CONSTRUYE TUS FINANZAS

Superintendencia de Bancos
Guatemala, C. A.

Innovación y ciberseguridad

www.sib.gob.gt SIB Guatemala @sib_guatemala SuperBancosGuatemala
sib_guatemala Superintendencia de Bancos (SIB)

CONSTRUYE
TUS FINANZAS

Superintendencia de Bancos
Guatemala, C. A.

Introducción

La Superintendencia de Bancos
con el objetivo de proporcionar una herramienta de consulta y aprovechar el adecuado manejo de sus finanzas personales, pone a su disposición el fascículo sobre Innovación y ciberseguridad.

En un mundo tan complejo y globalizado, se hace necesario investigar y entender cómo funciona el sistema financiero, así como conocer sobre los productos y servicios innovadores que este ofrece. El efecto de estar atentos será el contar con un buen manejo de las finanzas personales basado en conocer y comprender cómo funcionan estos productos y servicios, así como los elementos innovadores, además de identificar cómo estar mejor informados y tomar medidas pertinentes que resguarden la seguridad de los usuarios.

En ese sentido, la Superintendencia de Bancos ha impulsado el Programa de Educación Financiera que permite que los usuarios tomen decisiones basadas en una mejor información.

Es importante aclarar que la expresión finanzas personales se refiere a:

- El conjunto de recursos, como bienes, tecnología o dinero que tiene una persona para realizar una serie de actividades en su vida diaria.
- La forma de manejar y distribuir esos recursos.
- La manera cómo el manejo o distribución de los recursos repercute en el bienestar de la persona.

En el tratamiento y aplicación de temas financieros es importante considerar los valores personales para tomar decisiones. Estos valores son el conjunto de principios, virtudes o cualidades inherentes a la persona y se manifiestan en la forma de actuar y el ámbito financiero no es la excepción; en ese sentido, se presentan los siguientes como ejes transversales del manejo financiero.

- **Responsabilidad:** consiste en asumir las consecuencias del acto intencionado, resultado de las decisiones que se toman y aceptan; es obrar de manera consistente a las ideas propuestas.
- **Respeto:** es la consideración que se debe tener hacia sí mismo y hacia las demás personas; es un valor que nos lleva a honrar la dignidad de los demás y atender sus derechos.
- **Confianza:** proviene de la conjunción de las palabras "con fe". Implica fe en que alguien cumplirá lo convenido. La confianza es la base de las buenas relaciones interpersonales e institucionales. Se basa en el respeto mutuo y la responsabilidad ante los compromisos con los demás.
- **Honestidad:** implica, entre otras actitudes, administrar adecuadamente lo que se tiene a cargo; ser honestos consigo mismo y los demás respecto a los compromisos que se asumen.
- **Orden:** es organizar tanto el tiempo como el espacio y los recursos.

Innovación

En la prestación de servicios financieros, la tecnología ha favorecido la innovación con el objetivo de ampliar las oportunidades para que la población acceda a servicios financieros que pueden ir desde realizar pagos y transacciones cotidianas, hasta acceder a créditos, contratar seguros o realizar inversiones. Esto requiere que exista un marco que propicie un ambiente para que estos servicios se brinden de manera confiable y segura a las personas y empresas, por parte de los oferentes de productos y servicios financieros.

En el fascículo sobre medios de pago, presentamos información sobre el uso de cheques, tarjetas de débito y crédito, servicios financieros móviles y una introducción al concepto de dinero electrónico, por lo que, en este se ampliará información sobre la innovación en el acceso a servicios financieros, mediante nuevos canales y productos.

Agentes bancarios

Al referirnos a los canales y puntos de acceso podemos considerar las agencias bancarias, los cajeros automáticos y desde 2010 los agentes bancarios, que son:

Personas individuales o jurídicas que ejercen actividades comerciales, tales como una tienda, farmacia u otra similar, con las que un banco suscribe un contrato para que, por cuenta de este, puedan realizar algunas operaciones y prestar determinados servicios.

Entre otros, ejemplos de productos: recepción de depósitos, en cuentas monetarios y ahorro; pago de cheques, retiros de cuentas de depósitos, previamente constituidas en el banco contratante; pago de préstamos, recepción y envío de remesas.

Los establecimientos de agentes bancarios son:

Ubicaciones físicas en las que los agentes bancarios pueden realizar operaciones y prestar servicios en nombre de un banco.

Por ejemplo, en el caso de la Farmacia XYZ, la empresa es el agente bancario y sus diversas ubicaciones físicas o sucursales son los establecimientos.

¿Cómo debe un banco seleccionar un agente bancario?

Debe considerar para evaluar:

- Características del canal de distribución.
- Entorno geográfico.
- Las operaciones brindadas por el banco a través de los agentes bancarios.
- Los riesgos de reputación, operación, lavado de dinero u otros activos y financiamiento del terrorismo, determinando las medidas que se tomarán para mitigarlos.

Los requisitos de un comercio con el objetivo de ser un agente bancario son:

a. Acreditar ser persona solvente e idónea;
b. Estar inscrito en el Registro Mercantil;
c. Estar inscrito en el Registro Tributario Unificado; y,
d. Acreditar que el negocio tiene por lo menos un año de operación.

