VISIÓN® Financiera

Revista de la Superintendencia de Bancos (SIB)
Guatemala, junio 2023

Edición
Nro.48
Año 12

Un Sistema Financiero impulsado por la Innovación y Transformación Digital

Pág. 11

Nuevos paradigmas en la industria aseguradora
Pág. 4

Estafas o fraudes por medios tecnológicos *Phishing*
Pág. 23

Pagos digitales y sus riesgos
Pág. 27

www.sib.gob.gt

CONTENIDO

Superintendencia de Bancos
Guatemala, C. A.

"Promovemos la estabilidad y confianza en el sistema financiero supervisado"

Directorio

Superintendencia de Bancos

Oficina central
9.ª Avenida 22-00, zona 1, Guatemala, C. A.

Oficina zona 13
15 avenida 7-18, zona 13, Edificio Zepto, nivel 3, Guatemala, C. A.

info@sib.gob.gt

www.sib.gob.gt

Si desea recibir por correo electrónico esta publicación y otras que divulga la Superintendencia de Bancos, suscríbase:

comunicacion@sib.gob.gt

Al teléfono: (502) 2429-5000 extensiones 1+4330 / 4351

PRESENTACIÓN

Apreciables lectores:

La edición número 48 de la Revista Visión Financiera, presenta, gracias al valioso aporte de connotados expertos y profesionales, una serie de temas de actualidad relacionados con el sistema financiero, particularmente en cuanto a su evolución digital como consecuencia de la innovación en sus servicios financieros; y, el uso de tecnología en el desarrollo de nuevos modelos de negocios.

El tema central, *un sistema financiero impulsado por la innovación y transformación digital*, presentado por el licenciado Gustavo Adolfo Rodas Gómez, Director del Departamento de Normativa de la SIB, trata sobre los principales cambios que ha tenido la banca en materia de innovación en los últimos años derivado de la coyuntura mundial y el avance constante de la misma; aborda el desarrollo digital de las entidades financieras en dos sentidos: el primero orientado hacia la experiencia del usuario; y, el segundo hacia el cambio de los procesos internos de la institución.

Asimismo, se indica que la transformación digital del sistema financiero tiene como reto lograr incrementar la agilidad en los servicios y reducir los costos y riesgos, facilitando una mayor inclusión financiera y servicios personalizados mediante el rediseño en los modelos de negocio.

Como pluma invitada, me es grato presentar al licenciado Guido Monteverde, Director Actuarial en *PRS Prime Re Solutions*, a quien agradezco su valioso aporte como autor del tema: *nuevos paradigmas en la industria aseguradora*, nos comparte que este tipo de industrias está pasando de la gestión del flujo de caja a la gestión del riesgo y de capital, lo que implica un compromiso a largo plazo y una reorganización completa de la estructura de estas compañías.

Reconozco también la importante contribución de los colaboradores de la Superintendencia de Bancos, quienes presentan los artículos siguientes: *leasing y sus riesgos de lavado de dinero*, en donde a la luz del Decreto Nro. 2-2021 del Congreso de la República de Guatemala, Ley de *Leasing*, se analizan los riesgos emergentes, sobre lavado de dinero, que pueden estar asociados al desarrollo del contrato de *leasing*. *Finanzas sostenibles: alerta frente al cambio climático*, que aborda de manera general la interrelación e incidencia en el desarrollo, económico, social y ambiental a largo plazo. *Riesgos de lavado de dinero y financiamiento del terrorismo por activos virtuales*, que expone los riesgos que representan el uso de activos virtuales, así como las medidas prudenciales que organismos internacionales han dictado sobre este particular. *Estafas o fraudes por medios tecnológicos Phishing*, en el cual se aborda una serie de recomendaciones para evitar ciberataques y muestra algunas medidas adoptadas por las entidades financieras para evitar este tipo de estafas.

Finalmente, y no menos importante, se presenta el tema *pagos digitales y sus riesgos*, en donde se comparte sobre el avance en el tiempo de los sistemas de pagos y los diferentes riesgos al realizarlos de manera digital en comercios que utilizan redes sociales y servicios de mensajería digital, entre otros aplicativos, recalcando que la educación financiera y tecnológica juega un papel trascendental para mitigar los riesgos relacionados con estos servicios.

Espero que, dada la relevancia de los temas expuestos, esta edición sea del interés y agrado para el sistema financiero supervisado, usuarios, académicos y público en general.

Atentamente,

Saulo De León Durán
Superintendente de Bancos

Nuevos paradigmas en la industria aseguradora

Guido Monteverde

El desarrollo de la industria aseguradora ha contribuido significativamente a la economía de los países, siendo vital para que los agentes económicos puedan tomar riesgos. Por ello, se hace muy importante contar con industrias aseguradoras solventes.

Hasta hace algunos años, la administración de las compañías aseguradoras se basó en la percepción de la gestión de flujos de caja, por lo que cuando los ingresos por primas y los rendimientos de las inversiones eran mayores al pago de siniestros y los gastos administrativos, la empresa era considerada rentable y, por lo tanto, solvente.

Medidas tradicionales de rentabilidad

Algunas de las medidas tradicionales basadas en este enfoque han sido y siguen siendo el ratio combinado para riesgos generales y el margen de utilidad (o técnico) para riesgos de vida. Ambos indicadores permiten una fácil comparación entre empresas o productos; sin embargo, no reflejan otros aspectos relevantes para la gestión del negocio como son el tiempo de beneficio o pérdida, el costo de capital o el riesgo del negocio.

