UNIVERSIDAD Rafael Belloso Chacín
Revista Venezolana de Ciencia y Tecnología URBE REVECITEC

Gestión Social Educativa de la Banca en las Pymes para la Prevención del Delito Electrónico

Educational Social Management of Banking in Pyms for the Prevention of Electronic Crime

Marta Cecilia Sepúlveda Osorio / https://orcid.org/0000-0002-1992-4305
msepulv5@correo.tdea.edu.co

María Alejandra Arenas Muñetón / https://orcid.org/0000-0001-7717-5018
marenas6@correo.tdea.edu.co
Tecnológico de Antioquia, Institución Universitaria / Administración Financiera

Resumen

La presente investigación tuvo como objetivo analizar la gestión social educativa de la banca dirigida a la pequeña y mediana empresa (Pyme) para la prevención del delito electrónico y disminución de la suplantación de identidad (phishing), en la ciudad de Medellín (Colombia), en aras de elevar el conocimiento que tienen las Pymes en temas de cibercrimen y su importancia en las entidades financieras en el desarrollo de programas educativos enfocados en la prevención del fraude virtual. Para ello, se estudiaron las diferentes modalidades de fraude existentes, así como las acciones en caso de presentarse y reducir los índices de cibercrimen. Como método de investigación se consideró la técnica de la encuesta, la cual fue aplicada a 250 clientes seleccionados de bancos de dicha ciudad, pertenecientes a las empresas Pyme. Para determinar la confiabilidad del instrumento se aplicó una prueba piloto y se determinó mediante el coeficiente de Alpha de Cronbach, obteniéndose un puntaje de 0.91, altamente confiable. Entre los principales resultados se observaron: 1) los usuarios del sector bancario, no reciben suficiente información acerca de las medidas de seguridad por parte de los entes financieros, con el fin de disminuir el fraude virtual; y 2) los programas de educación financiera son un medio viable para evitar ser víctima del fraude electrónico.

Palabras claves: Educación Financiera, Pymes, Fraude Electrónico, Entidades Bancarias

Abstract

The objective of this research was to analyze the educational social management of banking aimed at small and medium-sized enterprises (SMEs) for the prevention of electronic crime and the reduction of identity theft (phishing), in the city of Medellín (Colombia), in order to raise the knowledge that SMEs have on cybercrime issues and its importance in financial entities in the development of educational programs focused on the prevention of virtual fraud. For this, the different existing modalities of fraud were studied, as well as the actions in case of presenting themselves and reducing the cybercrime rates. As a research method, the survey technique was considered, which was applied to 250 selected clients of banks in that city, belonging to SME companies. To determine the reliability of the instrument, a pilot test was applied and it was determined using Cronbach's Alpha coefficient, obtaining a highly reliable score of 0.91. Among the main results were observed: 1) users of the banking sector do not receive enough information about security measures by financial entities, in order to reduce virtual fraud; and 2) financial education programs are a viable means of avoiding becoming a victim of electronic fraud.

Keywords: Financial Education, SMEs, Electronic Fraud, Banking Entities

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Introducción

Actualmente las empresas bancarias cuentan con un amplio portafolio de productos y servicios para atender las exigencias del acelerado crecimiento y cambios en los mercados financieros. En consecuencia, se ha fomentado la participación de los usuarios en la elección de diferentes alternativas de inversión que les permitan obtener mayores beneficios. Ante este nuevo comportamiento de los consumidores y del mercado, la banca realiza esfuerzos por fortalecer los conocimientos de sus clientes en el ámbito financiero mediante programas educativos los cuales cuentan con la aprobación pública.

Asimismo, estos programas abordan conceptos definidos por la Organización para la Cooperación y el Desarrollo Económico (OCDE, 2019), la cual establece, la educación financiera es el proceso que permite mejorar en los consumidores/inversionistas financieros sus conocimientos sobre productos en esta área, por medio de la información y educación se desarrollan habilidades para identificar los riesgos para tomar decisiones eficaces (Lembert y García, 2015).

Por su parte, Grifoni & Messy (2012) plantean, que este tipo de orientación es un elemento clave en el mundo, pues se pueden desarrollar estrategias nacionales para mejorar la situación económica de los países y la calidad de vida de sus habitantes, tal como lo realizan Australia, Brasil, Canadá, Colombia, Estonia, India, Japón, España, Turquía; una vez determinaron sus debilidades existentes en este campo, buscaron mejorar los niveles de conocimientos de su sociedad frente a este concepto.

Respecto a Colombia, una de las economías miembro de la Red Internacional de Educación Financiera (INFE, siglas en inglés) de la OCDE (2019), provee información para implementar y reforzar programas con los objetivos antes mencionados (Banco de Desarrollo de América Latina CAF, 2013). El Fondo de Garantías de Instituciones Financieras (Fogafin, 2011) menciona la reforma financiera de 2009, la cual comprende la inclusión de educación en la mencionada área como elemento necesario para la protección de los consumidores; allí se expresa, las entidades procurarán educar a sus usuarios en los productos y servicios que ofrecen, naturaleza de los mercados donde actúan, instituciones autorizadas para la prestación de servicios financieros, dotarlos de herramientas para evitar ser víctimas de prácticas engañosas y de fraude electrónico, las cuales actualmente son más recurrentes.