En Guatemala, la Resolución de Junta Monetaria 065-2010 contiene el Reglamento para la Realización de Operaciones y Prestación de Servicios por medio de Agentes Bancarios.

Ecosistema Digital

En el entorno financiero observamos que, además de los puntos de acceso como los comentados anteriormente, podemos acudir a los servicios financieros por medios digitales, los cuales permiten potencializar los servicios y productos que se encuentran a disposición de los distintos segmentos.

Algunos de estos servicios digitales son brindados por entidades financieras bancarias y otros, generalmente asociados a los pagos y transferencias, los brindan entidades no bancarias de forma independiente o en asociación con el sector bancario.

A toda esta interacción entre usuarios, proveedores de servicios financieros digitales, la infraestructura tecnológica, los marcos regulatorios y las políticas que se aplican se le denomina Ecosistema Digital y funciona como se muestra a continuación:

Usuarios

Consumidores, empresas, gobierno u organizaciones que tienen necesidades de productos y servicios financieros.

Proveedores

Bancos, otras instituciones financieras que suministran productos y servicios a través de medios digitales.

Infraestructura

Financiera y técnica

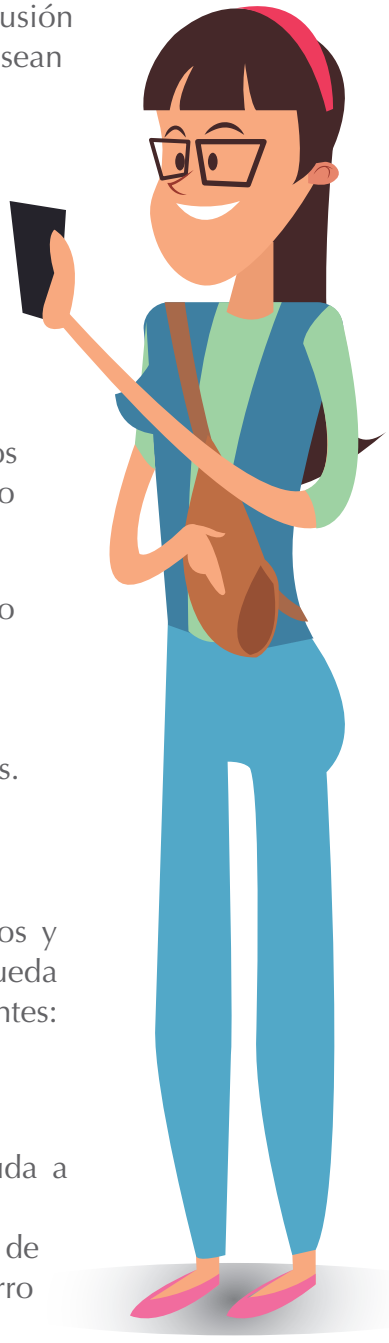
Políticas

Leyes, reglamentos u otros que propician el acceso a servicios financieros de forma ordenada, asequible y segura.

La digitalización y la inclusión financiera

La innovación en los productos y servicios financieros propende hacia la digitalización de los canales para acceder (como teléfono móvil, banca en línea) a los productos y servicios financieros, ambos aunados a favorecer la inclusión financiera, es decir que todos los segmentos de la población puedan acceder, obtener productos y hacer uso de manera asequible y segura, en función de las aplicaciones de los intermediarios y las necesidades de sus clientes y usuarios.

Según el *Center for Financial Inclusion* (ACCION International): "La inclusión financiera plena es un estado en el que todas las personas que desean hacer uso de los servicios financieros tienen acceso a los mismos a precios asequibles y provistos de forma adecuada y digna. **Los servicios financieros son provistos por una amplia variedad de proveedores**, la mayoría de ellos del sector privado**, con capacidad y voluntad de llegar a todos los potenciales clientes**, incluidas personas con diversidad funcional, intelectual, con bajos ingresos, en el ámbito rural y otras que se encuentran en situación de exclusión económica y social."



Lo anterior, confirma la importancia de la participación de distintos oferentes de productos y servicios financieros para facilitar el proceso de inclusión financiera, ya que:

- Se reducen los costos asociados a la presencia física de agencias o agentes bancarios.
- El usuario puede realizar pagos de forma más autónoma.
- Facilita el acceso a productos y servicios, inclusión financiera.
- Permite una bancarización eficiente y ágil para todos los segmentos.

Digitalización

Más allá de ser una "sofisticación" la digitalización de los productos y servicios financieros debe aprovecharse para que la población pueda acceder a la mayor cantidad de ellos, ya que presenta las ventajas siguientes:

- Reducen costos de operación
- Eleva la efectividad.
- Mejora la transparencia y trazabilidad de los pagos, lo cual ayuda a evitar o detectar fraudes.
- Reducción en el uso de fuentes informales de productos y servicios de crédito o productos y servicios en productos monetarios y de ahorro (Visita nuestros fascículos sobre Ahorro y Crédito).

