas de servicio.

Se han considerado focos de vulnerabilidad aquellas situaciones que permiten mayores actividades de fraude, condiciones o actividades que atentan contra las entidades del sistema financiero, y en el caso de los bancos que ponen entre dicho la imagen de entidades seguras y confiables. Haciendo una analogía, en el pasado, las entidades bancarias basaban su prestigio en la protección de sus valores con grandes cajas fuertes y recintos con altos estándares de seguridad e

[1]Producto derivado del proyecto calificado de innovación "*Desarrollo de soluciones tecnológicas orientadas a la identificación y prevención del riesgo transaccional para el sector bancario aplicado al botón de pagos pse*". Presentado a la convocatoria de Beneficios Tributarios de COLCIENCIAS.

J.C. Moreno, ACH Colombia, Bogotá, Colombia, email: jmoreno@achcolombia.com.co.
C. M. Sánchez, Empresa Colombiana de Innovación S.A.S, grupo de investigación COLINNOVACION, email: csanchez@colinnovacion.com.
J. C. Salavarrieta, Empresa Colombiana de Innovación S.A.S, grupo de investigación COLINNOVACION, email: jcssalavarrieta@colinnovacion.com.
L. M. Vargas, ACH Colombia, Bogotá, Colombia, email: lvargas@achcolombia.com.co.

Como citar este artículo: Moreno, J. C., Sánchez, C. M., Salavarrieta, J. C., y Vargas, L. M. Soluciones Tecnológicas para la Prevención de Fraude y diseño de un Modelo de Prevención del Riesgo Transaccional para el Botón de Pago, Entre Ciencia e Ingeniería, vol. 13, no. 26, pp. 36-42, julio-diciembre 2019. DOI: https://doi.org/10.31908/19098367.1154.

impenetrabilidad. De esta manera, la entidad bancaria protegía su principal activo de ataques de criminales [1].

En la actualidad, esa relación entre recinto físico "seguro" y seguridad de los valores del banco, ha evolucionado. Aquellos esquemas de seguridad han cambiado, de la misma forma que el concepto de valor que tienen los clientes. Actualmente, aquellos elementos físicos que contenían el dinero de los clientes son grupos de datos virtuales, los cuales pueden ser administrados a través de la Internet. Los valores se han convertido en datos que migran a nuevos sistemas de contención; la caja fuerte se ha transformado en un disco duro, o espacio en la nube. Esto representa un nuevo reto en términos de seguridad en el sector financiero y bancario [1].

Los sistemas de pago han sufrido el mismo tipo de transformación de tal forma que actualmente el servicio que se prestaba por medios análogos como el dinero, o a través de tarjetas débito y crédito, hoy en día se realizan a través de medios computarizados [2]. En el mercado diariamente se realizan cantidades importantes de transacciones financieras a través sistemas de pago electrónicos o por medios informáticos que tienen diferentes características de seguridad y posibilidad de acceso [3]. Uno de esos sistemas es el Botón de Pago Electrónico, que permite realizar pagos en línea como un servicio alternativo a las tradicionales tarjetas de crédito.

El presente artículo busca presentar los resultados de un proceso que pretende diseñar un modelo de prevención de riesgo transaccional y la implementación de sistemas de información que permitan anticipar y prevenir fraudes en el Botón de Pagos, servicio que ACH Colombia presta a diferentes actores sociales. En la primera sección se abarca el estado de la técnica relacionado con los tipos de riesgo en los sistemas financieros, los requisitos de generación de medios de pago confiables para los usuarios finales, mecanismos de prevención fraude y sus tecnologías asociadas, así como las tendencias actuales y de futuro para prevenir este tipo de actividades en el sector financiero y bancario. Posteriormente se hará una descripción del modelo planteado, los tipos de herramientas implementadas y las fuentes de información, para finalmente presentar algunos resultados e impactos del proceso de implementación.

