UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

Medidas de seguridad y acceso a la información personal en usuarios de Banca Electrónica

¿Qué medidas de seguridad aplican, los usuarios del sistema banca electrónica en Costa Rica, para realizar transacciones en Internet?

Francisco Alas Ortega

08/04/2011

RESUMEN

Realizar transacciones bancarias por medio de Internet resulta cada vez más interesante tanto para los bancos como para sus clientes, gracias a las facilidades y ventajas que el sistema bancario en línea ofrece. Aunque los usuarios ingresan desde la comodidad de sus hogares u oficinas, siempre deben tener en cuenta factores de seguridad que les permita llevar a cabo su transacción de la forma más segura y sin exponerse a ser víctimas de los delincuentes de la web. Este estudio tiene como propósito proveer información general sobre las medidas de seguridad que deben tomar en cuenta los clientes al hacer uso de los servicios de banca por Internet. La investigación gira en torno a conocer el comportamiento de los usuarios frente al uso de estos servicios en línea, con base en estadísticas realizadas en estudios anteriores por organizaciones como PayPal y BitDefeder, consejos y medidas de seguridad que las entidades bancarias ofrecen a sus clientes en sus sitios web y la situación actual que se vive en Costa Rica referente al tema.

Al hablar de seguridad bancaria en línea no sólo se hace referencia a las precauciones por parte de las entidades financieras, sino también al compromiso que adquiere el usuario como dueño de los datos que ingresa en los portales bancarios. Con el fin de divulgar la percepción que tienen los clientes de banca en línea ante el peligro latente en Internet y en qué forma buscan contrarrestar el riesgo al hacer uso de estos servicios es que se realiza la presente investigación. El estudio es aplicado a una muestra de la población de Costa Rica, el mismo revela el comportamiento y el nivel de riesgo que presentan los usuarios en nuestro país frente al peligro existente en la banca electrónica por Internet.

ABSTRACT

Internet banking allows customers to conduct financial transactions on a secure website operated by their retail. Online banking solutions have many features and capabilities. “Home banking users” entering the system from the comfort of their homes or offices must always consider safety factors to enable them to carry out their transactions in the most safe way and without exposing themselves to being victims of criminals to the web. This study is intended to provide general information on safety measures to be taken into account by customers to make use of Internet banking services. The research focuses on understanding the behavior of users over the use of these online services, statistics are based on previous studies by organizations such as PayPal and BitDefeder, advice and security measures that banks offer their customers in their web sites and the current situation that exists in Costa Rica on the topic.

Speaking of online banking security not only refers to the precautions on the part of financial institutions, but also the commitment that takes the user as the owner of the data entered in the bank portals. To spread the perception of online banking customers to the potential danger on the Internet and how they seek to balance the risk to make use of these services is that this research is done. The study is applied to a sample of the population of Costa Rica, it reveals the behavior and the level of risk posed by users in our country of the danger with existing electronic banking on the Internet.

INTRODUCCIÓN

Actualmente el acceso a la banca electrónica en línea es uno de los servicios que ofrecen los bancos a nivel mundial, y cada día más personas hacen uso de este servicio para realizar diferentes tipos de transacciones, tales como: consulta de saldos y movimientos, ejecutar pagos, llevar a cabo transferencias de dinero, y pago de tarjetas. Estas transacciones pueden ser realizadas desde cualquier lugar en donde se encuentre el usuario, ya sea casa, oficina u otro sitio donde tenga acceso a Internet. El número de usuarios ha crecido considerablemente; actualmente en Costa Rica se realizan más de 130 mil transacciones diarias, tomando en cuenta los diferentes bancos que operan en el país. (Melagatti C., 2010).

Con el surgimiento de la globalización y la modernización, las empresas han visto la necesidad de innovar e implementar medidas para brindar un servicio de mejor calidad a sus clientes. Entre las organizaciones que han fomentado mayor afluencia a la investigación y el desarrollo se encuentran las entidades bancarias. Esto debido a la época en que nos encontramos, en la cual se mueven grandes cantidades de dinero, por lo que la prevención de fraudes hacia sus clientes es fundamental. La seguridad en el sector financiero siempre ha representado una gran preocupación para los bancos (Cuadra C., 2010), es por ello que constantemente están implementando nuevas tecnologías y técnicas para brindar mayor seguridad a sus clientes, los usuarios de los servicios de banca en línea. La población costarricense ocupa uno de los puestos más altos entre los países en desarrollo en cuanto al uso diario de los servicios bancarios por Internet. Así mismo el volumen de las transacciones electrónicas superan en gran medida las transacciones manuales, lo que evidencia la atracción de los usuarios por estos mecanismos, ya que la velocidad con que se viene incorporando la población mundial a las redes, y sobre todo a Internet, es extraordinaria. En los últimos años ha aumentado el volumen de las transacciones bancarias realizadas por Internet (Melagatti C., 2010).

Cuatro de cada diez personas, cuando necesitan realizar una gestión que involucra una alta cantidad de dinero, prefieren realizarla de forma personal directamente en la entidad bancaria. Y aunque en la actualidad los bancos disponen de medidas con un alto porcentaje de fiabilidad que garantizan la ausencia de intrusos, los usuarios constantemente reclaman mayor seguridad a las entidades bancarias, lamentablemente la mitad de estos no están dispuestos a tomar alguna medida de acción en el tema de manera personal. Aunque las diferentes entidades bancarias ponen a disposición de sus clientes en su sitio web, e incluso en boletines, una serie de consejos importantes a acatar al momento de realizar transacciones en Internet, muy pocos toman el tiempo para conocerlos y aún más para aplicarlos (CentiSur y D'Alessio IROL, 2010), ignorando que estas les pueden evitar pasar por una experiencia no muy agradable.