FinTech

Son las innovaciones financieras propiciadas por la tecnología que podrían dar lugar a nuevos modelos de negocio, aplicaciones, procesos o productos con un efecto sustancial sobre los mercados y las instituciones financieras en la prestación de servicios financieros.

El origen de este término se encuentra en la contracción de las palabras "*Finance*" y "*Technology*", para la generación de canales y servicios financieros que puedan brindarse en los esquemas siguientes:

- B2B (*Business to Business*): de empresa a empresa (tanto del sector financiero como de otros).
- B2C (*Business to Customer*): de empresa a consumidores o usuarios.

Muchas de las empresas que ofrecen este tipo de servicios financieros digitales se consideran como *Start Ups* porque están iniciando en el entorno digital y *Scale Ups* cuando ya están en un nivel escalable en sus operaciones. Cabe indicar que según el Banco de Pagos Internacionales -BIS-, entre los principales productos y servicios *FinTech* se encuentran los siguientes:

- Servicios de crédito, depósito y captación de capital.
- Servicios de pago, compensación y liquidación.
- Servicios de gestión de inversiones.

En adición a lo anterior, existen los servicios de apoyo en el mercado, los cuales son los siguientes:

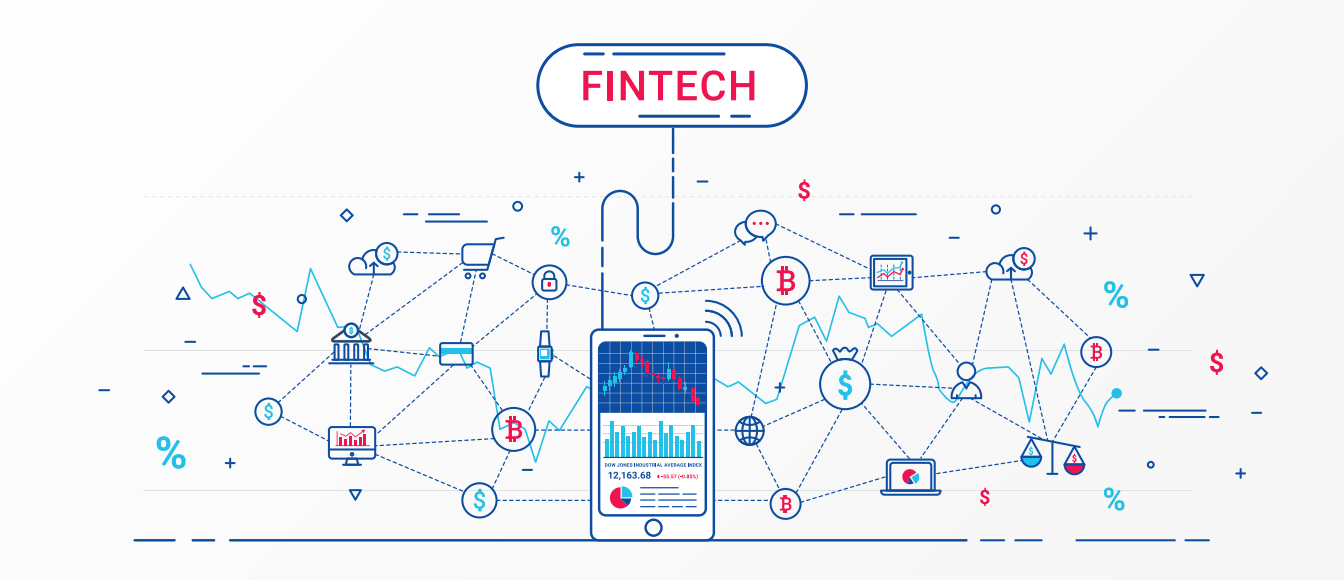
- Agregadores de datos y portales.
- Ecosistemas (infraestructura, código abierto, API).
- Aplicaciones de datos (*big data*, aprendizaje automático, modelación predictiva).
- Tecnología de registros (cadena de bloques, contratos inteligentes).
- Seguridad (identificación y autenticación de clientes).
- Computación en la nube.
- Internet de las cosas / tecnología móvil.
- Inteligencia artificial (*bots*, automatización en finanzas, algoritmos).

Por aparte también es importante conocer los distintos escenarios de la industria bancaria, ya que el auge que han tenido las *FinTech* ha dado lugar a lo que algunos han denominado la batalla por la relación con el cliente y los datos de clientes.

- *Neobanks*: startups *FinTechs* que ofrecen una experiencia 100% móvil de banca.
- *Open Banking* / o banca abierta: que brindan la apertura y acceso de los datos, propiedad de los usuarios o consumidores, para ofrecerles un valor agregado.
- *Digital Banking:* representa un proceso virtual que incluye banca en línea, ofreciendo los servicios a través de internet.