III. ESTADO DE LA TÉCNICA

Para las empresas independiente de su sector es fundamental identificar los aspectos y características que deben monitorearse en sus plataformas informáticas, con el propósito de prever los modos de operación de los posibles agresores, anticipando la posibilidad de comisión de fraudes y su frecuencia, para establecer no solo factores de diseño de estas plataformas sino los mecanismos y modelos de prevención frente a los diferentes tipos de ataques contra la información que en ellas se alojan. Dado que la inseguridad informática es una propiedad inherente y por lo tanto no se puede evitar, es fundamental realizar un proceso de concientización en la empresa, de tal forma que se identifiquen los riesgos para gestionarlos de manera exitosa [4]

Diferentes tendencias mundiales reflejan que el mundo financiero está basando sus estructuras hacia plataformas que conecten de manera directa a los usuarios de servicios bancarios y entidades bancarias o comerciales cubriendo las necesidades de los usuarios. Esto representa un gran desafío en materia tecnológica y en materia de seguridad. En la actualidad, es evidente el crecimiento en número de transacciones y la cantidad de pagos hechos por medios electrónicos móviles, tal como lo muestra la Fig. 1.

Las entidades financieras deben incrementar esfuerzos en el manejo de la seguridad transaccional en canales no tradicionales. En caso contrario, existen empresas que proveerán de servicios financieros enfocados a nuevos clientes que tienen necesidades específicas los cuales no dudarán en cambiar de proveedor de servicios financieros. Entre las necesidades de los nuevos clientes se encuentran la protección en canales como aplicaciones móviles, de los dispositivos electrónicos asociados con el internet de las cosas, entre otras.

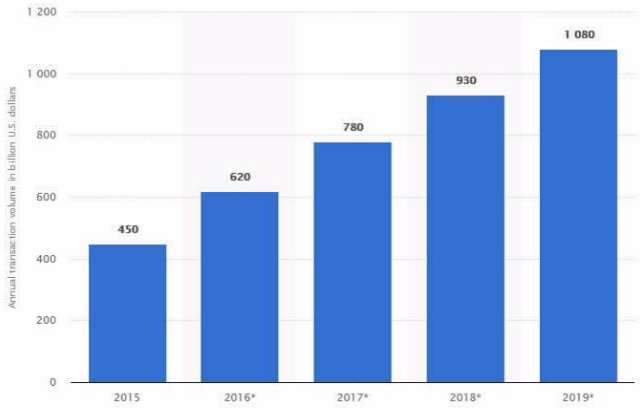

Fig. 1. Ingresos totales de pagos por medio de dispositivos móviles a nivel global 2015-2019 (billones de USD) [5].

A. Tipos de riesgo en sistemas financieros.

Algunos tipos de riesgo que enfrentan las entidades del sector financiero pueden ser: riesgos de pérdida ocasionados por falla en procesos, sistemas o personas que pueden atribuirse a situaciones internas o externas a las compañías [6]. Dentro de los fraudes que se han identificado como externos, se incluyen falsificaciones, intrusión que ocasiona pérdida de información o de operatividad en los sistemas o directamente robo de información [7]. Un ejemplo de tipología de fraude es el cibercrimen que se ha definido como el conjunto de actividades ilícitas realizadas a través de medios informáticos, cuyo objetivo es destruir, alterar o robar información o activos. El cibercrimen ha sido clasificado en tres grupos (ver Fig. 2), uno de los cuales es el acceso no autorizado, que tiene un gran impacto en el desarrollo de actividades financieras [8].

De acuerdo con estadísticas globales relacionadas con este tipo de fraude, se ha identificado que el robo de identidad se encuentra en primer lugar (69% para el 2017) por tipo de infracción, seguido por el acceso abusivo a sistemas financieros (15%) y en tercer lugar el acceso abusivo a cuentas (7%) [9].

En el caso de las transacciones de pago electrónico se ha identificado que tanto la entidad financiera como el usuario de sus plataformas puede ser víctima de este tipo de fraudes, por cuanto el objetivo de los delincuentes en este caso es tomar los recursos de cualquiera de las partes (entidad o cliente) [10].