Internet crece en usuarios, servicios y funcionalidad, la banca electrónica en línea más que una moda es una necesidad, que se refleja tanto para los usuarios como para el banco mismo en reducción en los tiempos de atención, evita el desplazamiento físico, y produce reducción de costos en general. Las entidades bancarias podrán invertir y contar con las

mejores tecnologías en temas de seguridad para los usuarios de banca en línea, pero qué tanto estas tecnologías son aprovechadas por los usuarios para proteger sus datos al realizar una transacción es una de las incógnitas, por lo que se realiza la presente investigación. El banco no tiene forma de constatar la identidad del cliente si no es por sus credenciales (usuario y clave), las cuales están a cargo de cada uno sus clientes (CentiSur y D'Alessio IROL, 2010). El objetivo es conocer qué medidas de seguridad de las emitidas por la entidades bancarias son conocidas y además son tomadas en cuenta por los usuarios en Costa Rica al realizar sus transacciones en Internet, así como cuáles de éstas son ignoradas o desconocidas. La seguridad bancaria en Internet depende en un gran porcentaje del banco que ofrece el servicio, sin embargo el otro porcentaje está en las manos de los clientes como dueños de sus datos (Grupo Financiero Acobo, 2010).

ANTECEDENTES

Utilizar los servicios de banca por Internet es cada vez más común entre los costarricenses. La seguridad en el tema financiero en línea juega un papel muy importante. Por un lado, los bancos constantemente se están actualizando con tecnología y estrategias que les permiten brindar mecanismos que ayuden a sus clientes a hacer uso de sus servicios de manera confiable y segura; por otro lado, todo cliente que haga uso de la banca en línea debe asumir el compromiso en el tema de seguridad, ya que de ellos depende el correcto uso de sus credenciales de acceso al sitio de su banco (Banco de Costa Rica, 2011). Ante esta responsabilidad, ¿qué tanto se preocupa el usuario de proteger su información?, y ¿en qué grado es conocedor de las medidas de seguridad que se deben aplicar al momento de hacer uso de los diferentes servicios que los bancos ofrecen por Internet? Cada día se hace más frecuente escuchar de fraudes electrónicos, razón por la cual la prevención ante estos ataques es un tema fundamental tanto para la entidad bancaria como para el usuario mismo.

Los usuarios de banca electrónica en línea se consideran más informados que en años anteriores, lo que contribuye como un factor positivo en cuanto al aumento en los niveles de confianza en lo que a medidas de seguridad se refiere (Bit Defender, 2008). Según reflejan estudios realizados por la compañía Bit Defender en cuanto a seguridad bancaria, contra las preocupaciones de los usuarios, un 68% de los encuestados indica haber incrementado sus conocimientos en tema de seguridad, de manera que protegen más el acceso a sus cuentas y a su computadora personal, un 8% declara desconocimiento absoluto en el tema y un 24% señala contar con conocimientos básicos en asuntos de seguridad informática. De igual manera el estudio mencionado muestra las principales preocupaciones con que cuentan los usuarios de Internet:

- Ataques por virus (36%)
- Privacidad (20%)
- Ataques por Malware (15%)

- Ataques por Cibercriminales (8%)
- Ataques por Hackers (11%)
- Ataques por Phishing (4%)
- No les preocupa ningún tipo de ataque (2%)
- Otros (4%)

Por las facilidades que ofrecen los bancos al brindar sus servicios en línea, cada vez son más los clientes que hacen uso de ellos. Sin embargo la banca por Internet es objetivo de los hackers o ciberdelincuentes, es por ello que se debe actuar con responsabilidad y precaución en los momentos en que se realizan todo tipo de transacciones por medio de Internet. Otro estudio referente a este tema fue realizado en Europa por PayPal, donde muestra que un 19% de los usuarios tiene accesible, en su perfil de redes sociales, información sobre sus claves bancarias (EBanking News, 2008), un descuido que le puede costar muy caro a los usuarios. De igual manera el estudio revela que los usuarios no conocen formas seguras de crear claves, ya que un 15% hace uso de sus apellidos y fecha de nacimiento, un 14% usa como clave el nombre de su mascota, pareja u otro familiar. Lo que agrava aún más el tema de seguridad bancaria es que un 63% indica que cambian sus contraseñas menos de una vez al año o solo cuando el banco se los solicita (EBanking News, 2008). Descuidos como estos son aprovechados por los hackers o piratas cibernéticos para realizar sus estafas. Dentro del mismo estudio, PayPal indica que un 10% de los usuarios que comente este tipo de imprudencias han sido víctimas de robo de identidad. Factores tan sencillos como el de no contar con la misma clave en las diferentes cuentas bancarias o el estar actualizándolas constantemente, elegir contraseñas complejas que combinen letras, números y símbolos, el memorizarlas y no colocarlas a la vista de terceros, le permiten a los usuarios hacer uso de los servicios de Internet de forma segura tanto para banca como para comercio electrónico en general.

Ante los hechos, las entidades bancarias se han visto en la necesidad de implementar nuevas medidas de seguridad para sus sitios en Internet y realizar campañas de prevención y sensibilización para el buen uso de estos canales, a fin de evitar que sus clientes sean víctimas de los cibercriminales. Las técnicas más usadas como instrumentos de fraude son: el phishing, el troyano bancario y robo de identidad o robo de claves (Dirección de Investigación Criminal, 2010). El phishing básicamente consiste en obtener datos personales y bancarios por medio de correos electrónicos o páginas web falsas que suplantan la de una entidad bancaria (Banco HSBC, 2011). Los troyanos son pequeños programas que se instalan en la computadora sin consentimiento del dueño del equipo, con el fin de obtener datos personales y bancarios. Estos se ingresan, en su mayoría, de forma oculta al realizar descargas de software gratuito, fotos, música, videos y juegos. El robo de identidad y robo de claves, por lo general se realiza por medio del envío de correos de remitentes desconocidos, que por medio de la estrategia de ofrecer algún producto o regalía solicitan que el usuario ingrese sus datos personales (Panda Security, 2011).

El objetivo principal del estafador normalmente va a ser tener acceso a las cuentas bancarias o número de tarjeta de crédito de la posible víctima, para poder transferir dinero o hacer cargos de forma ilícita. Aunque las entidades bancarias publican en sus sitios web una serie de recomendaciones que le permiten al usuario enterarse de cuál es el proceso correcto para conectarse de manera segura y realizar sus transacciones, son muy pocos los usuarios que toman el tiempo para conocerlas (CentiSur yD'Alessio IROL, 2010). Los siguientes son una serie de consejos que los usuarios de banca en Internet deben tomar en cuenta al momento de visitar el sitio de su banco de preferencia, para navegar en la web sin comprometer su información personal y conservar un equipo de cómputo libre de intrusos (Scotiabank Costa Rica, 2011).