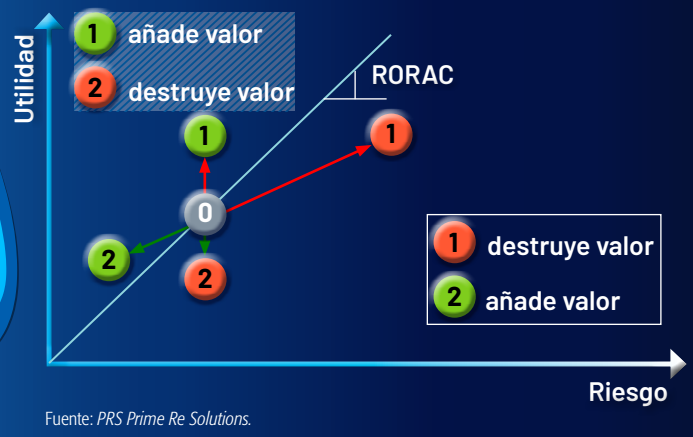
Medidas tradicionales de solvencia

La medida utilizada por los reguladores para evaluar la solvencia de las aseguradoras es el llamado ratio de solvencia, definido como el capital disponible entre el requerimiento de capital. Sin embargo, desde los años 70 utilizando un enfoque contable, también se han realizado mediciones basadas en primas, siniestros o reservas para calcular el requerimiento de capital.

En los últimos años, algunos países han cambiado el paradigma, migrando de un enfoque contable hacia uno basado en riesgos para medir el requerimiento de capital, ejemplos de este cambio son: Europa Occidental con Solvencia II, Suiza con *el Swiss Solvency Test*; México, China, Australia y algunos países de la región como Chile, Perú y Colombia, que vienen trabajando desde hace algún tiempo en sus respectivos modelos basados en riesgos.

Medidas de rentabilidad basadas en riesgo

Una vez que las compañías son requeridas de realizar la medición de solvencia con un enfoque basado en riesgos, se hace muy natural que exista presión para que sus métricas de rentabilidad también sean relativas al nivel de riesgo asumido. Un ejemplo de este tipo de indicador es el llamado RORAC *(Return On Risk-Adjusted Capital)*, el cual es calculado como la utilidad sobre el nivel de riesgo asumido para alcanzar esta. También se puede entender como la utilidad por unidad de riesgo.



Fuente: *PRS Prime Re Solutions.*

Decisiones de negocio en función de RORAC. *En el gráfico de dos dimensiones (utilidad-riesgo), el RORAC referencial es la pendiente que pasa sobre una decisión que representa la situación inicial (estado cero). La decisión uno que está exactamente encima de 0 y la decisión dos que está a la izquierda de cero, añaden valor porque se incrementa la utilidad sin aumentar el riesgo y se reduce la utilidad en menor proporción que la disminución del riesgo, respectivamente. Por otra parte, la decisión dos que está exactamente debajo de cero y la decisión uno que está a la derecha de cero, destruyen valor porque se reduce la utilidad sin disminuir el riesgo y se acrecenta el riesgo sin aumentar la utilidad, respectivamente.*

Decisiones de negocio

Con el enfoque contable, decisiones de negocio como comercializar a través de un nuevo canal de venta, adquirir un *software*, lanzar un nuevo producto o ingresar en un esquema de reaseguros, era analizado mediante los flujos de caja nominales de ingresos y egresos. Sin embargo, el enfoque basado en riesgos permite medir e incorporar el nivel asumido en estas decisiones de negocio. Por ejemplo, una compañía podría escoger

un esquema de reaseguros, luego optimizarlo en función del que obtenga mayor RORAC. También podría decidir lanzar un nuevo producto, únicamente si el RORAC de esa producción fuese mayor a un nivel mínimo aprobado por el directorio de la compañía.

Estructura organizativa

El nuevo enfoque de evaluación de solvencia basado en riesgos implica a su vez un cambio en las estructuras organizativas y claro, en la cultura de riesgo, requiriendo contar en todos los niveles de gestión con un fuerte conocimiento de las políticas y lineamientos, así como de la ejecución de los riesgos clave que enfrenta la organización.

Por ello, se requiere en este nuevo enfoque, tolerancia al riesgo general y apetito al riesgo claramente definidos, que indiquen cuáles tomar y en qué proporción; visión clara del perfil de riesgo general, límites para riesgos individuales a partir de la tolerancia al riesgo general, las preferencias de riesgo y el perfil de riesgo.

Actualmente, gestionar el riesgo significa también gestionar la estrategia de una compañía de seguros. La gestión integral de riesgos se basa en el reconocimiento de que existe un riesgo asociado con cada actividad.

En la mayoría de las empresas tradicionales, el Gerente de Riesgos (*Chief Risk Officer*) reportaba al Gerente Financiero (*Chief Financial Officer*) y su equipo era parte de este último. En la nueva estructura, el Gerente de Riesgos reporta al Director Ejecutivo (*Chief Executive Officer*) y forma parte del Comité Ejecutivo *(Group Executive Committee*). Su equipo es independiente del equipo de finanzas y contabilidad, y es transversal a la organización. El Directorio cuenta, además del Comité de Auditoría, con un Comité de Riesgos. Una consecuencia de este cambio se refleja en el papel de los actuarios, que pasaron de estimar reservas y cotizar pólizas de seguros, a estimar capital y riesgo.

En conclusión, la industria aseguradora está pasando de la gestión del flujo de caja a la gestión del riesgo y del capital. Esto implica un compromiso a largo plazo y una reorganización completa de la estructura de la empresa. A pesar de muchas controversias y escepticismo, el enfoque cuantitativo se está volviendo cada vez más importante. Los modelos internos y los complejos sistemas de Tecnología de la Información (TI) para procesar grandes cantidades de datos se están convirtiendo en actividades centrales. La valoración económica tendrá que evolucionar para tener en cuenta las especificidades de los pasivos de seguros, y sin lugar a duda, la gestión integral de riesgos pronto será parte del ADN de las aseguradoras.