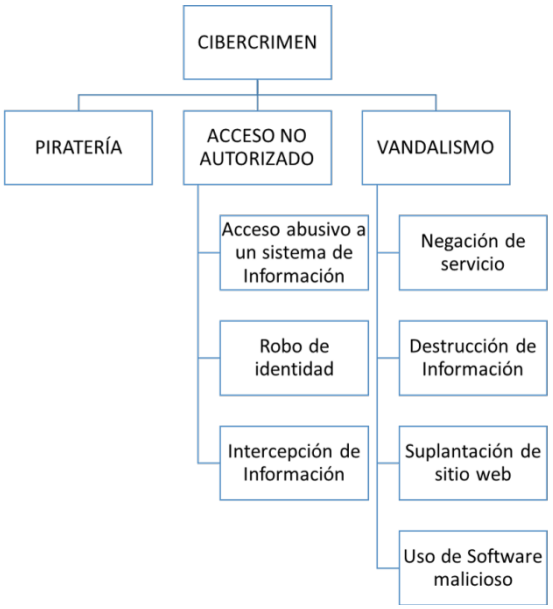

Fig. 2. Tipología de Crímenes Económicos [8].

B. *Medio de pago, confianza e investigación*

Diferentes estudios relacionados con el proceso de adopción de nuevos medios de pago por parte de los clientes de sector financiero han identificado que existen diversos factores que los usuarios analizan antes de decidir el medio de pago a utilizar al realizar transacciones. La confianza y la facilidad de uso se han definido como factores determinantes al momento de decisión del medio de pago a utilizar [11].

Al prevenir riesgos de fraude, las empresas pueden evitar también la aparición del riesgo reputacional que se ha definido como aquel tipo de riesgo intangible, que puede generarse gradualmente, que llega a afectar tanto el crecimiento como la sostenibilidad del negocio [12]. Por lo tanto, se hace necesario para las compañías de este sector generar aceptación entre los posibles usuarios de los servicios financieros, razón por la cual es necesario identificar y prevenir la posibilidad de fraude en las transacciones realizadas por canales que involucren TIC [13].

Proveedores de diferentes soluciones de medios de pago se encuentran desarrollando proyectos centrados en prevenir riesgos de seguridad y anticiparse a posibles situaciones de pérdida de privacidad [11]. Algunas de las soluciones en desarrollo incluyen el uso de sistemas y métodos inteligentes, así como algunas técnicas de minería de datos que buscan hacer un seguimiento a comportamientos inusuales para detectar y anticipar un posible fraude, generando alertas y restricciones que permitan proteger los activos del usuario y de la entidad financiera [13].

C. *Prevención de fraude*

Dentro de los procesos requeridos para anticipar y controlar posibles crímenes a través de medios electrónicos, se hace necesario establecer un marco de prevención de fraude que incluya una serie de capas para monitoreo, que estarían definidas de manera concreta para cada empresa de acuerdo con sus requerimientos, el tipo de negocio y transacciones que realiza [14]. Las capas pueden irse implementando a partir del análisis de prioridades y complejidad del sistema, con el objetivo de disminuir los riesgos tanto en la navegación, como en las transacciones que se realicen [14]. Un ejemplo de los tipos de capas puede verse en la Fig. 3.

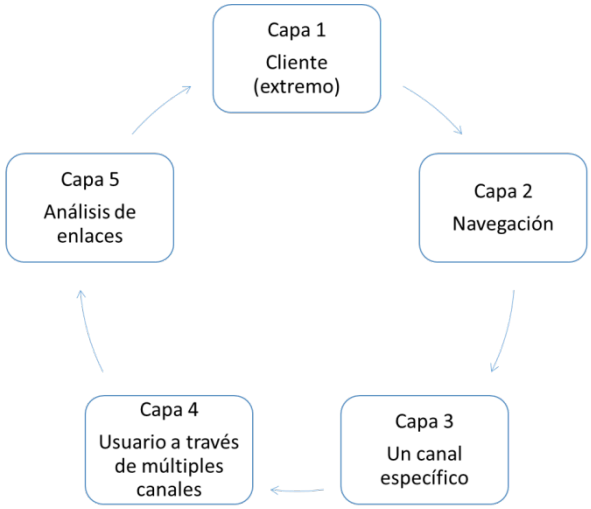

Fig. 3. Capas de prevención de fraude [14].

Se han desarrollado sistemas de monitoreo y control que facilitan el levantamiento de información relacionada con las transacciones a través de los medios electrónicos. Estos sistemas realizan el análisis de diferentes factores relacionados tanto con los procesos de acceso y la actividad que se realiza en las diferentes plataformas, como de los dispositivos desde los cuales se realizan estos trámites, buscando detectar acciones no habituales [14].