- Al ingresar a la página web del banco, el usuario debe digitar la dirección exacta en el navegador, debe evitar ingresar por medio de enlaces enviados por correo electrónico o enlaces ubicados en otras páginas de Internet.
- Antes de ingresar los datos (usuario y clave), el usuario siempre debe asegurarse de que la página del banco utiliza seguridad por medio de cifrado, en el explorador de Internet el usuario lo puede verificar por medio de la dirección del sitio que inicie con "https:" o con el ícono en forma del candado cerrado ubicado en la barra de estado del mismo explorador.
- Es recomendable que todo equipo de cómputo personal cuente con un software antivirus, antispyware, firewall y se mantengan debidamente configurados y actualizados.
- El usuario debe mantener el navegador de Internet con las últimas actualizaciones y parches de seguridad.
- Debe evitar instalar aplicaciones gratuitas de origen no confiable.
- El usuario no debe compartir sus claves con ninguna otra persona.
- Antes de ingresar al sitio web del banco, el usuario debe asegurarse de cerrar otras páginas en las que se encuentre navegando en ese momento.

Las entidades bancarias adoptan rápidamente nuevas tecnologías de seguridad, y se han dado cuenta de que los controles tradicionales (usuario y clave) ya no son suficientes para proteger a sus clientes. Es por ello que en busca de mejorar la seguridad han incursionado en tecnologías como el uso de dispositivos token, teclados virtuales, claves dinámicas, registro de cuentas favoritas y controles de montos máximos por transacción; todas estas son medidas implementadas por las entidades bancarias mismas. Los token y las claves dinámicas, a diferencia de los métodos convencionales de contraseñas, se basan en que el usuario es el único que posee el dispositivo, éste les permite generar claves únicas de forma sincronizada con otro generador de claves ubicado en la entidad bancaria. Las tecnologías y métodos de seguridad siempre están en constante avance con el objetivo de brindarle al usuario la suficiente protección, pero también al mismo ritmo se mueven las estrategias usadas para realizar estafas, es por eso que siempre se deben tomar todas las

precauciones del caso para evitar ser víctimas de los delincuentes informáticos (Deloitte, 2010).

Los clientes de la banca por Internet en Costa Rica, ante el conocimiento de diferentes experiencias expuestas por medio de periódicos y noticieros, se encuentran más alertas en los últimos años. Estadísticas presentadas por el Organismo de Investigación Judicial (OIJ) señalan que los fraudes relacionados con Banca Electrónica en Internet han presentado una disminución para el año 2010 con respecto al año anterior, ya que para el año 2009 se reportaron 493 casos de este tipo de delitos, mientras que para el periodo 2010 los delitos relacionados con este tema reportados fueron 214 (Organismo de Investigación Judicial, 2010). Asimismo "algunos directores de banca electrónica de varios bancos consultados, opinan que están utilizando sistemas muy seguros en informática" (Cordero C., 2001). Sin embargo, se manifiesta en el entorno bancario que al igual que con los cajeros automáticos u otros servicios, en Internet la seguridad depende en gran porcentaje de los clientes. Cada entidad ha establecido diferentes sistemas de seguridad para ingresar a las páginas, especialmente para realizar transacciones que requieren de procedimientos y claves, y si el cliente no se compromete a tomar las precauciones para asegurarse de la protección de sus datos, podría poner en peligro su dinero.

METODOLOGÍA

La investigación tiene un enfoque cuantitativo, los resultados son analizados a partir de encuestas aplicadas a la población de estudio, a fin de identificar los patrones de comportamiento de la muestra seleccionada. Ahora bien, es necesario lograr recolectar suficiente información para tener resultados coherentes y cohesivos en la investigación (Hernández, Fernández y Baptista, 1991). La recopilación de la información se da por medio de una encuesta a distribuir entre la población de estudio. La encuesta cuenta con respuestas estructuradas y previamente definidas según el objeto de estudio presentado.

Las preguntas de la encuesta son más generales con la idea de que apliquen a la mayor cantidad de personas, y no son tan profundas como la metodología de entrevistas en la investigación de tipo cualitativa. Este instrumento de recolección de información toma como referencia las tendencias que se especifican en los antecedentes de la investigación, con el fin de comparar los resultados nacionales con los obtenidos en estudios de diferentes países e investigaciones realizadas anteriormente con temas relacionados. El tipo de encuesta se centró en permitirle al encuestado escoger opciones dentro de una amplia gama, y de ser el caso, aportar sus propias respuestas para ciertas preguntas. El objetivo principal es hacer la encuesta de manera que el usuario de banca electrónica en línea se sienta identificado con los aspectos considerados en las diferentes preguntas y pueda dar una opinión valiosa para el estudio realizado.

La población de estudio está comprendida por personas que hacen uso de la banca electrónica en línea en Costa Rica, a fin de conocer a fondo qué medidas de seguridad son aplicadas por los usuarios del sistema banca electrónica al realizar transacciones en Internet, y cuáles de estas ignoran. Es necesario que se cuente con experiencia frecuente

en el uso de la herramienta en línea ofrecida por los diferentes bancos. Es deseable pero no imprescindible que los encuestados cuenten con cierto grado de educación que les permita reconocer los diferentes factores que se ponen en juego al realizar transacciones en línea. No existe ningún tipo de preferencia demográfica para la población encuestada, pero sí es deseable que sea lo más heterogénea posible, de manera tal que se logre llegar a resultados que muestren tendencias en el área para el tema investigado.