Guido Monteverde
Director actuarial para América Latina de la firma suiza de consultoría actuarial *PRS Prime Re Solutions*

Es *Fully Qualified Actuary* por la Asociación Suiza de Actuarios (SAV). Se graduó como *M.Sc. in Actuarial Science* por la Universidad de Lausana, Suiza; y B. A. *(Bachelor of Arts*) en Economía por la Universidad de Lima, Perú. Su experiencia profesional está relacionada con modelos de reservas, de tarificación de capital económico y regulatorio, así como modelación de riesgos y reaseguros. Se desempeñó como actuario principal en el Departamento de Supervisión Actuarial de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones del Perú. También, se ha desempeñado como Subgerente de Riesgos Técnicos y Jefe Actuarial en Rimac Seguros. Además, es docente de postgrado y dicta diversos talleres de entrenamiento actuarial a instituciones públicas y privadas en Latinoamérica y España.

y sus riesgos de lavado de dinero u otros activos

Lic. Carlos Fernando González Figueroa

El lavado de dinero u otros activos es un delito que busca dar apariencia de legalidad a dinero o bienes obtenidos a través de actividades ilícitas. Esto representa un problema mundial que afecta a las economías y la seguridad de los países. A lo largo del tiempo, las autoridades han adoptado medidas para prevenirlo a través de canales tradicionales; sin embargo, cada vez los lavadores de dinero buscan formas innovadoras para realizar sus actividades, siendo una de ellas el uso de la figura del *leasing*.

El *leasing* es un contrato por el cual un arrendador adquiere bienes para uso de un arrendatario a cambio de una renta o cuota por un plazo determinado de tiempo. Dentro de la legislación guatemalteca se encuentran definidos dos tipos de contratos: de *leasing* financiero y de *leasing* operativo[1].

En el primero existe la opción de compra una vez transcurrido el plazo pactado, el cual es otorgado por el tiempo de vida del activo; mientras que en el segundo, se otorga por un plazo menor al tiempo de vida útil y sin la opción de compra, ya que el mayor interés del arrendador es obtener un máximo provecho de los bienes.

El contrato de *leasing* como instrumento de financiero permite otorgar opciones versátiles a personas individuales o jurídicas para hacer uso de bienes productivos o de inmuebles. El *leasing* es cada vez más relevante en la economía mundial, puesto que existe un beneficio inmediato proporcionado por el bien, el cual no está directamente ligado a una pertenencia obligatoria por parte de quien hace uso de él.

El *leasing* financiero es ofrecido por entidades sujetas o no a un regulador o ente supervisor[2], y presenta diferencias sustanciales respecto a los créditos otorgados por una institución bancaria o financiera, entre ellas, que la compañía de *leasing* posee el activo y conoce su capacidad productiva y el mercado al cual está dirigido. El *leasing* financiero es utilizado ampliamente en el mercado económico de muchos países, expandiéndose a una tasa promedio de 11% anual y centrándose en tres regiones: Asia, Europa y Norteamérica, consolidándose en esta última con el mayor volumen de contratos. En países de América Latina ha presentado un importante crecimiento anual, bajo la expectativa de una mayor cobertura en su portafolio, incluyendo a Guatemala, considerando que últimamente las operaciones financieras de *leasing* ascendieron a USD1.290 millones con la expectativa de que estas puedan incrementarse en los próximos años de un 30 a un 50%[3].

1 Ley de *Leasing*, Decreto Número 2-2021 del Congreso de la República de Guatemala. Art. 2 definiciones, literal c. 1 de marzo de 2021, Guatemala.
2 Se refiere a las autoridades competentes designadas u órganos no gubernamentales responsables de asegurar el cumplimiento por parte de las instituciones financieras.
3 Gamarro U. (12 de febrero de 2021) De qué tamaño es el mercado de *leasing* en Guatemala y cuánto podría crecer con la ley (Prensa Libre).

La oportunidad de crecimiento del mercado de *leasing* en Guatemala se debe, en gran medida, a la entrada en vigencia, a partir del 2 de junio de 2021, de la Ley de *Leasing* contenida en el Decreto Número 2-2021 del Congreso de la República de Guatemala. A través de este instrumento se fortaleció el marco legal en el país, puesto que previo a su emisión no existía regulación específica que otorgara certeza jurídica que incentivara la inversión y que permitiera establecer otras modalidades de créditos para personas individuales y jurídicas.

El aumento proporcional de una actividad económica, sin importar su naturaleza, incrementará el riesgo inherente asociado a esta. Aunado a la posibilidad de que el producto o servicio sea utilizado en actividades ilícitas relacionadas al Lavado de Dinero u otros Activos y al Financiamiento del Terrorismo (LD/FT).

El Grupo de Acción Financiera Internacional (GAFI), por medio del Estándar Internacional sobre la Lucha Contra el Lavado de Activos, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva y las 40 Recomendaciones del GAFI, enfatiza la importancia de la identificación, evaluación y entendimiento de los riesgos a los que en materia de LD/FT están expuestas las actividades y sujetos partícipes en el *leasing*, quienes a su vez deberán adoptar medidas y ejecutar acciones efectivas para mitigar la posibilidad de que sus productos y servicios sean utilizados en actos ilícitos.

> En el caso de Guatemala, la actividad de *leasing* se encuentra regulada dentro del régimen Anti Lavado de Activos y Contra el Financiamiento del Terrorismo (ALA/CFT) toda vez que las personas individuales o jurídicas que la realicen, se encuentren inscritas como Personas Obligadas (PO) ante la Intendencia de Verificación Especial (IVE). A razón de esta inscripción, quienes realicen *leasing* deben establecer programas de cumplimiento y procedimientos destinados a prevenir y controlar el LD/FT en sus operaciones.

Las Personas Obligadas que tengan como actividad comercial el *leasing*, en cualquiera de sus formas, deben considerar las nuevas modalidades y tendencias emergentes de LD/FT; así como identificar el riesgo al cual están expuestas a través de una evaluación propia. Esta debe ser consistente con la identificación del riesgo que desarrolla el país a través de una Evaluación Nacional de Riesgos (ENR) o bien, una Evaluación Sectorial de Riesgos (ESR), lo cual permitirá establecer medidas razonables para contrarrestar las amenazas para este modelo de negocio.

El riesgo emergente que plantea el uso del arrendamiento financiero para actividades de lavado de dinero u otros activos es significativo, puesto que es una herramienta atractiva para los lavadores debido a su simplicidad, versatilidad y las distintas formas de legitimar su uso. Dentro de estos aspectos se deben considerar los escenarios donde el *leasing* se utiliza para la adquisición de bienes utilizando fondos de procedencia ilícita para arrendarlos a terceros, la

falsificación de contratos, la simulación de operaciones comerciales lícitas, la utilización de sociedades de pantalla y la realización de transacciones complejas con otros servicios y productos financieros.