En el ámbito de las *FinTech* las principales áreas en las cuales están ofreciendo servicios son las siguientes:

- Pagos y transacciones cotidianas como transferencias entre usuarios o negocios (*Peer to Peer* o P2P) y del gobierno (G2P) o al Gobierno como impuestos o tasas (P2G).
- Gestión de finanzas personales: soluciones para que los usuarios lleven el control de sus finanzas personales. Pueden ser desde el mismo sitio en internet de un banco, una aplicación móvil u otras.
- Acceso a crédito: ofrecen acceso a distintas formas de créditos de una forma más rápida.
- Acceso a seguros: mediante contratación de distintas formas de cobertura.
- Inversión: herramientas en función del perfil de riesgo de la persona y que, pueden variar desde un ahorro programado y automatizado hasta activos inmobiliarios, en *Start Ups*, entre otros.



Aunque los servicios de las *FinTech* están en el ámbito financiero, a estas no les está permitido realizar intermediación financiera.

En Guatemala, únicamente los bancos autorizados conforme la Ley de Bancos y Grupos Financieros pueden realizar operaciones de "intermediación financiera bancaria", es decir captar recursos del público y otorgarlos a otras personas, empresas o gobierno a manera de financiamiento.

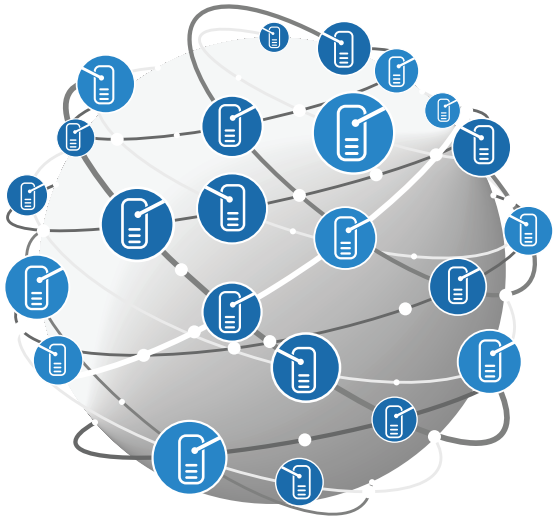
Debido a la evolución tecnológica, la Superintendencia de Bancos pone a disposición un espacio denominado "SIB InnovatioNHUB", el cual es un punto de encuentro entre la Institución y las personas que desarrollen o utilicen modelos de negocios que apliquen tecnologías financieras innovadoras, lo que permite conocer los desarrollos actuales y las tendencias de estos, así como un espacio que facilita la comprensión del marco jurídico financiero vigente.

Para más información visite: https://www.sib.gob.gt/SIBInnovationHUB/

Adicional, cabe resaltar que en muchos países se ha impulsado la creación de *sandbox* o espacios de prueba, con el acompañamiento del ente supervisor, para que los modelos de negocio puedan ser probados antes de lanzarlos al mercado, con el objetivo de experimentar la prestación de servicios financieros y así identificar y gestionar los riesgos de cara a la protección del público usuario, así como en el mismo funcionamiento del modelo.

Blockchain

Conocida como la cadena de bloques consiste en un registro de datos digitales descentralizado y compartido, que permite llevar a cabo transacciones entre dos o más partes de forma verificable, protegida criptográficamente, basada en la confianza mutua y anónima de quienes participan en ella y el consenso entre quienes intervienen.



Esta tecnología ha sido de utilización en la realización de pagos y transferencias digitales; adicionalmente, ha constituido la base para el desarrollo de activos digitales como las criptomonedas.

Para conocer acerca de estos conceptos y sus definiciones visite:

https://www.sib.gob.gt/web/sib/educacion-financiera/Glosario

Dinero electrónico

Consiste en el valor monetario equivalente al valor expresado en la moneda de curso legal del país y cuyo intercambio se efectúa principalmente a través de dispositivos móviles.

Con características similares al dinero en efectivo debido a que es aceptado como medio de pago y además reconocido como medio de acumulación de valor.

Tiene características propias:

- Se genera a partir de la recepción de fondos con un valor no menor al valor del dinero electrónico emitido.
- Almacenado en un dispositivo electrónico, entre otros, como: un chip, tarjeta de prepago, teléfono celular o sistema de cómputo.
- Puede convertirse en efectivo.