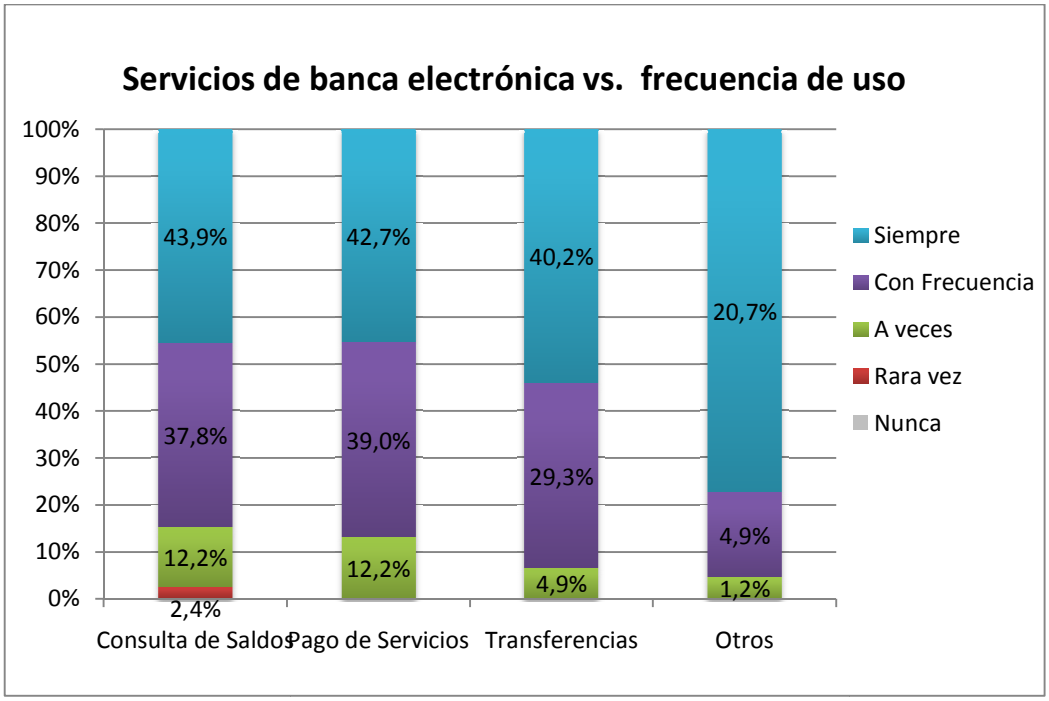
La encuesta fue creada con la herramienta en línea SurveyMonkey y divulgada por medio de un enlace (hipervínculo) enviado por medios electrónicos como correo y redes sociales. Si bien el número de usuarios de banca por Internet "actualmente supera los seiscientos mil clientes" (Melagatti C., 2010), la cantidad de personas a las que se contactó para colaborar con esta investigación fue de 100 usuarios de diferentes niveles educativos y profesiones que hacen uso del sistema bancario en línea. Se obtiene un total de 82 encuestas completadas. La muestra fue seleccionada por conveniencia debido a que los encuestados corresponden a personas con conocimientos en diferentes disciplinas, contactadas por medio de correo electrónico y la red social Facebook. El estudio presenta un nivel de confianza de un 95% y un margen de error de un 10,8% (Datum Internacional, 2011).

RESULTADOS DE LA INVESTIGACIÓN

Por medio de la encuesta se logran obtener resultados importantes sobre el comportamiento de la población de estudio, los cuales permiten conocer las medidas en seguridad que aplican los usuarios al ingresar sus datos personales en Internet para realizar transacciones a través de la banca electrónica en línea. El estudio revela que, cuando un cliente ingresa sus datos al sitio de la entidad financiera, un 53,6% tiene el cuidado de verificar que se cuente con cifrado de seguridad por medio del uso de "https://", un 49.9% valida que el sitio cuente con un certificado digital, y un 52,4% revisa que el sitio cuente con el símbolo del "*candado cerrado*", esto para constatar que es un sitio seguro. En contraste, un 19,5% no toma en cuenta ninguna de las consideraciones anteriores al momento de ingresar al sitio del banco por Internet.

En cuanto a los servicios que utilizan los clientes de banca electrónica en línea y la frecuencia de utilización de los mismos, el gráfico nº 1 muestra el comportamiento de los usuarios.

Gráfico Nº 1



Ante los cuidados que mantienen los usuarios en el uso de sus credenciales, la población encuestada revela una tendencia predominante con un 46,3% correspondiente a usuarios que no mantiene sus contraseñas escritas ni utilizan la misma en más de un sitio en Internet; no obstante se expresa que un 20,7% de los encuestados mantienen sus contraseñas escritas y también las usan en más de un sitio.

Tabla Nº 1

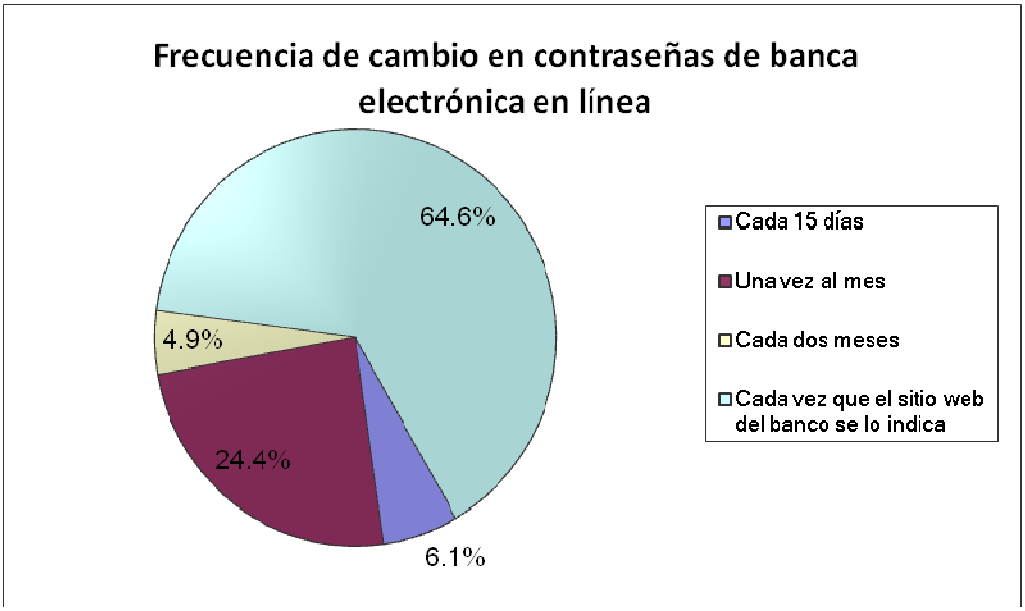
Claves escritas vs. uso de las mismas en más de un sitio en Internet

		Mantienen Contraseñas Escritas	
		Si	**No**
Misma Contraseña	**Si**	20,7%	17,1%
	No	15,9%	46,3%

El estudio indica que un 41,9% de las personas que mantienen escritas sus contraseñas también cuentan con un dispositivo token, clave dinámica u otro mecanismo que les ayudan a proteger sus datos al ingresar los portales bancarios. De estos usuarios, un 31,7% de los que no copian sus claves cuentan además con un dispositivo token o clave dinámica. El más alarmante de estos perfiles de usuarios corresponde al que se encuentra en el cuadrante del 21,95%, que escriben su clave, la usan en más de un sitio en Internet y no tienen ningún dispositivo adicional de seguridad como los mencionados anteriormente.