Es así como Colombia es un país donde se han ido incrementando los ataques electrónicos en diferentes entidades pertenecientes al sector público y privado. Como evidencia se tiene el informe de la empresa rusa Kaspersky (2017), donde señala que en el ámbito colombiano se presentó el 9% de ciberataques, ocupando el tercer lugar en América Latina durante los 2 primeros semestres de 2017. Por su parte, la Dirección de Investigación Criminal e Interpol (DIJIN) para ese mismo año, indicó los delitos en la red reflejaron un incremento del 28%, afectando sustancialmente el sector financiero por la vulnerabilidad, dado el frecuente uso de medios electrónicos para realizar diferentes transacciones (Revista Semana, 2017).

En base a lo anterior, las Pymes (pequeñas y medianas empresas) requieren apoyo en este campo. Son organizaciones en constante desarrollo, en Colombia, según información el Departamento Administrativo Nacional de Estadística (Dane, 2018), las Pymes son responsables del 35% del Producto Interno Bruto, generan el 80% del empleo y constituyen el 90% del sector productivo. Sin embargo, son empresas que a menudo se desarrollan dentro de la informalidad, conllevando a poco capital humano capacitado y dificultad para acceder

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

con seguridad a recursos financieros externos, aislamiento, heterogeneidad, desarticulación de políticas público–privadas en los niveles local, regional, nacional.

En referencia al campo específico de la tecnología, Caridad, Cardeño y Ramírez (2018), aseguran uno de los sectores que más ha experimentado una serie de obstáculos en alinearse con la nueva cultura tecnológica son las Pymes, viendo frustradas sus intenciones de desarrollar las competencias informáticas consideradas fundamentales para un desempeño óptimo en su vida laboral.

Por lo antes mencionado, se estudia un sector el cual pudiera estar vulnerable, influyendo en la necesidad de ser orientados para la prevención del fraude electrónico o Ciber-crimen, allí se agrupan delitos ejecutados de forma virtual, a través del uso de tecnologías de la información y la comunicación. De acuerdo con un reporte del periódico El Tiempo (2017) en los primeros meses de ese año, se produjeron en América Latina 677 millones de amenazas cibernéticas, es decir, cada hora se registraron 117 ataques, 33 en un segundo.

El presente artículo hace énfasis en la suplantación de identidad (phishing), puesto que, representa uno de los delitos cibernéticos más frecuentes en Colombia, país donde se reciben alrededor de 200 denuncias mensuales relacionadas con envíos de correos falsos, dirigidos especialmente al sector bancario (Revista Portafolio, 2017), Acevedo (2018) agrega el 74% del ciber-crimen, se agrupa entre ciudades como Bogotá, Cali, Medellín, Barranquilla, Cartagena y Bucaramanga.

Objetivo General

Analizar gestión social educativa de la banca en las Pymes para la prevención del delito electrónico en la ciudad de Medellín (Colombia).

Objetivos Específicos

Identificar los beneficios de una educación financiera a los usuarios Pymes en la prevención del delito electrónico (phishing) en la ciudad de Medellín (Colombia).

Caracterizar los principios básicos de una educación financiera para la prevención del delito electrónico (phishing) en la ciudad de Medellín (Colombia).

Identificar las causas que dan origen al delito electrónico (phishing) en la ciudad de Medellín (Colombia).

Metodología

El presente trabajo corresponde a una investigación cuantitativa de tipo descriptiva. Se aplicó una encuesta, realizada de manera virtual a través de un cuestionario mediante Google Forms con 20 afirmaciones derivadas de los objetivos específicos. Como opciones de respuesta se utilizó una escala tipo Likert, basada en la expresión de frecuencia, comprendida en cinco (5) rangos: siempre, casi siempre, algunas veces, casi nunca y nunca, siendo uno (1) siempre y cinco (5) nunca (Díaz y Luna, 2014).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Este estudio fue aplicado a una población conformada por 250 informantes, clientes de una entidad bancaria de la ciudad de Medellín, pertenecientes al sector Pyme, siendo uno de los más vulnerables a fraudes electrónicos de acuerdo a información suministrada por la misma entidad bancaria intervenida. Con respecto a la confiabilidad del instrumento, se aplicó el coeficiente de Alfa de Cronbach, para confirmar la veracidad de la escala de Likert (Bonett & Wright, 2015). El resultado obtenido al aplicar la fórmula en la herramienta ofimática Excel fue 0.91.

Fundamentación Teórica

Programas de educación financiera de calidad: principios básicos

Organismos como la Comisión Europea (2007) plantean principios dirigidos a instaurar programas nacionales enfocados a promover consumidores educados en términos de economía y finanzas; planes de formación sobre la comprensión, análisis de inconvenientes y riesgos financieros. Entre las condiciones para el éxito de estas iniciativas, se encuentra, contar con procesos de calidad que puedan operacionalizarse en forma transparente, neutral (Fernández, Martel, Príncep, Blanch, & Monfort, 2015).

Por su parte, la Comisión de la Comunidad Europea (2007) contempla que los planes de educación financiera deben promover principios de calidad donde se creen estrategias de educación financiera productivas. Los principios a los cuales se hace referencia, son ocho, sin embargo, solo cuatro se relacionan con el tema de investigación:

1) Los programas de educación financiera deben dirigirse a la satisfacción de necesidades específicas del usuario, para ello se requiere realizar investigaciones donde se descubran las necesidades a suplir. Programas que estén a su disposición, es decir, el programa debe ofertarse de forma clara y disponer del mismo en cualquier momento.

2) Los planes de educación financiera deben contener herramientas para el entendimiento de riesgos y problemas financieros; es decir, concientizar a las personas acerca de los riesgos y problemas como el fraude.

3) La educación financiera por parte de prestadores de servicios financieros debe ser de forma imparcial, justa y clara; que eduque a los consumidores para asegurar la diferencia entre la información de productos, la educación financiera, así como sugerir al usuario un producto o servicio financiero.