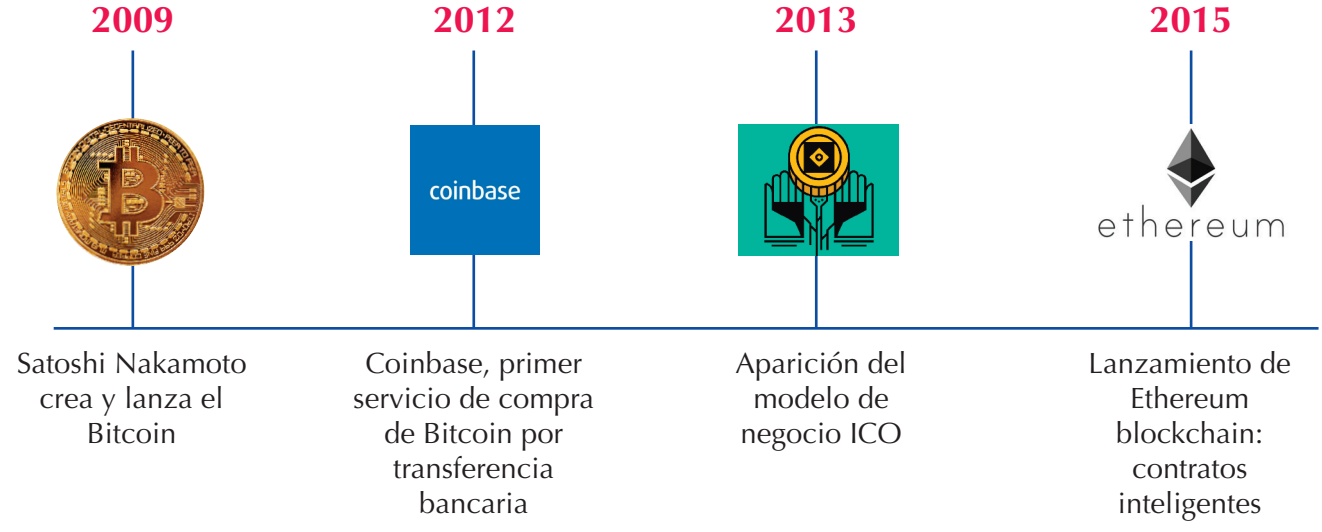
Cuando una persona dispone de dinero electrónico en un monedero digital, no constituye una forma de "ahorro", por lo que no gana intereses ni es protegido por el FOPA u otro fondo de cobertura.

Un monedero digital o *digital wallet* es un sistema que almacena de forma segura la información de pago y las contraseñas de los usuarios, el cual puede ser utilizado en numerosos métodos de pago y sitios web. Al usar una billetera digital, los usuarios pueden completar las compras de manera fácil y rápida con la tecnología de comunicaciones de campo cercano. Sustituye a tarjetas de plástico físicas y permite mejorarlas con la incorporación de nuevos servicios.

Historia de las criptomonedas

La creación de las criptomonedas surge con la idea de encontrar una alternativa digital al dinero que emiten los gobiernos y realizar transacciones instantáneas entre personas, sin la intermediación del banco central u otras instituciones financieras.

- El 3 de enero del 2009, fue lanzada al mercado la primera criptomoneda, desarrollada por "Satoshi Nakamoto" (pseudónimo) y que se denominó Bitcoin.
- En el 2012, se lanzó el proyecto *Ripple* para realizar transacciones interbancarias internacionales entre bancos, sin la necesidad de la participación de los bancos centrales. Junto con el proyecto se lanzó su criptomoneda, que actualmente se denomina XRP.
- En el 2013, apareció el uso de la denominada oferta inicial de monedas –ICO–, modelo de negocio que pretende vender criptomonedas, en forma de tokens, a los inversionistas a cambio de otras criptomonedas o monedas *fíat (del latín fíat, 'hágase')*.
- En el 2015, se lanzó Ethereum *blockchain* en su segunda versión que incluyó los denominados contratos inteligentes.



Riesgos asociados

Considerando que el uso de criptomonedas conlleva un análisis holístico y que la misión de la Superintendencia de Bancos es promover la estabilidad y confianza en el sistema financiero supervisado, a continuación se muestran los riesgos financieros asociados a las criptomonedas para comprender el impacto que existiría en la banca si se entra en contacto con dichas monedas virtuales:

Operacional: ante las múltiples formas de adquirir, utilizar y almacenar criptomonedas, los errores humanos y la exposición al fraude son elevados por el propio diseño del modelo de negocio y la falta de respaldo con garantías reales.

Tecnológico: las monedas virtuales son absolutamente dependientes de la tecnología, por lo que la ciberseguridad juega un factor importante, dado que las plataformas pueden ser objeto de ataques cibernéticos; asimismo, los usuarios pueden ser objeto de ingeniería social y permitir a los cibercriminales acceder a las cuentas donde se poseen las criptomonedas. Adicionalmente, la obsolescencia de tecnologías y la aparición de nuevos emisores privados o de monedas virtuales emitidas por bancos centrales pueden afectar de manera significativa el valor de las criptomonedas.

Legal: la incertidumbre sobre la regulación que cada jurisdicción adoptará y sus diferencias debilitan a la criptomoneda como medio de pago y como depósito de valor.

De mercado: las criptomonedas son consideradas como activos de alto riesgo derivado de las elevadas volatilidades en su cotización.

Lavado de Dinero y Financiamiento del Terrorismo LD/FT: las criptomonedas permiten el anonimato de las personas que están detrás de las transacciones, lo que dificulta el cumplimiento al procedimiento conoce a tu cliente (KYC) y esto puede aumentar el riesgo de LD/FT.

¿Cuál es la diferencia entre dinero electrónico y moneda virtual?

La diferencia radica en la emisión y respaldo:

Dinero electrónico	Moneda virtual
	
• Dinero electrónico es un mecanismo de transferencia digital para moneda fíat, es decir, electrónicamente transfiere el valor que tiene la condición de moneda de curso legal.	• La moneda virtual centralizada tiene una autoridad única de administración, la cual la emite, establece reglas de uso y tiene autoridad para retirarla de circulación. • La moneda virtual descentralizada no cuenta con una autoridad central de administración y ningún monitoreo o supervisión central.

