Síguenos en:

CIBERSEGURIDAD EN LA ERA DE LA REVOLUCIÓN FINTECH

Cámara de Comercio de Bogotá

Tus sueños son nuestra empresa

PRESENTACIÓN

La Cámara de Comercio de Bogotá (CCB) a través de la Vicepresidencia de Fortalecimiento Empresarial (VFE), ofrece servicios que promueven el emprendimiento, la formalización, el fortalecimiento y la innovación de las empresas de Bogotá y la Región.

Para acceder a estos servicios el empresario o emprendedor realiza un autodiagnóstico empresarial con el objetivo de identificar sus necesidades empresariales; a partir de la información recogida se construye una ruta de servicios acorde a las necesidades identificadas y dirigida al fortalecimiento y mejora continua de las empresas, buscando alcanzar una mayor competitividad en el mercado.

El portafolio que ofrece la CCB está enfocado a que el empresario alcance la optimización de la gestión empresarial, aprendiendo cómo diseñar, implementar y ajustar su estrategia para hacerla diferente y exitosa en el mercado.

Sumado al portafolio de servicios, la CCB realiza un acompañamiento a los empresarios a través del cual se establecen actividades, un cronograma a trabajar y el seguimiento del cumplimiento de los compromisos adquiridos por cada empresario. Todo esto se trabaja dentro de un enfoque sectorial que permita dar respuesta a las necesidades identificadas en cada uno de los sectores económicos.

El portafolio especializado incluye cuatro tipos de servicios: de información, formación, asesoría y contacto.

SERVICIOS DE INFORMACIÓN:
Corresponde a documentos de carácter empresarial y técnicos, disponibles para la consulta de cualquier persona; pueden ser de carácter virtual o físicos.

SERVICIOS DE FORMACIÓN Y APRENDIZAJE:
Son aquellos servicios necesarios para transmitir un conocimiento específico y aplicable para mejorar el desempeño de los clientes.

SERVICIOS DE ASESORÍA:
Actividad cuyo principal objetivo es resolver con la ayuda de un experto consultas específicas y puntuales de los clientes sobre temas de desarrollo empresarial.

SERVICIOS DE CONTACTO:
Son aquellos servicios orientados a brindar espacios de relación y/o cooperación empresarial entre actores económicos, y/o clientes, según el caso, para que interactúen, conozcan, identifiquen, comparen, generen contactos, realicen negocios, consigan financiación, teniendo en cuenta sus intereses y necesidades puntuales.

En este sentido, la Dirección de Fortalecimiento Sectorial con el objetivo de brindar información actualizada a los empresarios del sector, presenta este documento que busca apoyar el entendimiento del negocio financiero a partir del conocimiento de los nuevos modelos de negocio y las tendencias del mercado financiero internacional que determinan el avance de la industria.

CONTENIDO

CAPÍTULOS

1. Introducción
2. Un poco de historia
3. Los riesgos de seguridad más comunes
4. Casos famosos de ciberfraudes
5. Tendencias en ciberseguridad
6. Lo que trae el futuro
7. Conclusión

CAPÍTULO

1.

INTRODUCCIÓN

La aparición de las *fintech*, empresas innovadoras del sector de servicios financieros que se caracterizan por su fuerte componente tecnológico, está introduciendo profundos cambios en el sector financiero, debido a la utilización cada vez más frecuente de dispositivos móviles, la Internet y las redes sociales, los cuales se alejan cada vez más de los tradicionales procesos bancarios.

Al tratarse de empresas nacientes, estas nacen con estructuras cambiantes y modelos de negocio adaptados a las nuevas circunstancias que está demandando el mercado: *agilidad, flexibilidad, privacidad, seguridad, precios bajos;* pero, sobre todo, el aprovechamiento de los cuatro pilares de las tecnologías de la información y la comunicación en la actualidad: la nube o almacenamiento de información en la red; *el big data o grandes cantidades de información y la analítica de esta;* las redes sociales y la movilidad para conectarse desde cualquier lugar.