4) Aquellos prestadores de servicios en educación financiera deben evaluarse de forma periódica y renovar los planes que ejecutan para la mejora en dichas prácticas; dichos prestadores deben adherir a los programas las cuales permita hacer evaluación constante de logros obtenidos y verificar el cumplimiento de los objetivos planteados por el mismo.

En función a lo antes mencionado, para atender la satisfacción de necesidades de los usuarios, las entidades bancarias deben gestionar el desarrollo de programas que fortalezcan la comprensión y sensibilización sobre el tema; disponer de recursos para la práctica orientadora dirigida a disminuir la incertidumbre en términos financieros. Con información tan clara dirigidos a la diferenciación de un producto de otro, un beneficio de otro y pueda dicha información estar en todo momento a disposición de sus usuarios (Lucena y Repullo, 2013).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Fraude electrónico como tendencia mundial: caso colombiano

El impacto del auge tecnológico en la sociedad ha dado lugar a grandes transformaciones desde el ámbito económico, social, cultural y político, permitiendo alcanzar avances que han contribuido al progreso del mundo y la humanidad, pese a los beneficios, la era informática considerada como la cuarta revolución industrial ha dado paso a tendencias mundiales como la referida en este estudio: el ciber-crimen, definido por Romeo (2007) como el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual.

Asimismo, el fraude electrónico comprende una cantidad considerable de modalidades creadas y desarrolladas por individuos cuyos intereses se centran en los medios magnéticos, para sacar provecho de éstos de formas inadecuadas. A continuación, se describen las modalidades más relevantes del delito electrónico con su respectivo concepto.

Cuadro 1.
Modalidades de fraude electrónico

Autor	Modalidad	Concepto
Acurio del Pino (s.f)	Data diddling o manipulación de datos de entrada	Consiste en la alteración desautorizada de datos, buscando generar movimientos indebidos en las transacciones que realizan las empresas.
Fuentes, Mazún y Cancino {2017)	Manipulación de programas o troyanos	Virus que afecta en forma negativa los equipos de los usuarios, su principal objetivo es brindar acceso a la persona que se encuentra a cargo del fraude, otorgándole autoridad para ejecutar administraciones remotas no autorizadas en los servidores intervenidos.
Harb y Echeverría {2015)	Técnica del Salami	Se basa en la sustracción de pequeñas proporciones de dinero de cuentas bancarias determinadas, a través de programas diseñados con instrucciones específicas para remitir los recursos obtenidos a la cuenta del infractor.
Acosta {2012)	Sabotaje informático	Funciona bajo técnicas como virus informáticos y malware, los cuales facilitan la modificación y borrado de datos en los sistemas informáticos, dificultando su normal desempeño.
	Espionaje y hurto informático (data leakage)	Es la divulgación de datos reservados de forma no autorizada, generalmente de empresas; y la reproducción no autorizada de programas informáticos de protección legal, ocasionando pérdidas económicas significativas para los verdaderos propietarios.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Autor	Modalidad	Concepto
Sánchez {2017) Villalva (2011)	Robo de servicios	Constituye un delito cibernético cuya finalidad provocar daños patrimoniales.
	Hurto de tiempo del computador	Se trata de ceder claves usadas por funcionarios de empresas determinadas a otras personas que no tienen autorización para usarlas
	Scavenging	Apropiación de información residual o basura que busca obtener información desprotegida en los sistemas informáticos después de haberse llevado a cabo un trabajo
	Parasitismo informático (Piggybacking)	Basado en la suplantación de personas o nombres, adquiere datos personales privados para emplearlos en función de prácticas delictivas
Jaramillo {2012)	Puertas falsas (Trap doors)	Producen interrupciones en el curso normal de los programas en el sistema, con la finalidad de lograr accesos directos evitando la aparición de medidas de seguridad
	Llaves maestras (Superzapping),	Mecanismo capaz de abrir diversos archivos almacenados en computadores, sin importar que tan protegido se encuentre.
	Pinchado de líneas (Wiretapping)	Es la interferencia de líneas telefónica s para capturar la información que estas suministran por medio de un radio, módem e impresora
	Piratas informáticos o hackers	Personas que se apropian de datos personales, contraseñas, códigos, y demás contenidos virtuales para lucrarse, producto de las deficiencias halladas en las medidas de seguridad informática.
Monsalve {2018):	Ingeniería social	Es una práctica antigua utilizada con intenciones persuasivas derivadas de la psicología, aprovechándose de las emociones de las personas y situaciones donde éstas puedan reaccionar de forma predecible y, de este modo, lograr accesos a sistemas de datos e indagar en aspectos personales privados, que puedan llegar a ser utilizados en contra de las víctimas
Urueña {2015)		Observación, recuperación de contraseñas, uso del teléfono, cartas, fax o chats con requerimientos de información de las víctimas que pueda serle útil al individuo que comete el fraude, suplantación de identidad conocido como phishing, chantaje o extorsión, y posteriormente presión psicológica.

Fuente: Elaboración propia (2019)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

En Colombia las instituciones públicas y privadas han establecido una interconexión en el espacio virtual, al respecto Camacho y Amaya (2013) afirman que las mismas buscan realizar mejoras electrónicas, no obstante, han surgido inconvenientes relacionados en su mayoría con temas de seguridad informática, dando lugar a delitos electrónicos donde se afectan principalmente la estabilidad y funcionamiento del país.