Riesgos

Si bien es cierto la tecnología facilita el acceso a servicios financieros, existen algunos riesgos asociados a su uso y otros generados por personas mal intencionadas que utilizan la tecnología para cometer fraudes o estafas. Por ello, es importante que el usuario mantenga niveles de educación financiera y digital, para estar alerta y así evitar ser víctima de cibercrímenes.

El cibercrimen consiste en las actividades ilícitas que se realizan mediante internet o el ciberespacio para cometer un delito, que atenta contra la información e identificación del ciudadano.

Para cometer los ataques cibernéticos[1] se utilizan tecnologías muy sofisticadas; sin embargo, una de las estrategias más utilizadas por los delincuentes es la ingeniería social[2], que combina la habilidad del malhechor con la carencia de malicia o de conocimientos técnicos de la víctima. Las modalidades más comunes de ingeniería social son, entre otras el *phishing, smishing* y *vishing*.

A continuación, se presenta información de las más comunes:

Medios telefónicos

- Estafas telefónicas. Son una práctica muy utilizada en el ámbito internacional, en la cual el delincuente se hace pasar por un familiar o un ejecutivo de alguna entidad financiera o comercio, indicándole que debe realizar algún depósito urgente para ayudar al familiar o bien recibir algún beneficio o crédito posterior.

  Otra estrategia utilizada por los estafadores es decirle a la potencial víctima, que algún familiar sufrió un accidente o un secuestro y le piden dinero a cambio, para ello pueden indicar datos conocidos de la persona para que la estafa sea más creíble. Es recomendable que se cerciore de no atender este tipo de llamadas que provengan de números extraños; y en caso de duda procure comunicarse con su familiar, sin caer en pánico. Esta práctica también es conocida como *vishing*.

- Premio o concurso. El estafador le llama o manda un mensaje de texto indicándole a la persona que ha ganado un premio (desde un televisor hasta un vehículo de lujo) **PERO** para recibir el premio la víctima debe brindar información personal o de su tarjeta de crédito o realizar algún depósito.

  A esta técnica también se le conoce como *smishing*.

1 Evento con la intención de causar daño en el ciberespacio.
2 Técnica para interactuar con los usuarios y manipularlos para que entreguen su información.

En línea

Los medios cibernéticos, también pueden ser utilizados para cometer fraudes y estafas. Algunos más frecuentes son:

- *Botnets* o robots informáticos que se ejecutan de forma automática para una tarea maliciosa.

- Hackeo: es cuando una persona no autorizada ingresa a un sistema informático, puede darse desde que alguien accede a una cuenta en una red social ajena sin autorización, hasta acceso a sistemas de empresas o instituciones.

- *Phishing:* en esta el delincuente logra que la víctima revele información de su tarjeta de crédito, contraseñas o cuentas bancarias mediante correos electrónicos falsos en los que el delincuente se hace pasar por una empresa o entidad financiera.

  Se llama así ya que se origina de la palabra pescar en inglés (*fish*) puesto que la persona "muerde el anzuelo" y entrega su información.

- *Pharming*: el usuario, sin darse cuenta, ingresa desde correo electrónico a una página web que, en apariencia es muy parecida a la de una institución financiera, pero en realidad es falsa. Al acceder ingresa sus datos como números de cuenta y contraseñas, los cuales el delincuente copia y utiliza para sustraer el dinero.

- *Ransomware:* consiste en un programa informático que de forma mal intencionada impide que la víctima acceda a su computadora y archivos. El delincuente pide una suma de dinero a cambio de desbloquearlos; sin embargo, en muchos casos no obstante la víctima realice el pago no obtiene el acceso.

- Virus: los virus consisten en programas diseñados para contaminar o destruir discos duros, llegan a usuarios redes correos electrónicos, publicidad en línea u otros.

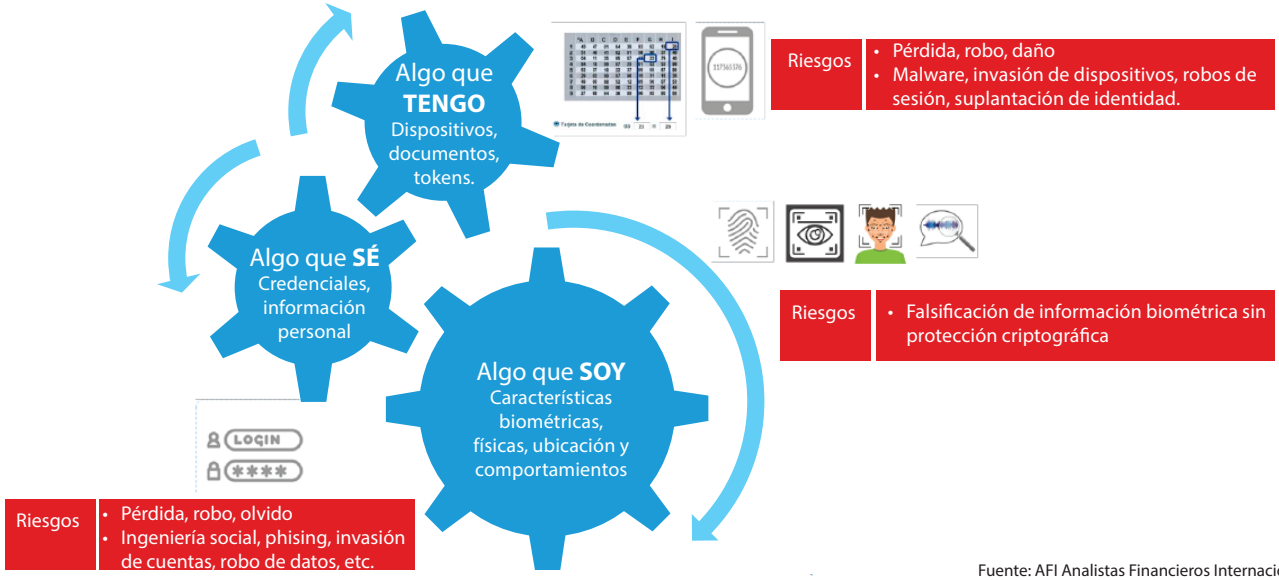
    - Los *malware* o software maliciosos son virus del tipo troyano mediante los cuales se tienden trampas a la víctima para que ejecute códigos que roban sus datos y contraseñas. Estas trampas suelen ser archivos adjuntos o vínculos fraudulentos.