Al ser la tecnología un pilar fundamental de su funcionamiento surge la importante pregunta por la seguridad de estos sistemas, *ya que las amenazas de fraude, suplantación de identidad, robo de información, entre otras, van ligadas con el uso de dicha tecnología.*

Aquí le contamos cómo van las fintech en materia de seguridad en la web o *"ciberseguridad"*.

CAPÍTULO

2.

UN POCO DE HISTORIA

Las fintech emergieron en el 2008, tras la pérdida de la imagen y confianza hacia la banca, que desencadenó la crisis hipotecaria global en los mercados financieros, ocasionada por una burbuja inmobiliaria y la crisis en el pago de hipotecas en Estados Unidos durante ese año.

El primer producto surgido de la revolución de la tecnología en la banca fueron las monedas virtuales, que aparecen gracias a la tecnología de *"blockchain" o "cadenas de bloques"* de información, sin estar respaldadas por ningún Gobierno ni depender de la confianza de ningún emisor central de monedas.

Desde este momento surgió la pregunta por la seguridad y defensa contra amenazas de estos sistemas que muchas veces, como en el caso de las monedas virtuales, para funcionar necesitan el intercambio de información con múltiples fuentes, sin más protección que el sistema mismo.

Entonces en una tecnología como el *"blockchain"* los riesgos sí existen y provienen de amenazas externas al sistema como *suplantación de identidad, robo de contraseñas o fraude,* que son los riesgos más comunes de cualquier sistema de transacciones en línea.

CAPÍTULO 3.

RIESGOS DE SEGURIDAD MÁS COMUNES

Estos son los problemas de seguridad más comunes que amenazan los sistemas de pagos electrónicos:

» **Falsificación de la información de pago o phishing:**
Se realiza a través del envío de un correo electrónico, suplantando a una fuente conocida como una *red social, tienda online, banco, institución pública,* con el objetivo de robar la información de pago del usuario para luego usarla en transacciones digitales.

El objetivo principal del phishing es la suplantación de identidad o fraude, que se posiciona como la gran amenaza de la economía digital y se observa en *el robo de contraseñas, tarjetas de crédito, datos financieros, usurpación de identidad en redes sociales,* entre otras acciones maliciosas; ya que, una vez robados los datos, pasarán a manos del estafador, el cual usará la identidad falsa para realizar transacciones en la web.

» **Sitios web falsos:** **Páginas web sin iconos de seguridad como el candado en la barra de estado del navegador, una *"s"* después de *"http"* en la dirección URL o las palabras *"Secure Sockets Layer" (SSL),* pueden ser sitios web falsos dedicados al robo de información de pago de los usuarios.**

» **Botnets y malware:** son robots informáticos y software malicioso que se ejecutan de manera autónoma y automática para obtener datos de una computadora y realizar fraudes en línea. Por esto, es importante que los equipos en los que se realicen transacciones electrónicas tengan antivirus instalados, que previenen que programas informáticos fraudulentos puedan estar registrando los pagos que se llevan a cabo, las teclas del ordenador que se usan o los números o letras marcados en el teléfono para obtener la información financiera de una persona.

Según cifras de la *Superintendencia Financiera de Colombia,* en el país son generados en promedio *542.465 ataques informáticos diarios,* de los cuales *39,56% los sufre el sector financiero*, principalmente en la modalidad de fraude o robo de identidad.

Por ejemplo, delitos como la clonación de tarjetas de crédito sucede en un *30% en los cajeros electrónicos* y 70% en las plataformas de comercio que no cuentan con suficientes procesos de verificación de identidad de los usuarios.

CAPÍTULO

4.

CASOS FAMOSOS DE CIBERFRAUDES

Uno de los casos más sonados de delitos en la web es el de *Facebook y Cambridge Analytica,* una firma de consultoría política afiliada a la campaña electoral del presidente Donald Trump en 2016, a la que se le acusa de haber obtenido datos de forma inapropiada de más de *87 millones de usuarios de la famosa red social Facebook* para ser usados en propaganda política. Se alega que la firma creó perfiles psicológicos para influir en cómo la gente votaba o incluso piensa en política y sociedad, y violó las políticas de privacidad de la plataforma social para obtener información de los usuarios. El caso aún está en desarrollo.