Un ejemplo se encuentra en la tipología del delito identificada por la Unidad de Información y Análisis Financiero de Colombia[4], en la cual para dar apariencia de legalidad al dinero ilícito una organización criminal compra apartamentos o casas a través de apoderados o testaferros, cuya actividad está dentro de la legalidad, y posteriormente los pone en venta mediante el contrato de *leasing*. A continuación, se describen algunas señales de alerta que fueron identificadas.

- Proveedores que venden los bienes sujetos a registro a través de apoderados.
- Proveedores de contrato de *leasing* desconocidos o sin trayectoria comercial.
- Proveedores que no se preocupan por la fecha de su pago, ni por facturar el servicio.
- Proveedores de bienes a entregar en *leasing* que no atienden directamente la compraventa del bien, sino que lo realizan a través de un "tercero apoderado" quien se presenta a formalizar la operación.
- Bienes recientemente adquiridos por montos inusuales (muy por encima o muy por debajo de su valor real).

Como se mencionó anteriormente, ninguna actividad comercial está exenta del riesgo inherente, ya que este no desaparece; no obstante, puede mitigarse mediante una adecuada gestión. Para que este riesgo se minimice es imperante identificar patrones y tendencias delictivas a nivel nacional, regional e internacional; así como instruir a las Personas Obligadas en la formulación de mejores prácticas antilavado y fortalecer la cooperación interinstitucional del sistema de prevención, detección y represión de LD/FT.

El *leasing*, en cualquiera de sus modalidades, representa una ventana de oportunidades para distintos sectores, beneficiando a cada una de las partes que intervienen en este negocio y a la vez aumenta el nivel de riesgo de lavado de dinero u otros activos en su utilización por parte de organizaciones criminales con el objeto de esconder el origen de bienes de ilícita procedencia. En consecuencia, es importante realizar esfuerzos en múltiples niveles en coordinación con las autoridades competentes, las instituciones financieras y la sociedad en general para evitar que este sea utilizado en actividades ilícitas relacionadas al LD/FT.

4 Unidad de Información y Análisis Financiero UIAF (2013), Compilación de Tipologías de Lavado de Activos y Financiación del Terrorismo 2004-2013. Colombia.

Lic. Carlos Fernando González Figueroa
Profesional del Departamento de Tecnología, Analítica e Internacional de la SIB

Licenciado en Ciencias Jurídicas y Sociales, Abogado y Notario por la Universidad Mariano Gálvez de Guatemala; es Magíster en Finanzas por la Universidad Rafael Landívar. Evaluador Certificado por el Grupo de Acción Financiera de Latinoamérica (GAFILAT) sobre la Metodología de Evaluación del Grupo de Acción Financiera Internacional (GAFI), en los Estándares Internacionales de LD/FT/FPADM. Posee experiencia como docente en la Escuela de Estudios de Postgrado de la Facultad de Ciencias Económicas de la Universidad de San Carlos de Guatemala.

UN SISTEMA FINANCIERO IMPULSADO POR LA INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

Lic. Gustavo Adolfo Rodas Gómez

En Guatemala el sistema financiero supervisado está conformado por 94 instituciones, entre las que se encuentran bancos, sociedades financieras, almacenes generales de depósito, compañías de seguros, casas de cambio, entidades fuera de plaza, casas de bolsa, entidades emisoras de tarjetas de crédito que forman parte de un grupo financiero, entidades de microfinanzas, entre otras. La banca guatemalteca representa aproximadamente el 93% del total de activos del sistema financiero supervisado en su conjunto.

Algunos datos importantes de conocer en la banca guatemalteca y de cómo ha logrado facilitar la inclusión financiera, se relacionan con la existencia de 33 mil puntos de acceso que incluyen agencias, agentes bancarios y cajeros automáticos, permitiendo que todos los municipios del país cuenten con alguno de estos. Los bancos guatemaltecos cuentan con banca electrónica y aplicaciones móviles, existen más de 4,200 cajeros con presencia en el 75% de los municipios, el uso de tarjetas de crédito sin contacto y de relojes inteligentes que pueden ser vinculados con medios de pago y la facilidad que ofrecen muchas de estas instituciones de apertura de cuentas 100% digital y en pocos minutos. Lo anterior evidencia que la banca guatemalteca ha incursionado en servicios innovadores y que la misma avanza constantemente.

Este proceso de innovación y transformación, guarda relación con los cambios generacionales y tecnológicos que existen en la actualidad, cobrando mayor relevancia en aquellos países con poblaciones jóvenes, quienes tienen preferencia por la tecnología, siendo Guatemala un país privilegiado por contar con una población altamente joven.

La transformación digital de las entidades financieras debe realizarse en dos sentidos: el primero orientado hacia afuera, es decir, se relaciona con la experiencia del consumidor; y, el segundo, hacia adentro, que guarda estrecha relación con la transformación de los procesos internos de la institución.