    - Los *scareware* o antivirus falsos aparecen generalmente mediante advertencias que le sugieren a la víctima la descarga de actualizaciones o navegadores que le hacen creer que hay archivos peligrosos y dañados. La connotación *scare* se debe a que atemorizan a la persona hasta que se siente presionada y da clic en el botón "eliminar todas las amenazas" pero en realidad ejecuta el virus.

Ciberseguridad

Las formas presentadas anteriormente suelen ser más comunes, los ciberdelincuentes frecuentemente actualizan la forma de operar y utilizan diversas estrategias, por lo que es recomendable que los usuarios tengan diversas medidas de prevención y alerta para proteger su dinero, así como su identidad digital.

Doble factor de autenticación (2FA). Autenticación reforzada



Fuente: AFI Analistas Financieros Internacionales

En Guatemala no existe una definición legal de identidad digital. En diversos países se ha regulado en favor de la protección de los atributos individuales que describen una entidad (tanto persona natural como jurídica); asimismo, se ha recurrido a elementos como la biometría y otros para brindarle mayor seguridad al usuario. A continuación, podrá observar algunos atributos reconocidos internacionalmente como parte de la identidad digital:

	Personas físicas	Personas jurídicas	Activos
Inherentes	• Edad • Altura • Fecha de nacimiento • Huellas dactilares	• Industria • Situación empresarial	• Naturaleza del activo • Emisor del activo
Acumulados / heredados	• Historial médico • Preferencias y comportamientos	• Registro mercantil • Registro legal	• Historial de propiedad • Historial de transacciones
Asignados	• DNI • Número de teléfono • Dirección de e-mail	• Números identificativos • Juridiscción legal • Directores	• Números identificativos • Custodia

Fuente: AFI Analistas Financieros Internacionales a partir de WEF (2017)

Recomendaciones de seguridad

Todos los participantes en el ecosistema digital deben tomar precauciones para reducir el riesgo de ser víctima de fraudes o estafas.

En Guatemala, el Reglamento para la Administración del Riesgo Tecnológico establece los lineamientos mínimos que los bancos, sociedades financieras, entidades fuera de plaza o entidades *off shore* y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deben cumplir para administrar el riesgo tecnológico.

Para aprovechar las bondades que ofrece la innovación y digitalización de los servicios financieros, es recomendable que los usuarios tengan mecanismos para una sana educación financiera que les permita:

Discernir

Entre comunicaciones reales o maliciosas.

Identificar

Sus necesidades respecto a la gestión de sus finanzas.

Elegir

Productos y servicios financieros acorde a sus necesidades.

Estas son algunas recomendaciones para los usuarios:

Evite atender llamadas de personas que se hacen pasar por "familiares" pidiéndole ayuda.	Conserve la calma y llame directamente a sus familiares.
Por ningún motivo brinde información de contraseñas o cualquier otra información personal mediante llamadas telefónicas, correos electrónicos o por redes sociales.	Memorice sus contraseñas, usuarios y otras claves de acceso.
Evite abrir enlaces a sitios web mediante correos electrónicos no solicitados, si tiene sospechas elimínelos o repórtelos al área de TI de su empresa (si fuera el caso).	Si necesita realizar operaciones por banca en línea o banca telefónica, acceda directamente al navegador o marque directamente el número telefónico.
Por nada guarde contraseñas con las opciones de "recordar contraseña".	Al finalizar sus operaciones, verifique "cerrar sesión".
Evite el acceso a servicios de banca en línea por medio de redes wifi-públicas o poco confiables.	Acceda a sus servicios mediante redes privadas o confiables.