La suplantación de identidad (Phishing) y sus causas principales

Para Sarikaa & Varghese (2017, p.3274) “el phishing es un ataque de ingeniería social para adquirir y utilizar ilegalmente los datos de otra persona en nombre de un sitio web legítimo para beneficio financiero o personal”. Fraude ejecutado por un phisher, nombre adoptado por la persona que comete el engaño, a través del uso de correos electrónicos con contenidos aparentemente provenientes de entidades e instituciones reconocidas, llamando la atención del usuario para proporcionar datos confidenciales, posteriormente usados con intenciones fraudulentas. La palabra phishing se deriva del término fishing en inglés, tiene como significado pescar, dicha práctica ilegal se enfoca principalmente en atrapar a sus víctimas (López, 2019).

Los servicios más utilizados por los phishers interesados en suplantar identidades están direccionados a los bancos, con el propósito de adquirir claves secretas o números de tarjetas de crédito; a las redes sociales como facebook, twitter, instagram, linkedln, entre otros, para conseguir cuentas de usuarios y datos personales; al comercio electrónico en páginas como Amazon, eBay, entre otras; a los servicios de almacenamiento en la nube, servicios a empresas públicas (Paesani y Stucher, 2017).

Dadas las anteriores definiciones, el phishing cuenta con algunos tipos de estrategias engañosas, descritas como: ataques al servidor, donde alteran los sistemas de nombres de dominio (DNS) de páginas web, suplantando portales de marcas o empresas reconocidas, así, cuando el usuario digite la dirección correcta de la página, es conducido a un sitio web falso con características idénticas al original. URLs falsas, fundamentadas en la creación de direcciones web extensas para confundir el usuario, por lo tanto, a simple vista, el link al cual va a ingresar es seguro y confiable, sin embargo, es una URL falsificada. Formularios html (lenguaje de marcas de hipertexto), usados para enviar correos electrónicos errados, donde usuarios inocentes, ingresan información allí requerida que luego se encuentra a disposición del defraudador.

Adicionalmente, Pecoy (2011) presenta dentro de las formas de phishing tres clasificaciones: Copia idéntica de un sitio web, modificaciones de sitios originales con características similares, dando lugar a páginas virtuales incorrectas al momento de acceder a ellas. Spoofing, basado en cambios de los nombres de dominio de sitios web, normalmente los cambios comprenden reemplazos de letras por números, por ejemplo, la letra o es sustituida por el número 0. Lavado de dinero, dirigido por empresas ficticias al ofrecer la posibilidad de trabajar desde casa generando altos ingresos, convirtiendo en víctima a quién acepta las ofertas de empleo, ya que al momento de recibir los pagos se solicitan datos sensibles, produciendo efectos desfavorables.

Por otra parte, el spear phishing de acuerdo a lo expuesto por Rodríguez (s.f), una de las amenazas orientadas a sacar provecho de clientes que utilizan los servicios de entidades bancarias y usualmente realizan actividades electrónicas como pagos en línea. Gómez (como se citó en Guerrero y Castillo, 2017) asevera el phishing como una de las mayores preocupaciones en el sector bancario colombiano; en consecuencia, las entidades financieras se han visto en la obligación de invertir sumas de dinero considerables para contrarrestar sus efectos, utilizando métodos de prevención, detección y eliminación del mismo. A ello debe sumarse la educación continua a sus clientes como es el caso de la Pymes.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Asimismo, Pons (2017), expone entre las causas principales del phishing, el constante aumento y desarrollo de las tecnologías informáticas, así mismo, el desconocimiento por parte de la sociedad en general acerca de prácticas fraudulentas como esta, que invaden a diario el ciberespacio, produciendo alta vulnerabilidad y deficiencia en conocimientos sobre medidas de protección individual, de las cuales necesariamente se debe tener información al momento de manejar cuentas de correo electrónico, navegadores de internet, sitios web y otro tipo de servicios relacionados con la implementación de medios digitales.

Finalmente, se destacan los aportes de Noreña y Calderón (2018) quienes indican que las causas fundamentales en las credenciales de correos electrónicos y redes sociales son los enlaces provenientes de los phishers con nombres de marcas o empresas prestigiosas, enlaces maliciosos aparentemente confiables con características fraudulentas, correos/spam con contenidos engañosos, administraciones de servicios web de forma inadecuada y aplicaciones erróneas instaladas en los Pc´s de los usuarios.

Resultados

Una vez aplicada la encuesta a través de medios electrónicos a 250 clientes Pymes de un banco de la ciudad de Medellín, se agruparon los resultados obtenidos en tablas por dimensiones de acuerdo con los objetivos planteados, y la asociación de las variables a estudiar: programas de educación financiera, fraude electrónico.