Específicamente en el sector financiero, las principales técnicas y herramientas utilizadas por los cibercriminales son: *Denegación de Servicio (DoS), códigos maliciosos en terminales puntos de venta (PoS) o cajeros automáticos,* explotación de vulnerabilidades e incluso el uso de herramientas para ataques dirigidos. Además, se comenzó a emplear técnicas como watering hole, donde sitios web son alterados para llevar a cabo actividades maliciosas, mientras que los usuarios que usualmente visitan las páginas ignoran que se encuentran ante una amenaza.

Un caso muy famoso de ataques a bancos, *es el del robo de US$81 millones al Banco Central de Bangladesh realizado en el año 2016,* mediante el uso de un código malicioso que permitió a los cibercriminales acceder y alterar el software de mensajería para transacciones internacionales *"SWIFT Alliance Access",* utilizado por más de 11.000 bancos e instituciones financieras en más de 200 países.

Cámara de Comercio de Bogotá

CAPÍTULO

5.

TENDENCIAS EN CIBERSEGURIDAD

Como respuesta a estas amenazas de seguridad, el sector busca innovar cada día con mejores métodos y tecnologías cada vez más sofisticados contra los riesgos en las transacciones digitales. Estos son los últimos avances en el sector:

» **Biometría:** es un sistema de identificación de la identidad de una persona que *usa herramientas como reconocimiento de voz, huellas dactilares, reconocimiento facial, entre otras;* y se aplica en muchos procesos de autenticación de identidad en el sector financiero debido a la eficacia y comodidad de este método.

El uso de datos biométricos para autenticar la identidad es algo ya familiar para todos, gracias al uso de los lectores de huellas dactilares en los teléfonos inteligentes a lo largo de los últimos cinco años.

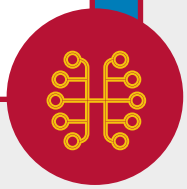
Ahora esta tecnología está mirando más allá de las huellas dactilares, hacia la comprobación de identidad *mediante el iris o patrones de las venas,* e incluso características únicas en cuanto a la forma en que una persona escribe sobre un teclado o mueve el mouse. Esto es *"biometría del comportamiento",* un enfoque innovador de la autenticación biométrica que se basa en la creación de un perfil único para cada cliente.

En la actualidad, mediante tecnologías de vanguardia de aprendizaje automático y grandes volúmenes de datos, la biometría del comportamiento emplea una rica combinación de características personales y de dispositivos para distinguir entre clientes legítimos y estafadores.

» **Uso de inteligencia artificial:** de acuerdo con la empresa de *ciberseguridad VU*, el *phishing* se va a poder combatir con un componente de *"machine learning"* o *inteligencia artificial.* Es decir, que es probable que pronto sea posible predecir cuál será el tipo de transacciones que un usuario hará en el futuro, teniendo en cuenta la inteligencia de las máquinas y de esta forma se podrían no autorizar las operaciones sospechosas.

"Con el avance de la inteligencia artificial las máquinas van a poder crear un perfil transaccional de una persona, hacer el análisis de qué dispositivos usa, en qué momentos del día, desde qué ubicaciones y evitar así las operaciones anormales", explicó la empresa VU.

» **Redes definidas por software:** esta es una herramienta de seguridad que se desprende de la tecnología de un software al dar acceso a la conexión en redes seguras. *Esto se aplica en el caso de las API,* donde distintos software trabajan en conjunto y comparten información y su seguridad depende de una limitación a las redes que pueden conectarse a través de protocolos, claves y algoritmos cifrados de última generación, y el uso de un directorio o una función de administración entre *las API y las aplicaciones que pueden acceder a ellas,* de manera que se puede proporcionar acceso directo y controlado a la información.



CAPÍTULO

6.

LO QUE TRAE EL FUTURO

En materia de seguridad aún está todo por desarrollarse en el mundo digital, además que este aspecto debe evolucionar tan rápido como lo hace la tecnología en estos días.

Para el futuro se espera que, cada vez más, las instituciones financieras implementen la *biometría facial* o de voz para reemplazar el pin y la clave, y mejorar así la seguridad en las operaciones bancarias diarias.