1

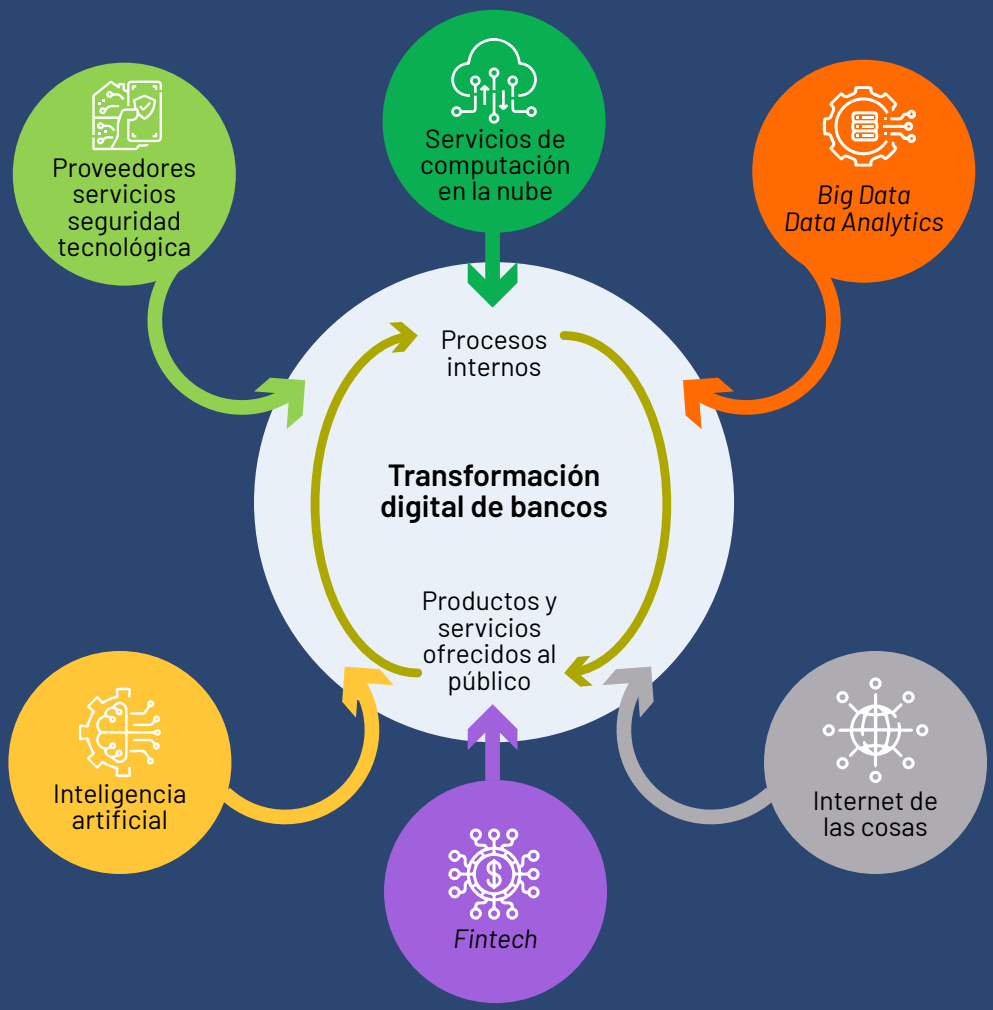
El primero, está enfocado al usuario para que pueda obtener servicios eficientes, personalizados y adaptados a sus necesidades. Las entidades deben considerar que las nuevas generaciones buscan menos fricción en las transacciones, menor tiempo en la realización de gestiones y una mayor seguridad con sus datos, todo ello puede verse beneficiado mediante la aplicación de tecnologías utilizadas desde el dispositivo móvil o computador, evitando ir de manera presencial a una sucursal para realizar estas operaciones.

2

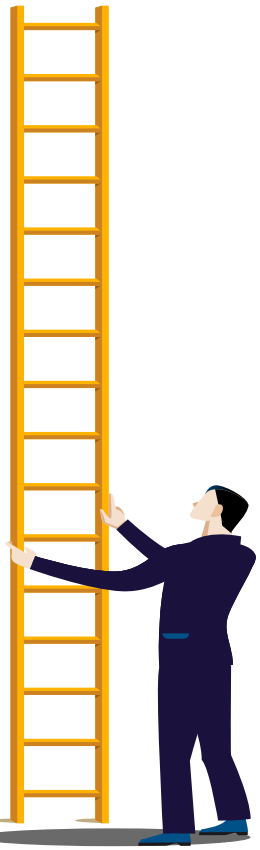
El segundo, inicia con una visión clara del gobierno corporativo, en cuanto al compromiso que adquieran y luego ser permeado en toda la organización, facilitando la reingeniería en los procesos, para luego sistematizar y posteriormente automatizar los mismos, lo que permitirá una profunda transformación digital. Para ello, las instituciones tienen que desarrollar nuevas políticas y procedimientos que permitan de forma clara adoptar nuevas tecnologías y utilizar recursos disruptivos que faciliten la versatilidad de la gestión. Esta experiencia suele ser laboriosa y en algunos casos hasta traumática, ya que no es posible que todos puedan adaptarse al cambio que requiere el nuevo entorno, ya que en la mayoría de los casos se deben romper paradigmas y eliminar algunas cuotas de poder originadas por el desorden, la concentración y custodia de procesos, datos y decisiones.

Todo proceso de transformación digital requiere un ordenamiento y estructuración de lo que se hace, es decir, no se puede mejorar algo cuando no se tiene clara certeza de qué se está haciendo y cómo se está realizando una actividad. Para ello, el papel de la gobernanza de datos y de los BPM (*Business Process Management*) juegan un papel fundamental y orientativo en el reemplazo de sistemas y procesos heredados, ya que permite gestionar y adoptar una serie de pasos que modifican la forma de trabajar de la entidad con el objetivo de mejorar los procesos y facilitar la colaboración con un enfoque orientado hacia los grupos de interés (*stakeholders*), permitiendo ver aquellos cuellos de botella que impiden avanzar y reducir tiempos.