Tabla 1.
Resultados por Dimensión y Asociación

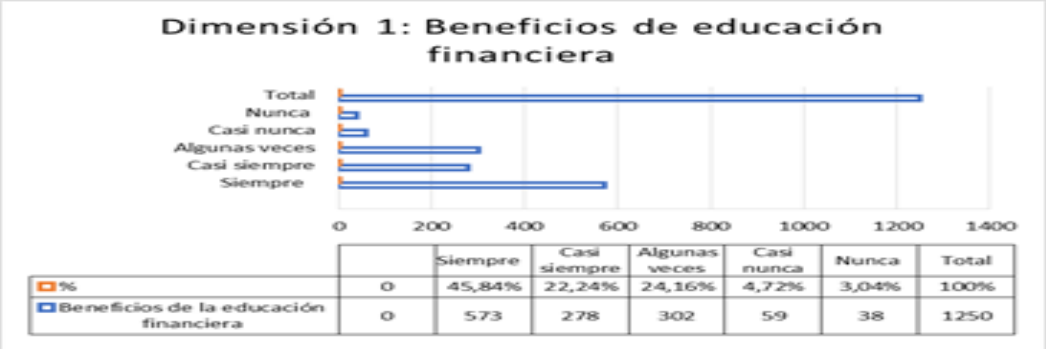
Opciones de respuesta	Resultados por Dimensión y Asociación									
	Beneficios de la educación financiera		Principios de programas financieros		Asociativas: Programas de educación financiera y fraude electrónico		Modalidades de fraude electrónico		Causas del Phishing	
	5 ítems	(%)	4 ítems	(%)	3 ítems	(%)	4 ítems	(%)	4 ítems	(%)
Siempre	573	45,84%	223	22,3%	345	46%	247	24,7%	55	5,5%
Casi siempre	278	22,24%	95	9,5%	173	23,06%	404	40,4%	238	23,8%
Algunas veces	302	24,16%	135	13,5%	149	19,9%	139	13,9%	41	4,1%
Casi nunca	59	4,72%	322	32,2%	83	11,06%	67	6,7%	552	55,2%
Nunca	38	3,04%	225	22,5%			143	14,3%	114	11,4%
Total	**1250**	**100%**	**1000**	**100%**	**750**	**100%**	**1000**	**100%**	**1000**	**100%**

Fuente: Elaboración propia.

En la tabla anterior se presentan los resultados referidos a las 5 dimensiones estudiadas sobre la educación financiera: beneficios, principios de los programas financieros, programas, modalidades de fraude y cusas del fraude electrónico, se muestran los porcentajes obtenidos para la escala de frecuencia: siempre, casi siempre, algunas veces, casi nunca y nunca, en cada una de las dimensiones. A continuación se presenta en detalle el análisis de los datos relacionados para cada dimensión.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Tabla 2.
Dimensión 1: Beneficios de educación financiera.



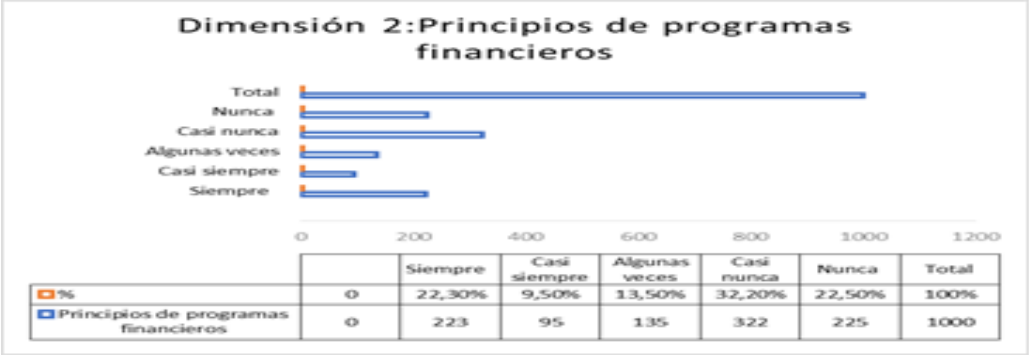
		Siempre	Casi siempre	Algunas veces	Casi nunca	Nunca	Total
%	0	45,84%	22,24%	24,16%	4,72%	3,04%	100%
Beneficios de la educación financiera	0	573	278	302	59	38	1250

Fuente: Elaboración propia

Al realizar el análisis de los datos acerca de la primera dimensión, referida a beneficios de educación financiera, se puede apreciar en las tablas 1 y 2, el 45.84% y el 22.24% de los clientes, indican su entidad financiera siempre o casi siempre, respectivamente, realiza esfuerzos para identificar sus necesidades de información; además señalan los programas y la educación financiera ayudan a mantener seguridad y equilibrio en las operaciones bancarias, contribuyendo al desarrollo de habilidades para hacer frente a riesgos financieros; ello refleja lo planteado por Grifoni & Messy (2012), cuando proponen a las orientaciones financieras como un componente esencial para el mundo de la banca.

Por otro lado, el 24.16% señala la información proporcionada por el banco, solo algunas veces, les permite tomar mejores decisiones financieras, dentro del mismo porcentaje se ubican clientes que informaron, dicha institución ofrece programas de educación financiera con la misma frecuencia señalada; por su parte el 4.72% y el 3.04% revelan casi nunca y nunca reciben información útil con este fin, es decir, resultados donde se demuestra, los entes bancarios deberían incrementar la oferta de estos programas, para orientar y beneficiar a su público, más aún al sector Pyme considerado como sector emergente para la economía colombiana, requiriendo para ello del apoyo del estado e instituciones privadas.

Tabla 3.
Dimensión 2: Principios de programas financieros



		Siempre	Casi siempre	Algunas veces	Casi nunca	Nunca	Total
%	0	22,30%	9,50%	13,50%	32,20%	22,50%	100%
Principios de programas financieros	0	223	95	135	322	225	1000

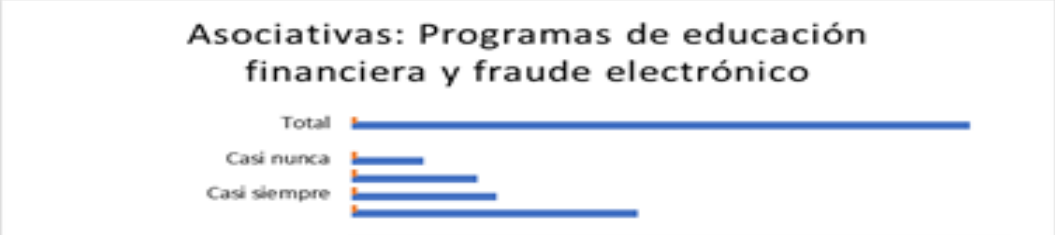
Fuente: Elaboración propia.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

En la tabla 3 se presentan los resultados referentes a la segunda dimensión, donde se muestra tanto el 32.20% como el 22.50% de los encuestados, coinciden en que la educación financiera promovida por su entidad casi nunca o nunca se presenta de forma imparcial, justa y clara, agrupando más del 50% de la población estudiada; en consecuencia, este tema se consideraría un aspecto prioritario a mejorar al interior del banco, pues dentro de los principios establecidos por la Comisión de la Comunidad Europea (2007), este aspecto tiene gran importancia, al contribuir con la sensibilización de los usuarios en relación al tema en cuestión.