También se espera que pronto sea una realidad la *tarjeta de pago biométrico,* la cual permitirá al *titular tocar un sensor de huellas dactilares* incorporado a la tarjeta al realizar una transacción para verificar su identidad, sin necesidad de usar una clave.

Además, para confirmar la identidad del cliente, esa imagen es comparada con la imagen almacenada de manera segura en el *chip de la tarjeta,* pero nunca sale de la tarjeta. No hay necesidad de enviar dato alguno a un tercero para autenticación, eliminando así la necesidad de crear una *base de datos biométricos* y el riesgo de que las huellas dactilares sean interceptadas o se produzca cualquier otra interferencia en el proceso.

De la misma forma se espera que evolucione la *biometría facial* de tal manera que en lugar de poner una clave, a través de una foto del rostro del usuario, se pueda confirmar su identidad en el momento a la hora de realizar transacciones digitales.

Por esto, los expertos afirman que, de cara al futuro, el mayor requerimiento de las empresas será eliminar el centro transaccional. Es decir, usar tecnologías como el reconocimiento facial, que no requieran de un tercero para comprobar la identidad de las personas y garantizar así una seguridad máxima.

CONCLUSIÓN

CAPÍTULO 7.

El avance de la tecnología en el sector financiero representa un reto de múltiples dimensiones y una de las más importantes es el aspecto de la seguridad, pues a medida que la tecnología en este sector avanza, también lo deben hacer los sistemas de prevención de riesgos.

Por esto, se puede concluir que la seguridad de un sistema de transacciones digitales no es una estrategia estática, sino que necesita evolucionar y adaptarse constantemente, basándose en la información sobre tendencias, las nuevas amenazas y las técnicas de seguridad más recientes para mantener verdaderamente segura una red.

Además, al ser las fintech una industria naciente, que encuentra en la tecnología su razón de ser con el propósito de brindar servicios financieros de manera eficiente, ágil, cómoda, accesible, confiable y segura; de forma que, para mitigar y evitar riesgos de naturaleza criminal, lo imperativo es la gestión y tratamiento de dichos riesgos poniéndolos en el radar de especialistas que contribuyan con sus conocimientos, experiencia y buenas prácticas en su mitigación.

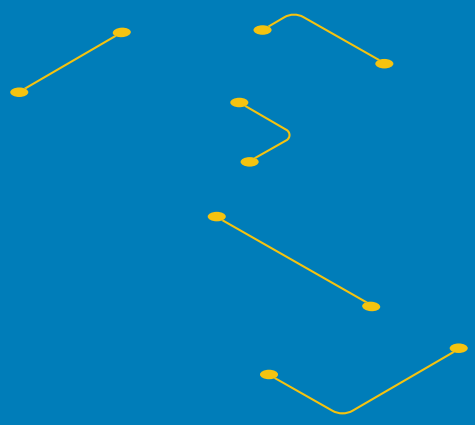
Así que, a medida que la tecnología avanza y el sector fintech invierte recursos y atención en desarrollar soluciones más innovadoras y cómodas para los servicios financieros, la seguridad debe evolucionar a la par, porque de nada sirve tener los sistemas más avanzados y sencillos para realizar operaciones financieras, cuando son tan frágiles como una pared de cristal. Tecnología y seguridad deben ir de la mano en las fintech.

La CCB cuenta con un portafolio especializado para empresas del sector de servicios financieros que les permite a los empresarios conocer e identificar nuevas oportunidades y sumarse a la revolución digital que está cambiando la forma de hacer negocios en el sector. Conozca más información en: ***www.ccb.org.co***

BIBLIOGRAFÍA

Organización de los Estados Americanos. Ebook: Estado de Ciberseguridad en el Sector Bancario en Latinoamérica y el Caribe. Junio de 2018, disponible en la web.

Innovation Center BBVA. Ebook: Observatorio sobre Regulación Digital y Tendencias. Mayo de 2018, disponible en la web.



Cámara de Comercio de Bogotá

Tus sueños son nuestra empresa