Evite el acceso a cualquier sitio que le llegue por correo electrónico, en especial si no viene de una fuente confiable.	Verifique el sitio web inicia con https:// lo que indica que es seguro o bien que dispone de un certificado digital de seguridad.
Tener desactualizados los antivirus o dar clic en *scareware*.	Procure mantener antivirus reconocidos y actualizados en su computadora y teléfono móvil.
Evite compartir información sobre tokens u otros datos si alguien le llama telefónicamente para pedírselos, puede tratarse de un delincuente que accedió a su cuenta y quiere realizar alguna transferencia.	Al realizar transferencias, adicional al ingreso de usuario y contraseña al inicio, normalmente las entidades solicitan otro medio de seguridad como la generación de un token, coordenadas u otros, después de utilizarlos elimínelos.
Dejarse llevar por el impulso al comprar en línea en cualquier sitio web o red social.	Al realizar compras en línea tenga especial cuidado que el sitio sea seguro y confiable. Además, recuerde llevar un control de los gastos que realiza en línea para evitar sorpresas, cargos inesperados o no poder cubrir los pagos.
Por nada atienda falsas promociones o premios, donde se requiere información confidencial o pagos a cambio de obtener el premio.	Si algo le suena "muy bueno para ser cierto" desconfíe y evite atender cualquier tipo de llamada o mensaje de texto de esa naturaleza.
Evite prestar atención al cuidado de sus documentos, ya que sus datos pueden ser mal utilizados por delincuentes para "robar su identidad". No preste sus documentos personales, tarjetas o números de cuenta.	Preste atención a los lugares donde utiliza sus documentos personales o a quien brinda copias de ellos, ya que contienen información sensible. Con ello evitará ser víctima de fraudes, estafas o lavado de dinero.
Evite consultar periódicamente su historial crediticio.	Consulte periódicamente su historial crediticio para monitorear que la información que aparece corresponda a los créditos en los que sea deudor directo o indirecto.[3] De esa forma podrá detectar si hay alguno no reconocido y realizar las gestiones que corresponda ante el banco o la entidad que reporta el crédito.

3 https://www.sib.gob.gt/web/sib/atencion-al-usuario/record-crediticio

Además, para mantener claves seguras es recomendable que tengan las características siguientes:

1 **Aleatorias:** fácil de recordar, pero no asociada a su vida personal como fechas de nacimiento.

2 **Distintas:** no usar las mismas contraseñas en todas las plataformas o accesos.

3 **Alfanuméricas:** que combinen letras y número o símbolos.

4 **Actualizadas:** cambiar contraseñas periódicamente.

Si cree haber sido víctima de un fraude o estafa se le propone atender lo siguiente:

Comuníquese de inmediato con su entidad financiera, para reportar la situación y bloquear los accesos a sus tarjetas, datos personales, contraseñas u otros. Así reduce el riesgo que terceras personas continúen haciendo mal uso de su información.

Solicite formalmente, mediante los canales que su entidad financiera tenga disponibles y de preferencia si es por escrito, la devolución de los montos en caso se identifique sustracción de dinero o cargos no reconocidos.

Tome nota del número de reporte y en la medida de lo posible del ejecutivo que atendió su solicitud, hora y fecha de presentación.

Realice las denuncias ante las instancias o autoridades correspondientes e indicar detalles como:

- **Fecha en que se identificó el fraude.**
- **Montos sustraídos o cargos no identificados.**
- **Referencias.**

Tendencias

Los mecanismos digitales favorecen el acceso a recursos de educación financiera y a diferentes productos y servicios financieros que pueden beneficiar a los usuarios.

Le presentamos algunas de las tendencias que se esperan con la innovación tecnológica:

Acceso y uso de productos financieros ofrecidos por entidades financieras y tecnológicas de una forma más rápida y sencilla.

Utilización de mecanismos biométricos (como reconocimiento facial, asistentes de voz, huella digital, entre otros que se están desarrollando) y con ello poder acceder a servicios financieros.

Operaciones encriptadas con el objetivo de efectuar retiros de efectivo en cajeros automáticos sin necesidad de llevar consigo la tarjeta, lo que reduce el fraude y la clonación de tarjetas.

Mejorar la gestión de finanzas personales mediante aplicaciones que facilitan la recordación o la realización automatizada, por ejemplo de pagos, ahorros y otros.

Facilitación de la gestión de cuentas, otorgamiento de microcréditos y otros para micro, pequeñas y medianas empresas.

Implementación de Inteligencia Artificial y realidad aumentada para brindar al usuario una experiencia en el uso de los servicios financieros.

Innovación y ciberseguridad

**La Superintendencia de Bancos
con el objetivo de proporcionar una herramienta de consulta y
aprovechar el adecuado manejo de sus finanzas personales,
pone a su disposición el fascículo sobre
Innovación y ciberseguridad.**

**SUPERINTENDENCIA DE BANCOS
Oficina Central
9ª. Av. 22-00 zona 1, Guatemala, C. A.
PBX: (502) 2429-5000
Correo electrónico: info@sib.gob.gt**

Curso de Finanzas Personales modalidad e-learning
www.sib.gob.gt/PortalEF

www.sib.gob.gt SIB Guatemala @sib_guatemala YouTube SuperBancosGuatemala
sib_guatemala Superintendencia de Bancos (SIB)