Por su parte, el 22.30%, 9.50% y 13.50% de los usuarios manifiestan siempre, casi siempre o algunas veces, respectivamente, estarían interesados en que su entidad ofrezca programas de educación sobre aspectos básicos financieros; se podría señalar la existencia de poca sensibilización en relación al tema, a pesar de los planteamientos de Rojas (2006), pues señala, la educación financiera aporta beneficios a los clientes reflejados en el aprovechamiento de oportunidades de inversión y aplicación de medidas de prevención para hacer frente al fraude.

Tabla 4.
Asociativas: Programas de educación financiera y fraude electrónico



		Siempre	Casi siempre	Algunas veces	Casi nunca	Nunca	Total
%	0	46%	23,06%	19,90%	11,06%		100%
Asociativas: Programas de educación financiera y fraude electrónico	0	345	173	149	83		750

Fuente: Elaboración propia.

Con la finalidad de conocer la percepción del público encuestado frente a este tipo de iniciativas de interés social implementadas por la banca, asociadas a temas financieros, se establecieron afirmaciones que conectaron las dos variables de la investigación, de las cuales se obtuvo (Ver Tabla 4), tanto el 46% como el 23.06% de los clientes consideran los programas de educación financiera siempre o casi siempre, son un medio viable para evitar ser víctima de fraude electrónico. Es significativo como se incrementa la valoración en esta consulta en relación a la anterior, los usuarios Pymes muestran menor interés por recibir este tipo de información, pero incrementa su percepción favorable ante los beneficios aportados.

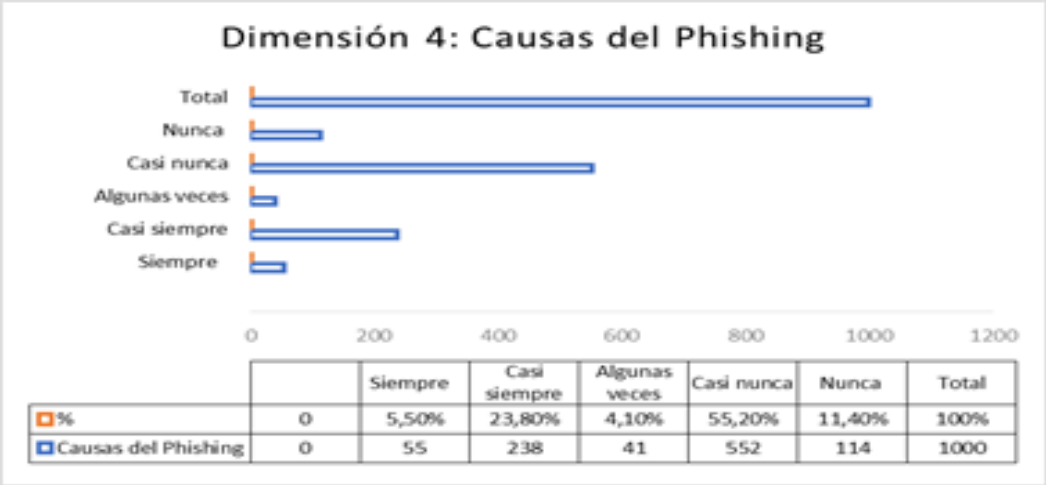
Según lo anterior, resulta importante que los bancos lleven a cabo programas de sensibilización orientado a la prevención de dicha problemática, haciendo posible desarrollar habilidades las cuales conduzcan a la fácil identificación de riesgos, logrando mitigar sus efectos por medio del uso de medidas de protección aplicables a estos escenarios.

Asimismo, con base a los datos analizados, el 19.90% y el 11.06% de los clientes indican que la prevención de fraude electrónico, algunas veces o casi nunca, forma parte de las

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

instrucciones ofrecidas por la entidad bancaria. Estas cifras igualmente deben ser consideradas y evitar su incrementa, tal como lo menciona Camacho y Amaya (2013), el sector empresarial colombiano en el ámbito financiero, al mantener una relación directa con los medios electrónicos, se ha visto afectado principalmente por delitos informáticos, desfavoreciendo el crecimiento, equilibrio de la economía del país.

Tabla 6.
Dimensión 4. Causas del Phishing



		Siempre	Casi siempre	Algunas veces	Casi nunca	Nunca	Total
%	0	5,50%	23,80%	4,10%	55,20%	11,40%	100%
Causas del Phishing	0	55	238	41	552	114	1000

Fuente: Elaboración propia.

En la tabla 6, se puede comprobar que el 23.80% y el 5.50% de los clientes Pymes del banco, casi siempre o siempre han brindado información personal, número de cuentas, tarjetas o claves cuando reciben correos electrónicos provenientes de su institución solicitándoles ingresar a un link; motivo por cual se reafirma la importancia de reforzar los programas de educación financiera; el 55.20% y el 11.40% indican casi nunca o nunca lo hacen.