El análisis de información implica un proceso previo de implementación de políticas a partir de reglas, que son fruto de modelos matemáticos predictivos y de conocimiento de los funcionarios del banco, estableciendo puntuaciones para cada variable, que permita detectar la probabilidad de fraude en una transacción [14]. De acuerdo con los retos presentes y futuros que enfrenta el sector financiero, sería necesario que las reglas y políticas fueran alimentadas adicionalmente por procesos de captura automática de información, de manera que pudiese ser usada para adaptarlas y refinar el modelo establecido, con el fin de realizar mejoras en los procesos de control [15].

D. *Minería de datos en procesos de prevención*

El proceso de automatización de captura y procesamiento de datos puede darse a partir de información procesada, que se encuentra alojada en bases de datos, que permitan la implementación de procesos de minería de datos, para

identificar regularidades de la información y patrones de comportamiento a través de: técnicas como asociación de datos, clasificación de los mismos, la aplicación de redes neuronales para la generación de clústeres, la generación de un modelo que permita describir las relaciones entre las variables, el análisis de datos a través de series de tiempo o secuencia de patrones, con el fin de describir o predecir comportamientos [16].

Un ejemplo de implementación de minería de datos para el desarrollo de procesos de prevención de fraude, es el uso de redes neuronales, las cuales permiten construir sistemas que se adapten a las condiciones variables y aprender de ellas o partir de cúmulos de datos de magnitud suficiente para desarrollar procesos predictivos de los modelos analizados. En el caso de transacciones en el sector financiero, se tiene como referente el uso de redes neuronales para identificar tanto el comportamiento de usuarios de tarjetas de crédito, como las posibles acciones irregulares correspondientes a la ocurrencia de fraudes previamente registrados al usar ese medio de pago. La identificación de cambio en los patrones de comportamiento del usuario y la acción inmediata de generación de alerta al identificar posibilidades de fraude, ha facilitado una alta tasa de detección de movimientos irregulares, resultando en el desarrollo de respuestas de control sobre las transacciones, evitando la ocurrencia del fraude [17].

E. Tendencias de investigación en el sector financiero y Bancario

Los retos de las empresas del sector financiero relacionados con los procesos de prevención de fraude y desarrollo de sistemas antifraude, ha generado la necesidad de desarrollar e implementar soluciones que puedan contrarrestar los crecientes peligros relacionados [9].

Algunos temas que se encuentran en desarrollo, como la implementación y pruebas para contrarrestar el incremento de ciberataques y fraudes o violación de datos, se listan a continuación:

- Sistemas cognitivos e inteligencia artificial [18].
- Sistemas contables distribuidos particularmente en pagos y tarjetas de crédito [18].
- Sistemas basados en tecnología de Blockchain que permiten asegurar la inmutabilidad de datos, utilizando hash criptoráficos.
- Herramientas de autenticación biométrica con el fin de debilitar riesgos relacionados con robo de identidad [18].
- Herramientas de autenticación biométrica, autenticación con base en geolocalización, así como claves criptográficas (ver Fig. 4) que garanticen que la operación de los sistemas de pago de las empresas que ofrecen este servicio no es propensa a sufrir fraude o violación de datos [19].
- Modelos de análisis de comportamiento con el fin de realizar continuos procesos de monitoreo para prevención de fraude [19].
- Automatización de procesos y aprendizaje de máquina para detectar y prevenir fraudes electrónicos [19].

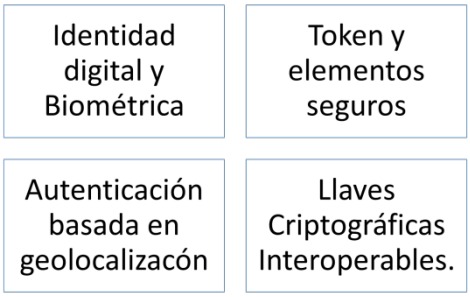

Fig. 4. Técnicas de autenticación [19].