En cuanto al cambio de contraseñas, la población claramente muestra que la mayoría de los clientes lo hacen cada vez que el banco se los solicita.

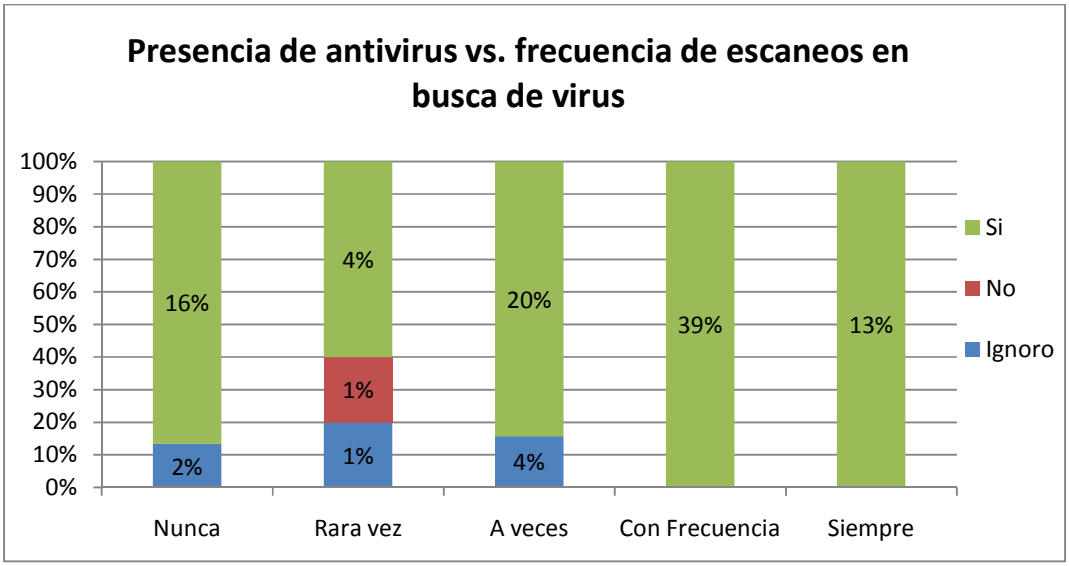
Gráfico Nº 2



Un 90,2% de los encuestados considera que las credenciales de usuario y contraseña son información confidencial, sin embargo existe un 9,8% que las comparte con un familiar o amigo de confianza.

Un 91,5% de la población encuestada indica que cuenta con antivirus actualizado en sus equipos de cómputo. De este porcentaje predomina que un 39% con frecuencia realiza escaneos que les permite detectar a tiempo un ataque de un virus que ponga en peligro su información personal, un 20% a veces y un 16% dice nunca realizar este tipo de tarea.

Gráfico Nº 3



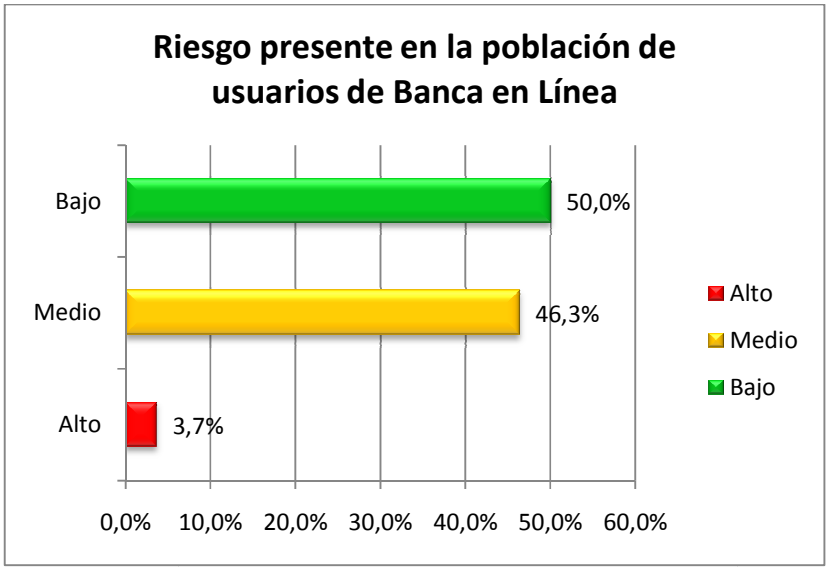
Como protección adicional, un 62,2% de los encuestados considera importante contar con el uso de firewall debidamente configurado a fin de que les proteja contra los intrusos en sus equipos de cómputo.

Tomando en cuenta variables como: cerrar todos los sitios de Internet antes de ingresar al portal bancario, abandonar el sitio haciendo uso de la opción “Finalizar Sesión”, el uso de contraseñas escritas, uso de contraseñas compartidas, no contar con un dispositivo token o clave dinámica como protección adicional, antivirus actualizado, uso de firewall y escaneos frecuentes en busca de virus, se realiza una matriz de riesgo con la cual se logra determinar el nivel de riesgo presente en la población de estudio.