Dentro del mismo hallazgo, se sitúan los que no conocen las recomendaciones de seguridad brindadas por los entes financieros, con el fin de disminuir la exposición al riesgo frente a fraudes virtuales. Resultados orientados a la gestión educativa con interés social de la entidad bancaria hacia las Pymes; aquí es pertinente recordar a Pons (2017) quien menciona dentro de las causas de la suplantación de identidad (phishing) la falta de información acerca de métodos de protección personales, esenciales en el manejo de operaciones relacionadas con sistemas electrónicos.

Conclusiones

La investigación es concluyente al afirmar por sus resultados que los programas de educación financiera permitirán el progreso y bienestar de la sociedad. Los consumidores financieros Pymes muestran interés por participar y beneficiarse de estos planes, los cuales además de múltiples ventajas otorgadas a quienes los reciben, dinamizan los mercados financieros, haciendo más efectiva la realización de inversiones y operaciones bancarias. Es

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

necesario entonces, por parte de las entidades del sector, aumentar considerablemente la gestión, frecuencia para ofrecer a sus clientes estos programas.

Existe la necesidad que las instituciones financieras atiendan en la gestión, planeación y aplicación de los programas, los principios básicos propuestos por la Comisión de la Comunidad Europea (2007), dada la demostración de algunas iniciativas propuestas por estas no están acorde a los mismos. Se debe tener en cuenta aspectos como satisfacción de necesidades de los clientes, imparcialidad de la información, evaluación constante del personal encargado de instruir a los clientes sobre herramientas para prevenir riesgos.

Se evidenció además la importancia, tanto el sector financiero como los entes que lo componen, complementen las orientaciones en finanzas, brindadas a sus Pymes con mensajes dirigidos a la prevención de fraude electrónico, considerando la identificación del desconocimiento con relación al phishing. Es responsable socialmente explicar a estos usuarios sobre las diferentes modalidades existentes, tratando particularmente aquellas donde se afecta de manera constante la ejecución de transacciones y demás acciones virtuales.

Los programas emitidos por entidades bancarias están enfocados en proporcionar información financiera, apuntando a las finanzas personales, toma de decisiones responsables al momento de invertir, entre otros, sin embargo, de acuerdo a los clientes Pymes consultados, no se brinda esta información como parte de programas integrales dirigidos a sensibilizar a su público en relación a los fraudes electrónicos.

Referencias Bibliográficas

Acevedo, A. (2018). *Panorama del Cibercrimen en Colombia*. Colombia Digital. (2018). Recuperado de https://colombiadigital.net/actualidad/analisis/item/10103-panorama-del-cibercrimen-en-colombia.html

Acosta, B. (2012). *Los delitos informáticos y su perjuicio en la sociedad.* Tesis de pregrado. Unidad Académica de Ciencias Administrativas y Humanísticas. UTC. Latacunga.

Acurio Del Pino, S. (s.f.). *Delitos informáticos: generalidades*. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Banco de Desarrollo de América Latina-CAF (2013). *La educación financiera en América Latina y el Caribe. Situación actual y perspectivas* (N° 12). Recuperado de http://scioteca.caf.com/bitstream/handle/123456789/379/caf_12_educaci_n_financiera5.pdf?sequence=1&isAllowed=y

Bonett, D., Wright, T. (2015). *Cronbach´s alpha reliability: Interval estimation, hypothesis testing, and sample size planning*. Journal of Organizational Behavior 36, 3-15. Doi: 10.1002/job.1960

Camacho, R. y Amaya, A. (2013*). Ciberseguridad y Ciberdefensa en Colombia*. Recuperado http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/00001172.pdf?sequence=1

Caridad, M., Cardeño E. y Ramírez, W. (2018). *Marketing hiperconectado fundamentado en la usabilidad de las tecnologías de la información y comunicación en las pymes*. Capítulo 9. pp. 235-259. En Rincón, Y., Restrepo, J. y Vanegas, J.G. (Coords.). (2018). Estudios de

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Comunicación y Marketing. pp. 330. Medellín, Colombia. Sello Editorial Publicar-T. Tecnológico de Antioquia, Institución Universitaria.

Comisión de la Comunidad Europea. (2007). *Comunicación de la comisión la educación financiera.* Bruselas. Recuperado de

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0808:FIN:ES:PDF

Departamento Administrativo Nacional de Estadística (Dane, 2018). *Estadística por temas*. Recuperado de https://www.dane.gov.co/index.php/estadisticas-por-tema

Díaz, A. y Luna, A. (2014). *Metodología de la Investigación Educativa*. Tlaxcala, México: Editorial Díaz de Santos. Recuperado de https://books.google.com.co/books?isbn=8490520232

El Tiempo (2017). https://www.eltiempo.com

Fernández, A. S., Martel, Y. B., Príncep, M. B., I. Blanch, J. P., & Monfort, N. G. (2015). *La educación financiera: un contenido hasta ahora invisible que ha irrumpido en el currículum de Ciencias Sociales*. En A. Hernández, C. García, J. Montaña (Eds.). Una enseñanza de las ciencias sociales para el futuro: recursos para trabajar la invisibilidad de personas, lugares y temáticas (pp.593-600). Cáceres, España: C/ Caldereros.