IV. MATERIALES Y MÉTODOS

El botón de pago es un servicio diseñado hace más de 10 años en Colombia, para dar solución a necesidades identificadas por parte de entidades principalmente del Estado, que buscaban facilitar pagos a través de medios electrónicos. Para el desarrollo del proyecto, se diseñó un modelo de prevención como estrategia de anticipación, control y detección de fraudes. Dentro de esta estrategia se integran diferentes herramientas tecnológicas, desarrollo de nuevos procesos y desarrollo de competencias en talento humano.

A. Modelo prevención fraude

El modelo diseñado permite que el usuario del botón de pago ingrese al portal transaccional del comercio a través del cual va a realizar su operación, realizar una autenticación y a partir del análisis de antecedentes transaccionales, se realiza a través del sistema una validación que permitirá aprobar o declinar una transacción, dependiendo de la probabilidad de riesgo que se identifique.

En caso de que el sistema de monitoreo no hubiera logrado filtrar un posible fraude, se hace un reporte y se investiga la situación, de tal forma que se pueda establecer si existió. En caso positivo, se hace un reporte de fraude que entraría a alimentar el sistema de información, para generar posteriormente procesos de análisis de la información, además de procesos de investigación de fraude complementarios. Un diagrama del modelo con el flujo de información puede verse en la Fig. 5.

B. Herramientas de TI

Con el fin capturar y tratar la información, se realiza integración de herramientas de TI que incluyen:

1. *Un sistema de captura y perfilamiento*, a través del cual se recopila la información relacionada del usuario que realiza las transacciones y es remitida a un sistema para perfilamiento del usuario e identificación del dispositivo usado en la transacción. A su vez, esta información se envía a un motor de detección y análisis. A los datos mencionados anteriormente se agrega información de la transacción específicamente, como monto, fecha, entre otras.
2. *Un sistema de prevención de fraude* a través del cual se

realiza la autorización o detención de las transacciones. Adicionalmente se integran reglas en línea para realizar simulaciones que permitan establecer qué tan efectivos son los modelos planteados y recoger información sobre tasa de alertas, contribución a la detección de fraudes, entre otras.

3. *Sistema de Monitoreo, información y análisis* a través del cual se generan alertas por posibles fraudes, que estén fundamentadas en reglas de industria y sean aplicables para una entidad o grupo de entidades. La generación de las alertas se podrá realizar a partir del procesamiento de información en tiempo real, así como de procesar lotes de información. Se utilizará para este sistema modelos de redes neurales, que estará alimentada por un grupo de condiciones o reglas que al ser medidas generarían valores (1, o -1), los cuales, al ser sumados, alcanzan un valor umbral. Utilizando redes neuronales es posible realizar un entrenamiento continuo del modelo de prevención de fraude y su identificación, mediante el análisis de tendencias y correlaciones en las transacciones.

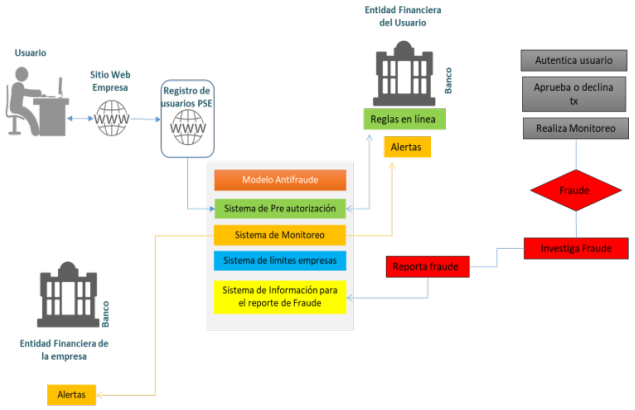

Fig. 5. Esquema Modelo de prevención fraude para botón de pago.

C. Fuentes de Información y Análisis de Información

Dentro del desarrollo metodológico realizado, se ha requerido de la información del botón de pago, los bancos y los comercios. Con la información mencionada, se realiza un proceso exploratorio [20], teniendo en cuenta que se han realizado procesos previos de evaluación en prevención de fraude, pero ninguno de ellos hasta la fecha de inicio del proyecto se había relacionado específicamente con el botón de pago.

Inicialmente se levantó información relacionada con aspectos asociados a las dimensiones integrantes del fenómeno de fraude en pago electrónico, posterior a la cual se requirió de un análisis descriptivo para especificar los perfiles de los usuarios y los fenómenos de fraude en las transacciones electrónicas correspondientes al botón.