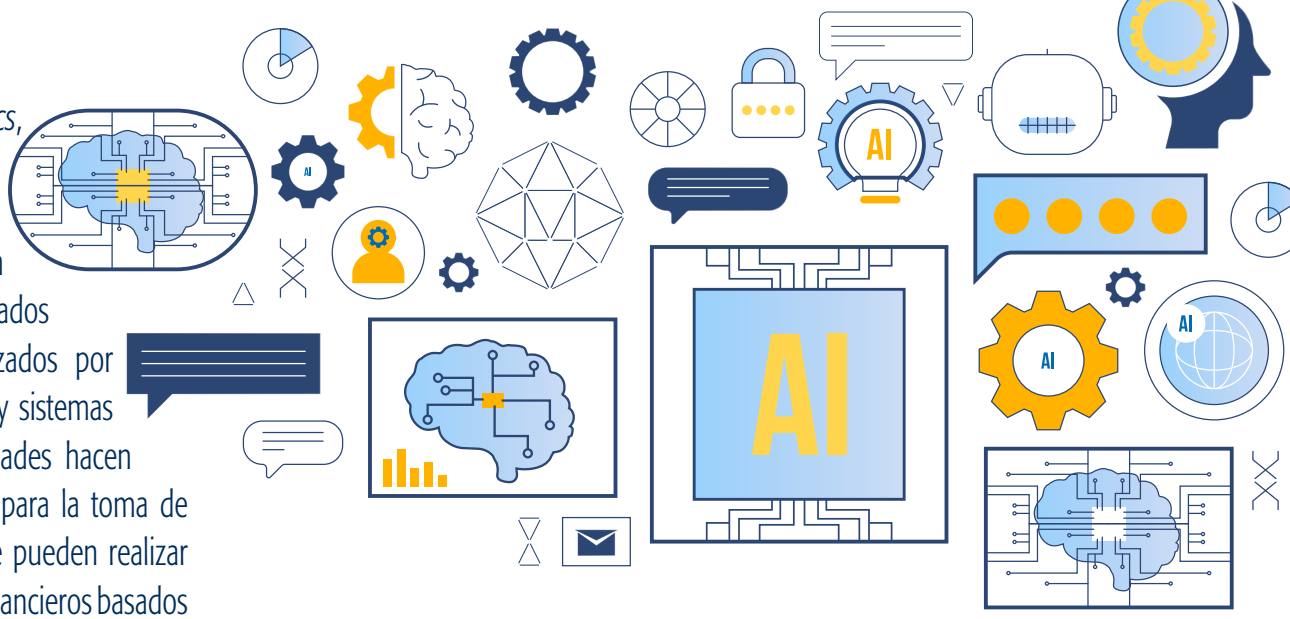
Existen por lo menos seis mecanismos que facilitan la innovación y transformación digital del sistema financiero y que constituyen retos para su adecuado funcionamiento. A continuación, se detallan los aspectos siguientes:



Fuente: elaboración propia del autor.



El mecanismo inicial de una adecuada transformación digital requiere de seguridad tecnológica, esto permite acceder a redes como el internet y contratar servicios de terceros para procesamiento y almacenamiento de información, es decir, el uso de la nube. Sobre este particular la Junta Monetaria, a propuesta de la Superintendencia de Bancos, emitió la Resolución JM-104-2021 que contiene el Reglamento para la Administración del Riesgo Tecnológico, con lo cual se sientan las bases normativas que permiten ser el punto de partida de la transformación digital.



Big Data y *Data Analytics*, se refieren al uso de grandes volúmenes de datos que pueden ser generados, analizados y cada vez más utilizados por herramientas digitales y sistemas informáticos. Las entidades hacen uso de muchos datos para la toma de decisiones, con esto se pueden realizar análisis y pronósticos financieros basados en un cúmulo de datos históricos. Por otra parte, el Internet de las cosas (IoT) permite la interconexión de dispositivos físicos, que tienen integrados dispositivos electrónicos, *software*, sensores e interruptores, así como la conectividad de la red que permite que estos objetos recolecten e intercambien datos.

No debemos olvidar el papel de las entidades que ofrecen servicios financieros basados en tecnología conocidas como *Fintech*, estas instituciones tienen capacidad para generar nuevos modelos de negocio, y también de interactuar con las instituciones financieras para proveerles servicios y aplicaciones que coadyuven en su proceso de transformación digital; finalmente, pero no menos importante resulta el papel que ahora tiene la Inteligencia Artificial (IA), la cual hace referencia a sistemas informáticos que realizan funciones precisando capacidades humanas. La inteligencia artificial puede hacer preguntas, generar respuestas, formular y probar hipótesis, así como tomar decisiones de forma automática basadas en análisis avanzados de conjuntos de datos muy amplios.

En conclusión, la transformación digital del sistema financiero tiene como reto lograr incrementar la agilidad en los servicios, reducir costos y considerar riesgos, facilitando una mayor inclusión financiera y servicios personalizados mediante el rediseño en los modelos de negocio.

Lic. Gustavo Adolfo Rodas Gómez
Director del Departamento de Normativa de la SIB

Contador Público y Auditor egresado de la Universidad de San Carlos de Guatemala, con Maestría en Administración de Negocios con orientación en Dirección Estratégica por la Universidad Mesoamericana. Certificado en Ciberseguridad emitido por Némesis de España, Asociación de Supervisores Bancarios de las Américas (ASBA), Club de Gestión de Riesgo de España y Federación Latinoamericana de Bancos; y, como Experto en Innovación emitida por *International Bureau of Knowledge and Innovation (IBKIN)*. Actual Coordinador del Comité *FinTech* por el Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO); es el representante por parte de la Superintendencia de Bancos en el Foro *Fintech* del Centro de Estudios Monetarios Latinoamericanos (CEMLA) y ante la red ecosistema *Fintech* en América Latina y el Caribe (*FintechLAC*). Fue coordinador del Comité Técnico de Implementación de la Estrategia Nacional de Inclusión Financiera (ENIF); miembro de la Mesa Técnica de Identificación de Infraestructuras Críticas para la Seguridad de la Nación; y, coordinador de campo para la Mesa Técnica para Fortalecer el Crédito en Bancos Públicos en los que el Estado tiene participación dirigida por la Vicepresidencia de la República; representó a Guatemala ante el Banco Central de España en el Modelo de Supervisión Basado en Riegos (*SupTech*, por sus siglas en inglés). Dentro del área académica ha sido docente universitario durante 25 años. Ha desarrollado su carrera profesional en la Superintendencia de Bancos por más de 20 años, ocupando cargos como Inspector Bancario, Supervisor; y, Asesor de la Intendencia de Estudios y Normativa.

Finanzas sostenibles: alerta frente al cambio climático

Lcda. Flor de María Herrera Palacios

En los últimos años se ha incrementado el interés a nivel global por el cambio climático y las finanzas sostenibles, derivado de su interrelación e incidencia en el desarrollo económico, social y ambiental a largo plazo, siendo relevante la contribución que cada sector realiza para lograr que dicho proceso sea sustentable.