Tabla Nº 2

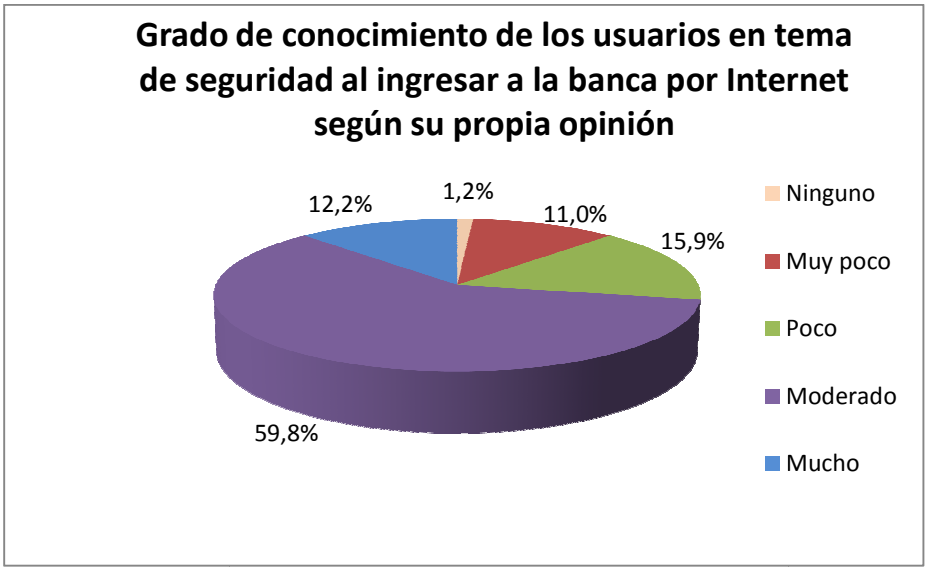
Riesgo usuarios de Banca en Línea		
Nivel de riesgo	**Porcentaje de riesgo usuarios de Banca en Línea**	**Número de encuestados**
Alto	3,7%	3
Medio	46,3%	38
Bajo	50,0%	41
	Total Encuestados	**82**

Gráfico Nº 4



Finalmente ante la pregunta de ¿Cuál es el grado de conocimiento de los encuestados en el tema de seguridad?, se obtiene los siguientes resultados:

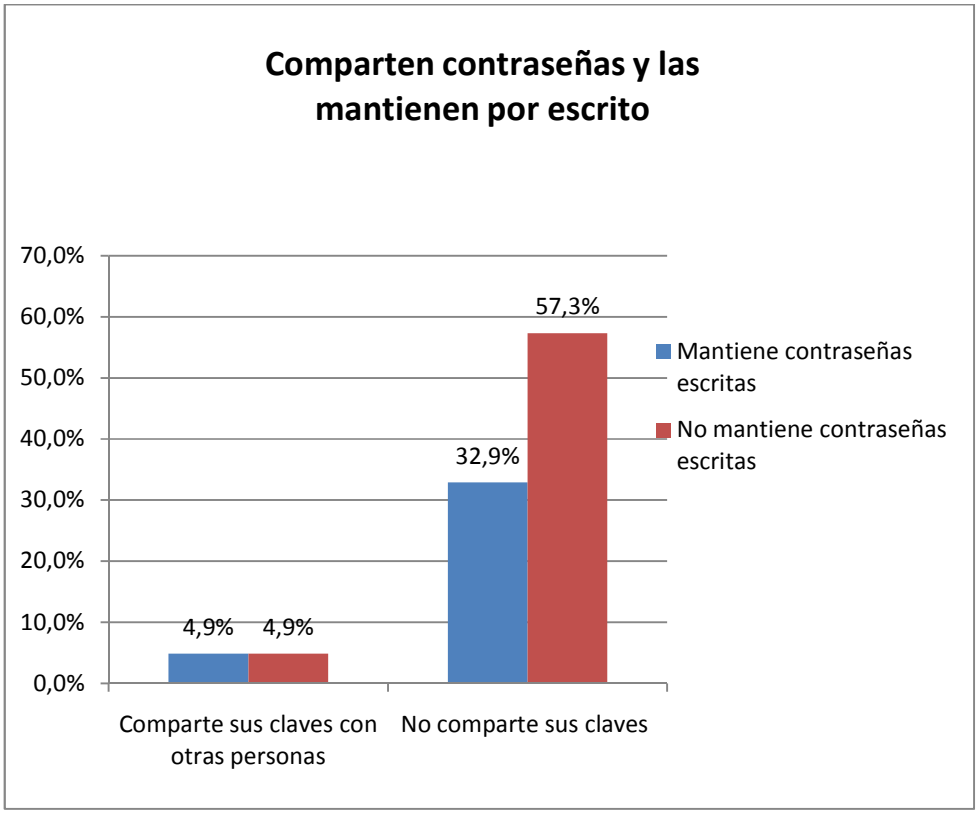
Gráfico Nº 5



DISCUSIÓN DE RESULTADOS

Según la información recopilada por medio de la encuesta, se logra identificar cuáles de las medidas de seguridad de banca electrónica en línea son tomadas en cuenta por los usuarios de estos servicios. La tendencia que se muestra en el gráfico nº 6 señala que un 57,3% de los usuarios de banca en línea no comparte ni usa por escrito las contraseñas, de manera que evitan exponerlas a terceros. El caso contrario lo indica el estudio realizado por PayPal, que muestra que un 19% no sólo las tiene por escrito, sino también las publica como parte de su perfil en las redes sociales (EBanking News, 2008).

Gráfico Nº 6



Según señala PayPal en su estudio realizado en Europa, un 63% de los encuestados realiza los cambios de sus contraseñas cada vez que el banco se los solicita (EBanking News, 2008). De igual manera los resultados de la investigación indican que los usuarios en Costa Rica siguen este mismo esquema de comportamiento, ya que como se observa en el gráfico Nº 7, un 64,6% de los encuestados menciona que realizan el cambio de clave cada vez que el banco se los solicita. Bajo esta conducta, si el equipo de cómputo de un cliente de banca electrónica es infectado por un tipo de virus troyano y éste obtiene información sobre las contraseñas, se puede suponer que el delincuente cuenta con suficiente tiempo para convertirlo en víctima de fraude.

El gráfico nº 7 realiza una comparación entre la presente investigación y el estudio realizado por PayPal en Europa, donde se evalúan factores como uso contraseñas y conocimientos en seguridad de banca en línea (EBanking News, 2008).

Gráfico Nº 7

Si bien es cierto las entidades bancarias ofrecen dispositivos OTP (One Time Password, "una clave a la vez") como los token y claves dinámicas que complementan la forma tradicional de ingreso a los portales bancarios, brindándole a sus clientes una mayor protección al realizar sus transacciones en Internet, el estudio muestra que un 53,7% de los encuestados no hace uso de este dispositivo, contra el 46.3% que sí. Este primer porcentaje de los clientes representan los que, en caso de sus claves sean conocidas por un tercero, se convierten en una presa fácil para consumar una estafa.