Posteriormente, se realizó el análisis a partir de redes neuronales, que permite adicionalmente detectar posibles fraudes en tiempo real, tal como la prestación del servicio del botón de pago lo requiere.

Con la información recogida y analizada, a partir de los sistemas de información y su implementación en entidades bancarias con las cuales se desarrolló el proyecto, se identificaron las variables relevantes del comportamiento de los usuarios, permitiendo realizar procesos de correlación y análisis frente a variables que se habían identificado previamente, relacionadas con comportamientos de fraude, con el fin de diseñar reglas que faciliten la intervención de los sistemas de información, a partir del modelo de ACH y de los bancos.

Posteriormente se simularon las reglas, en los sistemas de información, para verificar que los valores de los indicadores de funcionamiento cumplirían con las condiciones de servicio.

V. RESULTADOS Y DISCUSIÓN

Se implementaron los procesos de gestión de fraude para hacer el monitoreo transaccional, analizar los datos e implementar reglas paramétricas en el sistema. Como medida complementaria, se inició la marcación y reporte de fraude en la herramienta por parte de las Entidades Financieras. Estas actividades vinculadas a estrategias de reducción de fraude a nivel de sistema son la base para el modelo de prevención de fraude del medio de pago.

Se implementaron módulos de Analytics, simulador y redes neuronales, para procesos de análisis, los cuales se encuentran continuamente siendo alimentados por los datos de las fuentes mencionadas previamente.

Particularmente con respecto al módulo de Analytics, se realizaron ajustes que permitieran incluir información para extraer información asociada con la inteligencia de negocio y reportes adicionales con características más adecuadas a los requerimientos de la empresa.

Los módulos de redes neurales necesitan lapsos largos de recopilación de información. En estos módulos se han realizado ajustes en la estructura de los datos, que permitieron incluir mayor cantidad de información relacionada con los fraudes ocurridos previamente.

A partir del proceso de analítica de fraude, se han identificado en diferentes lapsos, los comercios con mayor tasa de siniestralidad de fraude, adicional a un análisis preliminar de los datos de la trama transaccional, con el fin de identificar posibles patrones básicos de fraude.

Periódicamente se realizan simulaciones de reglas paramétricas para seleccionar aquellas que cumplen con los indicadores para detección y generación de alertas de posibles fraudes. Una vez identificadas, se da a conocer a las entidades financieras las reglas y se implementan en los sistemas de información, haciéndoles seguimiento permanente a las variables y consecuentemente al comportamiento. Se realizó la implementación de aproximadamente 180 reglas de parametrización para los procesos de generación de alertas, pre-autorización y “hold” relacionados con el botón de pago.

A partir del análisis del comportamiento de los usuarios del botón de pago, se logró establecer la marcada diferencia entre el usuario y el defraudador en hábitos transaccionales, que se hacen evidentes por ejemplo en los montos de dinero con los cuales realizan cada transacción, el número de transacciones por intervalo de tiempo, así como la cantidad de bancos y de

comercios a través de los que realizan las transacciones.

Para el segundo año de implementación, se observó una disminución para todo el sistema en el monto de fraude total (31%), así como en la tasa de siniestralidad (41%). La Tabla I permite identificar las mejoras significativas presentadas por los indicadores, a raíz del desarrollo e implementación del proyecto.

TABLA I
IMPACTOS OBTENIDOS A PARTIR DE LA IMPLEMENTACIÓN DEL MODELO Y LOS SISTEMAS DE INFORMACIÓN.

Impacto	Indicadores	Por año	
		2016	2017
Reducción de fraude	Monto total de fraude (%)	35%	31%
	Número de casos de fraude (%)	30%	28%
	Tasa de siniestralidad (%)	43%	41%
Pérdida evitada	Valor aproximado (millones de pesos)	10.837	93.241

VI. CONCLUSIONES

Las estrategias de reducción a nivel de sistema pueden tener un impacto más grande en la disminución de fraude, que las estrategias individuales. Es decir, al desarrollar este tipo de actividades de manera colaborativa, es posible tener un mayor nivel de impacto con respecto a los posibles resultados de la implementación a nivel de bancos, comercios o incluso ACH Colombia a nivel individual.