Fondo de Garantías de Instituciones Financieras – Fogafín (2011). *El rol de la educación económica y financiera en el Sistema Educativo Colombiano*. II Taller Internacional de Educación Económica y Financiera 2011. Recuperado de https://www.fogafin.gov.co/web/imagenes/file/Noticias/II%20TALLER%20EEF/2_%20Maria%20Mercedes%20Cuellar%20%20El%20rol%20de%20la%20educaci%C3%B3n%20econ%C3%B3mica%20y%20financiera%20en%20el%20Sistema%20Educativo%20Colombiano.Pdf

Fuentes, T., Mazún, R. & Cancino, G. (2017). *Perspectiva sobre los delitos informáticos: un punto de vista de estudiantes del Tecnológico Superior Progreso*. Advancesin Engineering and Innovation. 2(4), 1-8. Recuperado de http://www.itsprogreso.edu.mx/revistaAEI/index.php/aei/article/view/17

Grifoni, A. & Messy, F. (2012). *Current Status of National Strategies for Financial Education: A Comparative Analysis and Relevant Practices*. OECD Working Papers on Finance, Insurance and Private Pensions No. 16. Publicaciones de la OCDE, Paris. https://doi.org/10.1787/5k9bcwct7xmn-en

Guerrero Lozano, B. y Castillo Caicedo, D. (2017). *Desafíos técnicos y jurídicos frente al ciberdelito en el sector bancario colombiano*. Colombia. Recuperado de https://repository.unad.edu.co/handle/10596/13387

Harb, J. y Echeverría, G. (2015). *Los delitos informáticos y el derecho constitucional a la seguridad pública*. Tesis de pregrado. Repositorio Universidad Técnica de Ambato.

Jaramillo, F. (2012). *Delitos informáticos prevención modificación y creación de nuevos tipos penales.* Facultad de Derecho y Ciencias Políticas e Internacionales. UPAC. 118 p.

kaspersky (2017). *La República (Colombia): Inseguridad y poco acceso tienen rezagada a la banca móvil.* https://latam.kaspersky.com/

Lembert, P. y García, G. (2015). 1*,2,3 educación financiera para niños y jóvenes*. LID. México. Recuperado de: https://books.google.com.co/books?isbn=6079380196

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

López, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing.* Tesis de Maestría. Universitat Oberta de Catalunya.

Lucena, M. y Repullo, R. (2013). *Ensayos sobre economía y política económica: homenaje a Julio Segura*. España: Antoni Bosch editor, S.A. Recuperado de: https://books.google.com.co/books?hl=es&lr=&id=WBYLFUdrdpUC&oi=fnd&pg=PA433&dq=educaci%C3%B3n+financiera+imparcial&ots=dPkmggmCp4&sig=3s1da72QJUYNon2wPoXRtgS7Xh8#v=onepage&q&f=false

Monsalve, J. (2018). *Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos) 1-10*. Especialización en Seguridad Informática. Universidad Piloto de Colombia

Noreña Cardona, P. y Calderón Restrepo, S. (2018). *Técnica de protección para credenciales de autenticación en redes sociales y correo electrónico ante ataques phishing.* Revista Especializada en Ingeniería, 12 (2), 24-34. Doi: https://doi.org/10.22490/25394088.2960.

Organización para la Cooperación y el Desarrollo Económico (OCDE, 2019). https://www.oecd.org/

Paesani, M. y Stucher, V. (2017). *Ingeniería social, el arte de engañar* (Tesis de grado en Ingeniería de Sistemas. Universidad de la Defensa Nacional

Pecoy, M. (2011). *Delito en el Comercio Electrónico*. Prisma Jurídico, 10 (1), 209- 224. doi: 10.5585/PrismaJ.v10i1.2865

Pons Gamón, V. (2017). *Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad*. Revista Latinoamericana de Estudios de Seguridad, (20),80-93. http://dx.doi.org/https://doi.org/10.17141/urvio.20.2017.2563

Portafolio (2017). *¿Sabe usted qué es el "phishing", el delito cibernético más común del país?*. Recuperado de https://www.portafolio.co/mis-finanzas/que-es-el-phishing-delito-informatico-503702

Revista Semana. (2017). *El cibercrimen en 2017: la amenaza crece sobre Colombia*. Recuperado de https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

Romeo, C. (2007). *De los delitos informáticos al cibercrimen*. Salamanca. España. Recuperado de:

https://books.google.com.co/books?id=ikq7AwAAQBAJ&pg=PA655&dq=el+cibercrimen&hl=es419&sa=X&ved=0ahUKEwjF5Sp5JvhAhXy01kKHQ7wBJkQ6AEINTAD#v=onepage&q=el%20cibercrimen&f=false

Rodríguez, F. (s.f). *Nuevos delitos informáticos: Phishing, Pharming, Hacking y Cracking*. Recuperado de http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

Rojas, L. (2006). *El acceso a los servicios bancarios en América Latina: Identificación de obstáculos y recomendaciones*. Center for Global Development, Washington DC.

Sánchez Castillo, Z (2017). *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia*. Recuperado de: https://repository.unad.edu.co/handle/10596/11943

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020

Sarikaa, S. & Paul, V. (2017). *Parallel phishing attack recognition using software agents. Journal of Intelligence & Fuzzy Systems* 32(5), 3273-3284. https://tdeabasesdedatosezproxy.com:2128/10.3233/JIFS-169270

Urueña Centeno, F. (2015). *Ciberataques, la mayor amenaza actual*. Instituto Español de Estudios Estratégicos. Recuperado de https://aurelioherrero.blogs.upv.es/files/2015/02/DIEEEO09-015 AmenazaCiberataques Fco.Uruena. pdf

Villalva, D. (2011). *La inexistencia de la tipificación de los delitos informáticos en la ley de comercio electrónico, firmas y mensajes de datos vulneran al derecho de propiedad* (Tesis de grado en derecho). Universidad Técnica de Ambato.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen Único – Año 2020