Los bancos publican en sus sitios web consejos que le permitan al cliente realizar transacciones de forma segura. Entre estos consejos se encuentra que el usuario, antes de ingresar los datos (usuario y clave), siempre debe asegurarse que la página del banco utilice seguridad por medio de cifrado, que el ícono del candado ubicado en la barra de estado del explorador se encuentre en estado cerrado. Sin embargo el estudio señala que solo un 53,6% de los usuarios encuestados verifica al ingresar sus datos que el sitio cuente con cifrado seguro, un 52,4% comprueba que el candado se encuentre en estado cerrado,

mientras un 19,5% ingresa sus datos sin revisar ninguna de estas opciones. Con esto, sumado a que un 11% de los encuestados también ingresan al sitio de su banco sin digitar la dirección directamente en el explorador de Internet, se potencializan como víctimas de phishing. Otro de los consejos que los bancos ofrecen es el de no compartir las claves con otras personas; de la población de estudio un 90,2% acatan esta solicitud, mientras que un 9,8% la comparten con un alguna otra persona.

Frente a precauciones como el cerrar otros sitios de Internet mientras se ingresa a la página del banco, un 32,9% de los encuestados asegura siempre hacerlo, mientras que un 22% señala nunca realizar esta práctica. De igual manera, en cuanto a hacer uso de la opción "*Finalizar Sesión*" antes de abandonar el sitio del banco (otro de los consejos de los bancos), se señala que un 87,7% hace uso de esta opción, mientras que una minoría de un 3,2% simplemente abandona el sitio sin finalizar sesión, poniendo en peligro su información.

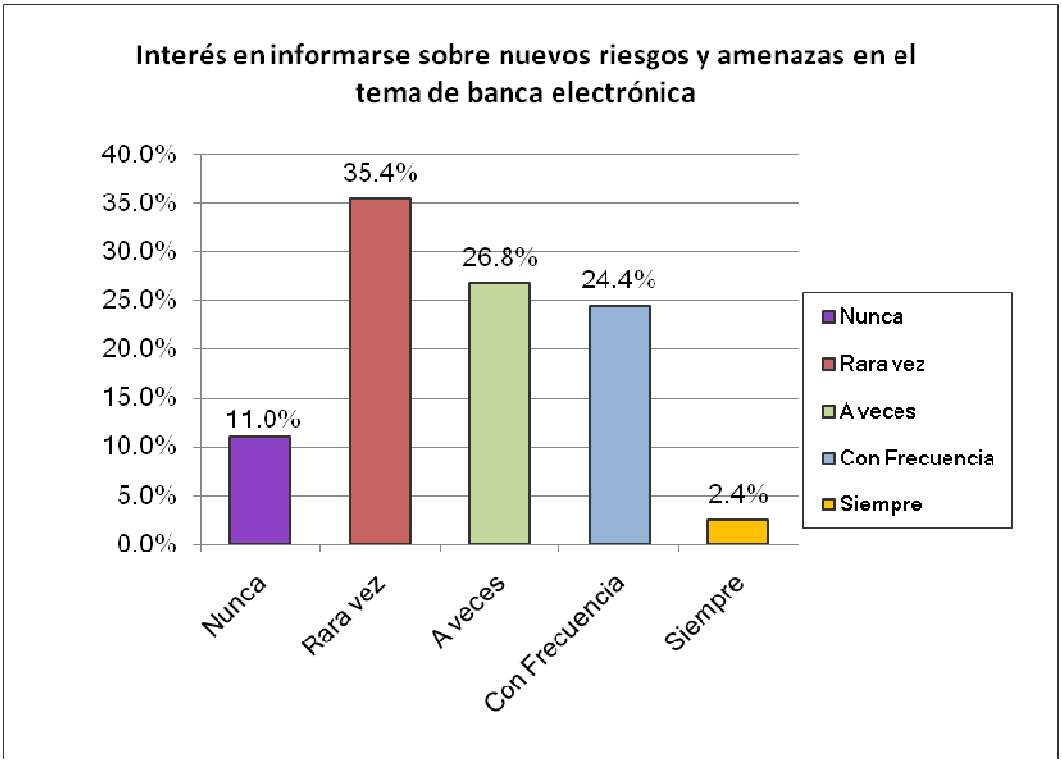
Ante la recomendación realizada por las entidades financieras de que el equipo de cómputo personal cuente con un software antivirus, antispyware, firewall y se mantengan debidamente configurados y actualizados, un 91,5% dice contar con un antivirus actualizado, mientras un 7,3% ignora si su equipo cuenta con este tipo de software de protección y un 1,2% señala que no cuentan con este tipo de protección. De igual manera con el uso del firewall un 62% dice contar con este tipo de software, un 32,9% ignora si lo tiene instalado o configurado correctamente y un 4,9% indica no contar con la protección del firewall. Asimismo los bancos aconsejan a sus clientes el no contar con la misma contraseña en más de un sitio en Internet; frente a este consejo de seguridad un 63,4% de los clientes, bajo el conocimiento del peligro que esto significa, no hace uso de la misma clave en más de un sitio, contra un 36,6% que sí hace uso de la misma clave en más de un sitio en Internet.

Según informes presentados por el Organismo de Investigación Judicial (OIJ, 2010), han disminuido el número de fraudes de banca por Internet en comparación con años anteriores. Ante la consulta a la población de estudio sobre el conocimiento adquirido en el tema de seguridad bancaria en línea, como lo muestra el gráfico nº 7, predomina con un 59,8% los que dicen contar con un conocimiento moderado, seguido por un 15,9% que indica contar con poco conocimiento en el tema, contra un 12,2% que comenta tener un alto nivel de conocimiento sobre cómo proteger sus datos en Internet y evitar ser víctimas de fraudes.

Finalmente, frente a los constantes y novedosos tipos de ataques que los piratas cibernéticos realizan, las entidades financieras publican frecuentemente en sus sitios de Internet información sobre éstos y cómo protegerse. En el gráfico nº 8 se observa claramente el comportamiento de la población encuestada, donde revela que un 35,4% de estos usuarios rara vez se preocupa por informarse de las nuevas amenazas existentes, y

con mayor riesgo un 11% indica que nunca se preocupan por informarse de peligros de este tipo.