A pesar de tener una estrategia de sistema, se hace necesario que cada entidad financiera, así como el prestador del servicio de pago (ACH Colombia) implemente estrategias individuales que tengan en cuenta el tipo de mercado, la diferencia entre clientes, las particularidades de su negocio, de tal forma que sea posible cerrar los focos de fraude a nivel individual y posteriormente, facilitar la identificación y cierre entre comercios y bancos.

La implementación del proyecto ha permitido detectar y generar disminuciones en la ocurrencia del fraude. Sin embargo, la tipología de fraude varía de manera constante. Por esta causa, la alimentación prolongada de los sistemas de información es fundamental para identificar patrones que antes no eran evidentes, de manera que sea posible seguir afinando las reglas y el modelo establecido para prevención de fraude.

VII. EL FUTURO

Dada la constante evolución de las ciber amenazas sobre el mercado financiero y los mecanismos de pago electrónico, ACH y sus entidades financieras asociadas se encuentran explorando otra serie de tecnologías, que fortalezcan sus modelos de prevención de fraude.

El crecimiento exponencial de uso de dispositivos móviles en las transacciones financieras, así como el gran número de sensores con los que cuentan estos dispositivos, han hecho que la biometría del comportamiento sea un área de estudio relevante para fortalecer los procesos de autenticación de clientes. En los casos donde un usuario vea expuestas sus claves de acceso a canales de Banca virtual, se hace muy difícil que el atacante utilice el dispositivo de la misma forma que el cliente vulnerado. La velocidad con que digita el cliente, los errores que comete, la forma como sujeta el dispositivo, la velocidad a la que se mueve, entre otros, permiten generar una huella de comportamiento muy difícil de replicar.

Por otro lado, ACH se encuentra explorando la utilización de cadena de bloques (*blockchain)* en algunos de sus servicios, aprovechando características de seguridad que brindan este tipo de tecnologías. El uso de criptografía fuerte y la generación y validación de hash de integridad sobre bloques de información, ofrece características de inmutabilidad sobre los datos que son interesantes desde la perspectiva de seguridad en los pagos electrónicos.

REFERENCIAS

[1] Liébana-Cabanillas, F. et al. «Analysing user trust in electronic banking using data mining methods,» *Expert Systems with Applications,* pp. 5439-5447, 2013.

[2] Ali, R., Barrdear, J., y Clews, R. «Innovations in payment technologies and the emergence of digital currencies,» Park Communications Limited, Londres, 2014.

[3] Peha, J. M., y Khamitov, I. M. «PayCash: a secure efficient internet payment system,» *Electronic Commerce Research and Applications,* p. 381–388, 2004.

[4] Cano, J. J. «Inseguridad Informática: Un Concepto Dual En Seguridad Informática,» de *IV Jornada Nacional de Seguridad Informática - ACIS 2004.*, Bogotá, 2004.

[5] PWC, «(Don't) take it to the bank: What customers want in the digital age,» PwC, Nueva York, 2017.

[6] Comité de Supervisión Bancaria de Basilea, «Buenas prácticas para la gestión y supervisión del riesgo operativo,» Banco de Pagos Internacionales, Basilea (Suiza), 2004.

[7] Asociación de Supervisores Bancarios de las Américas, «Temas de Supervisión,» 2010. [En línea]. Available: http://www.ccsbso.org/sites/default/files/g6_es.pdf.

[8] KPMG Advisory Services Ltda., «Encuesta de Fraude en Colombia 2013,» KPMG Advisory Services Ltda., Bogotá, 2013.

[9] Gemalto, «Breach Level Index 2017,» gemalto, Nevada, 2017.

[10] ASOBANCARIA, «Seguridad bancaria en canales no presenciales: una ruta hacia la inclusión financiera,» *Semana Económica 2015,* nº 1002, pp. 1-11, 2015.

[11] Gomber, P., Koch, J. A., y Siering, M. «Digital Finance and FinTech: current research and future research directions,» *Journal of Business Economics,* vol. 87, nº 5, p. 537–580, 2017.

[12] Perry, y Fontnouvelle, P. «Measuring Reputational Risk: The Market Reaction,» Federal Reserve Bank of Boston., Boston, 2005.