Las finanzas sostenibles parten del concepto de desarrollo sostenible[1] que se origina en 1987 en el informe de la Comisión Mundial sobre el Medio Ambiente y el Desarrollo[2], luego hubo un primer punto de inflexión en 1992 en la Cumbre de la Tierra en Río de Janeiro donde se resaltó la importancia de transformar las finanzas como un aspecto clave para alcanzar el desarrollo sostenible; se impulsó la Iniciativa Financiera del Programa de Naciones Unidas para el Medio Ambiente (UNEP FI); y, se lanzó la Declaración de Compromiso de las Instituciones Financieras sobre el Medio Ambiente y el Desarrollo Sostenible, en la que estas entidades reconocieron su rol para que la economía y estilos de vida sean sostenibles y se comprometieron a integrar en sus operaciones los factores o criterios ambientales y sociales.

Sin embargo, el momento significativo fue en 2015, cuando 196 países (incluyendo Guatemala) firmaron el Acuerdo de París[3], en el que se comprometieron a combatir el cambio climático y adaptarse a sus efectos, aspectos esenciales para lograr los Objetivos de Desarrollo Sostenible (ODS); dicho acuerdo brinda una hoja de ruta de las medidas necesarias para reducir las emisiones de gases de efecto invernadero y aumentar la resiliencia al cambio climático, impulsando y requiriendo la sostenibilidad en todos los ámbitos, entre estos, las finanzas.

1 Se define como "la satisfacción de las necesidades del presente sin comprometer la capacidad de las generaciones futuras para satisfacer sus propias necesidades".

2 En 1987 se publicó el informe de la Comisión Mundial sobre el Medio Ambiente y el Desarrollo de las Naciones Unidas, titulado "Nuestro Futuro Común", conocido como Informe Brundtland.

3 Acuerdo internacional sobre el cambio climático jurídicamente vinculante, cuyo objetivo principal es limitar el aumento de la temperatura global muy por debajo de 2° centígrados, de preferencia a 1.5° centígrados y reducir las emisiones de gases de efecto invernadero, para lograr un planeta con clima neutro para mediados del siglo. Disponible en <https://unfccc.int/es/acerca-de-las-ndc/el-acuerdo-de-paris>

¿Qué son las finanzas sostenibles?

El Fondo Monetario Internacional[4] (FMI) se refiere a las finanzas sostenibles como *"la incorporación de principios ambientales, sociales y de gobernanza (ASG) en las decisiones comerciales, el desarrollo económico y las estrategias de inversión"*, indicando que la falta de gestión en los factores ASG expone a los sectores financieros a riesgos de pérdidas asociadas al cambio climático, lo cual puede afectar a la estabilidad financiera de los países. A continuación se describe el alcance de las finanzas sostenibles.

Fuente: elaboración propia del autor.

4 Informe sobre la estabilidad financiera mundial de 2019. Disponible en <https://www.imf.org/en/Publications/GFSR/Issues/2019/10/01/global-financial-stability-report-october-2019#Chapter6>

Considerando la amplitud del concepto de finanzas sostenibles, se presentan los factores o criterios ASG, con los temas asociados a estos y ejemplos de algunos elementos a considerar en la gestión del riesgo climático:

Factor	Tema	Aspectos clave	
Ambiental Considera las acciones que tienen impacto medioambiental directa o indirectamente	Cambio climático	✓ Huella de carbono	✓ Vulnerabilidades a los eventos de cambio climático
	Recursos naturales	✓ Eficiencia energética ✓ Abastecimiento de materias primas	✓ Eficiencia de agua ✓ Uso de la tierra
	Contaminación y residuos	✓ Emisiones tóxicas ✓ Manejo de aguas residuales ✓ Manejo de materiales peligrosos	✓ Calidad del aire ✓ Manejo de residuos electrónicos
	Oportunidades y política	✓ Energía renovable ✓ Tecnología limpia	✓ Edificios verdes ✓ Metas ambientales y de biodiversidad e inversión
Social Prácticas empresariales que afectan a la sociedad	Capital humano	✓ Salud y seguridad laboral ✓ Oportunidades de desarrollo	✓ Diversidad e igualdad laboral ✓ Prácticas laborales con salarios y condiciones de trabajo dignos
	Responsabilidad social del producto	✓ Seguridad y calidad del producto ✓ Prácticas de venta y etiquetado del producto	✓ Privacidad del cliente y seguridad de datos ✓ Acceso a productos
	Relaciones	✓ Comunidad ✓ Gobierno	✓ Derechos humanos
Gobernanza Gestión de la gobernanza, transparencia y administración de la empresa	Gobierno corporativo	✓ Estructura de la junta y rendición de cuentas ✓ Prácticas contables y de divulgación	✓ Compensación de ejecutivos y eficacia de la gestión ✓ Propiedad y derechos de los accionistas
	Comportamiento corporativo	✓ Gestión de la corrupción ✓ Gestión de riesgos sistémicos ✓ Calidad de las ganancias	✓ Ética empresarial ✓ Gestión del entorno empresarial ✓ Transparencia fiscal y operaciones vinculadas

Fuente: elaboración propia del autor, considerando el Informe de Estabilidad Financiera Global del FMI, octubre 2019.

El sector financiero desempeña un rol fundamental para afrontar los retos ambientales y sociales, por lo cual diversas instituciones apoyan la transición hacia una economía con bajas emisiones de carbono, siendo relevante considerar para el efecto, entre otros aspectos, los principios y mejores prácticas emitidos con el fin de promover la implementación de las finanzas sostenibles y la gestión del riesgo climático.

Al respecto en 2003, surgen los Principios del Ecuador[5], un marco de gestión de riesgos adoptado por instituciones financieras para determinar, evaluar y gestionar el riesgo ambiental y social en la financiación de proyectos, brindando un estándar mínimo de diligencia debida para la toma de decisiones de riesgo de manera responsable.

Posteriormente, en 2019 la ONU divulgó los Principios de Banca Responsable[6], los cuales cuentan con más de 300 bancos signatarios, que representan casi la mitad de la industria bancaria del mundo.