Gráfico Nº 8



CONCLUSIONES

Los resultados que se lograron obtener con el estudio reflejan el comportamiento de los usuarios de banca por Internet. La demanda en el uso de los servicios de banca electrónica en línea ha aumentado exponencialmente, de igual manera los delincuentes cibernéticos ven ante este comportamiento una oportunidad para realizar fraudes por medio de Internet. La población en la cual se realiza el estudio demuestra tener conocimiento del riesgo existente al hacer uso de estos servicios, sin embargo no todos acatan las precauciones necesarias para evitar ser víctimas de robo por medio de la web. No existe diferencia entre el mundo real y el virtual al momento de tratar con dinero. Así como los usuarios aplican medidas de seguridad cuando ingresan a un banco a retirar dinero o directamente en un cajero automático, siempre observan a su alrededor, tienen el cuidado de que nadie observe la clave al digitarla, evitan que un tercero logre observar cuánto dinero se está retirando; y si perciben que algo no está bien y sienten inseguridad, no realizan la transacción. En Internet ocurre exactamente lo mismo, todos los cuidados como los anteriormente mencionados también se deben aplicar, los usuarios deben ser observadores y minuciosos al momento de ingresar sus datos en los portales bancarios y constatar que el sitio es el correcto y no una réplica montada por un estafador.

Aunque las entidades bancarias publican en sus sitios en Internet consejos para hacer uso de sus servicios en línea de forma segura, no todos los usuarios toman el tiempo para conocerlos. Como producto de esto es que cometen imprudencias de compartir claves, usarlas en más de un sitio, mantenerlas por escrito, no contar con dispositivos token o claves dinámicas, ingresar al portal bancario haciendo uso de los buscadores u otros enlaces en lugar de digitar la dirección del banco, abandonar el sitio sin hacer uso de la opción "*finalizar sesión*", de manera que aumentan su riesgo al ingresar a la entidad bancaria. Actualmente es imprescindible contar con sistemas de seguridad para evitar ataques de todo tipo. Ante esto, de igual manera los bancos aconsejan contar con software como antivirus, antispyware y firewall. Aunque los usuarios tratan de cumplir esta recomendación, en muchas ocasiones estas aplicaciones no cuentan con las últimas actualizaciones, ni los usuarios se preocupan por realizar chequeos frecuentes de sus equipos en busca de virus.

Es importante que los usuarios de banca electrónica en línea sean conocedores de estas diferentes formas de realizar estafas, y sobre todo que cuenten con los conocimientos de cómo protegerse. El nivel de riesgo señalado en los encuestados indica claramente que un 49% de los usuarios debe mejorar sus conocimientos y habilidades en el tema de seguridad en línea a fin de evitar ser víctimas de estos delincuentes. En definitiva, el estudio demuestra que los usuarios son precavidos, no obstante el interés que los encuestados dicen tener en cuanto a informarse sobre nuevos riesgos y amenazas es muy bajo, factor que los puede exponer a ser víctimas de los delincuentes informáticos.

BIBLIOGRAFÍA

Banco de Costa Rica. (2011).Prevención de Fraude y Seguridad en Línea. Recuperado el 5 de febrero del 2011, de http://www.bancobcr.com/personas/prevencion%20de%20fraude%20y%20seguridad%20en%20linea/

Bit Defender. (2008). Encuesta de Bit Defender Muestra las Principales Preocupaciones de los Usuarios en lo que a Seguridad Informática se Refiere. Recuperado el 25 de enero del 2011, de http://www.bitdefender.es/NW870-es--Una-encuesta-realizada-por-BitDefender-uestra-las-principales-preocupaciones-de-los-usuarios-en-lo-que-a-seguridad-inform%C3%A1tica-e-refiere.html

Banco HSBC. (2011). Phishing. Recuperado el 06 de marzo del 2011 de http://www.hsbc.fi.cr/a/be/alertas.asp

CentiSur y D'Alessio IROL. (2010). Seguridad en Internet: La Visión de los Usuarios. Evol. 2006 – 2010. Recuperado el 26 de enero del 2010 de http://www.certisur.com/sites/default/files/docs/201006-EncuestaSeguridadInternet.pdf

Cordero, C. (2001). Desarrollan directrices de riesgo tecnológico. Recuperado el 27 de febrero del 2011 de http://www.elfinancierocr.com/ef_archivo/2001/diciembre/22/tecnologia1.html)

Cuadra, C. (2010). Por su seguridad, claves de 12 caracteres. Recuperado el 19 de febrero del 2001 de http://www.elfinancierocr.com/ef_archivo/2010/agosto/29/tecnologia2487274.html

Datum Internacional.(2011). Calculadora del Margen de Error. Recuperado el 21 de marzo del 2011, de http://www.datum.com.pe/margendeerror.php

Deloitte. (2010). 2010 Global Financial Services Security Survey. Recuperado el 29 de enero del 2011, de http://www.deloitte.com/gfsi/securitysurvey

Dirección de Investigación Criminal. (2010) No sea víctima del fraude electrónico. Revista *Élite*, 15, 2-4.

EBanking News. (2008). Estudio sobre Seguridad en Internet. Recuperado el 26 de enero del 2011 de http://www.ebanking.cl/seguridad/estudio-sobre-seguridad-en-internet-00886

Hernández, Fernández y Baptista (1991), *Metodología de la investigación*, México: McGraw-Hill.

Melagatti, C. (2010). Bancarización en línea. Recuperado el 02 de marzo del 2011 de http://www.nacion.com/2010-07-19/Opinion/Editorial/Opinion2451711.aspx

Melagatti.C (2010, 19 de Oct.). Bancos reportan aumento en transacciones por Internet. La Nación, p. 20A.

Organismo de Investigación Judicial. (2010, 11 de Nov.). OIJ Reporta Disminución en Delitos por Fraude Bancario. La Nación, p. 28A.

Panda Security. (2011). Trojans. Recuperado el 06 de marzo del 2011 de http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/trojan/

Scotiabank Costa Rica. (2011). Seguridad Medidas Preventivas. Recuperado el 4 de marzo del 2011, de http://www.scotiabankcr.com/acercade_seguridad_medidas_preventivas.shtml

ANEXOS

Ver Encuesta Adjunta