[13] Langari, et al. «Introducing a model for suspicious behavior detection in electronic banking by using decision tree algorithms,» *Journal of Information Processing and Management,* pp. 681-700, 2014.

[14] GARTNER, «Documentos Gartner Inc.,» 11 abril 2011. [En línea]. Available: https://www.gartner.com/doc/1646115/layers-fraud-prevention-using-beat.

[15] SAS Institute Inc., «Recursos / White Paper,» 06 junio 2011. [En línea]. Available: http://www.sas.com/resources/whitepaper/wp_5819.pdf.

[16] Valencia, E. «Aplicación de las Redes Neuronales a la Mineria de Datos,» UNAM, México D.F., 2006.

[17] Patidar, R., y Sharma, L. «Credit Card Fraud Detection Using Neural Network,» *International Journal of Soft Computing and Engineering,* pp. 32-38, 2011.

[18] Capgemini, «Top 10 Trends in Banking – 2017,» Capgemini, Paris,

2017.

[19] Garg, G., Vudayagiri, G., Pillai, S. G., y Sharma, R. «Top 10 trends in payments,» Capgemini, Paris, 2018.

[20] Hernandez, R., Fernandez, C., y Baptista, P. Metodología de la Investigación, México: McGraw-Hill, 2006.

Julio César Moreno. Ingeniero de sistemas de la Universidad Nacional de Colombia. Recibió certificaciones internacionales en auditoría de sistemas de información (CISA - Certified Infiormation System Auditor - ISO 27001 auditor), evaluaciones de seguridad (CEH - Certified Ethical Hacker), CISSP (Certified Information System Security Professional), Gerencia de seguridad de la información (CISM), Continuidad de negocio (CBCP - Certified Bussines Continuity Professional), COBIT e ITIL v3. Su experiencia profesional se ha centrado en análisis de riesgos informáticos, debido a sus conocimientos en metodologías de prevención de fraude transaccional, auditoría de sistemas de información, evaluaciones de seguridad y diseño e implementación de planes de continuidad de negocio.

Claudia Marcela Sánchez. Ingeniera mecánica de la Universidad Nacional de Colombia, Especialista en Innovación y Desarrollo de Negocios y Master en Gerencia de la Innovación Empresarial de la Universidad Externado de Colombia. Parte de su experiencia profesional la desarrolló como asesora técnica de los Programas Nacionales de Desarrollo Tecnológico Industrial y Calidad y en el de Investigaciones en Energía y Minería en el área de Innovación en Colciencias, donde tuvo relación con proyectos de diferentes temáticas y sectores. Actualmente es consultora sr. en innovación en COLINNOVACIÓN S.A.S. en donde ha asesorado grandes empresas del sector petrolero, eléctrico, automotor, entre otros.

Juan Salavarrieta. Se graduó de la Pontificia Universidad Javeriana como Administrador de Empresas, 2005, y de la Escuela de Economía y Leyes de Berlín como Magister en Economía Internacional, 2011.
Ejerció profesionalmente en Siemens S.A. en el área de PTD-Services como Commercial Project Manager y actualmente es consultor Sr. en Innovación en la empresa COLINNOVACIÓN S.A.S., en donde ha asesorado grandes empresas del sector petrolero, eléctrico, automotor, bancario entre otros sectores, como consultor en importantes proyectos de innovación y desarrollo tecnológico. Su área de investigación se centra en desarrollo de gerencia de proyectos y economía energética.

Lina Marcela Vargas. Se graduó de la Universidad Distrital Francisco José de Caldas como Ingeniera Industrial, 2006, y de la Universidad Militar Nueva Granada como Especialista en Gerencia de Proyectos - PMP, 2011. Recibió certificaciones como Gerente de Proyectos (PMP, de acuerdo con la metodología de PMI). Ejerció profesionalmente en entidades del sector bancario como el Grupo Aval, el Banco Agrario de Colombia, y en Allianz Colombia y actualmente es Gerente de Proyectos en ACH Colombia, en donde ha liderado proyectos importantes para el sector financiero utilizado metodologías ágiles para el diseño del servicio y su implementación. Su área de investigación se centra en desarrollo de nuevos servicios para el sector financiero y de seguros.