5 Disponible en <https://equator-principles.com/app/uploads/EP4_Spanish.pdf>

6 Disponible en <https://www.unepfi.org/wordpress/wp-content/uploads/2022/07/PRB-Guidance-Document-Spanish-Principios-Para-La-Banca-Responsable-Documento-Guia.pdf>

Dichos principios brindan a la banca un marco que incorpora la sostenibilidad con el alineamiento estratégico de las entidades, para que sea coherente y contribuya con los ODS y el Acuerdo de París.

Los principios mencionados, sentaron las bases para la emisión de estándares internacionales sobre finanzas sostenibles, como: los "Principios para la gestión y supervisión efectiva de los riesgos financieros relacionados con el clima"[7], publicados por el Comité de Supervisión Bancaria de Basilea en junio de 2022, que buscan mejorar la gestión de riesgos en la materia; y, las normas ISO 14001, que establecen los criterios para un sistema de gestión ambiental. Paralelamente, derivado del creciente interés en el desarrollo sostenible, han surgido alianzas, asociaciones, redes, comisiones y grupos de trabajo entre bancos centrales, órganos supervisores, entidades financieras, así como acuerdos con organismos internacionales, para apoyar la implementación de los referidos principios y normas.

En esa línea, a nivel global el sector financiero desempeña un rol relevante en el impulso de las finanzas sostenibles, al ser un agente que apoya decisiones de inversión que incidan en el alcance de los objetivos de desarrollo sostenible y la reducción de las emisiones de carbono; todo ello, acompañado de la implementación de las mejores prácticas que induzcan a fortalecer la transparencia, garantizar la incorporación de los criterios ASG y la consideración del riesgo climático en la gestión integral de riesgos, a efecto de contribuir a preservar la estabilidad financiera.

En conclusión, es evidente que el cambio climático es un desafío a nivel global, respecto del cual, si no se adoptan las medidas oportunas para mitigarlo, podría tenerse implicaciones ambientales y consecuencias onerosas e irreversibles no solamente para las empresas, si no para la humanidad en general; por lo que, se requieren medidas integrales y la participación colectiva y coordinada de todos los sectores de la sociedad. Entre dichas medidas se encuentran la gestión de los factores ASG, que promuevan las finanzas sostenibles con el propósito de reducir los efectos negativos derivados del cambio climático, así como crear oportunidades de negocios sostenibles.

7 Disponible en <https://www.bis.org/bcbs/publ/d532.pdf>

Lcda. Flor de María Herrera Palacios
Supervisor del Departamento de Supervisión de Riesgos Específicos de la SIB

Contadora Pública y Auditora, con Maestría en Administración Financiera, ambos títulos otorgados por la Universidad Mariano Gálvez de Guatemala. Posee Certificación en Ciberseguridad y Riesgo Operacional otorgada por Némesis-España. Capacitación en Finanzas Sostenibles para Reguladores realizada por *Green Banking Academy (GBAC) e International Finance Corporation (IFC)*. Con estudios del Programa Internacional de Especialización en Finanzas y Administración de Riesgos, organizado por la Superintendencia de Bancos, Seguros y AFP del Perú.

RIESGOS DE LAVADO DE DINERO Y FINANCIAMIENTO DEL TERRORISMO POR ACTIVOS VIRTUALES

Lcda. Karen Celenia Pivaral Rodríguez

Los activos virtuales y los servicios que se relacionan con estos tienden a obtener mayor auge o participación en el mundo del negocio financiero, bajo el supuesto de que tienen el potencial de estimular la eficiencia e innovación, así como promover mejor la estrategia de inclusión financiera, considerando entre otros aspectos, que estos han sido utilizados como una estrategia de cobertura inflacionaria y representan opciones de bajo costo en las transacciones internacionales. Según el Grupo de Acción Financiera Internacional (GAFI), un activo virtual *es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los activos virtuales no incluyen representaciones digitales de moneda fiat, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI* [1].

1 Glosario General Recomendaciones del GAFI, actualización a julio de 2022.

Bajo ese contexto, los activos virtuales, conocidos como criptomonedas, crean nuevas oportunidades para que lavadores de dinero o personas que se dedican a recolectar fondos para financiar actos terroristas, puedan realizar operaciones a través de estos instrumentos considerando que poseen características como el rápido movimiento de fondos, incluyendo modalidades transfronterizas, anonimato, almacenamiento digital fuera del sistema financiero regulado así como el ocultamiento del origen o destino de los fondos, lo cual dificulta a las Personas Obligadas a identificar transacciones sospechosas oportunamente. Al respecto, el GAFI en 2018 realizó una actualización de sus estándares -Las Recomendaciones del GAFI- en las que en su Recomendación 15 incluye lo referente a estas nuevas tecnologías; adoptando en junio de 2019, una nota interpretativa hacia esta misma recomendación con el propósito de enfatizar sobre los requisitos de aplicación e implementación de actividades relacionadas con activos virtuales y los proveedores de estos.

Es preciso indicar que las medidas que el GAFI requiere que los países implementen se derivan de los riesgos identificados en la utilización de criptomonedas en delitos relacionados con lavado de dinero, como la venta de sustancias controladas, artículos ilegales, fraude, evasión fiscal, ataques cibernéticos que resultan en robos o secuestro de archivos o información, explotación infantil, trata de personas y financiamiento del terrorismo. Cabe comentar que, el uso indebido que puede darse a los activos virtuales puede combinarse con transacciones que involucran al sistema financiero regulado, y a su vez desarrollarse a través de entidades público-privadas, lo que genera procesos cíclicos y evolutivos que tienden a presentar mayores exposiciones subyacentes de sus clientes, productos y operaciones, aumentando así los riesgos convencionales. En este contexto se deben considerar los aspectos siguientes:

Volumen y frecuencia de las operaciones

En los últimos años la utilización de las criptomonedas ha cobrado importancia en el público, de la misma forma su utilización se ha popularizado en el mundo criminal. De esa cuenta, el uso indebido de estas nuevas "representaciones digitales de valor" tienden a menudo a ser parte de la etapa de estructuración del lavado de dinero, puesto que dan lugar a cambios o transferencias entre distintos tipos de criptomonedas, realizando múltiples operaciones en sucesiones breves, con patrones escalonados, a cuentas recién creadas o inactivas, así como la conversión de activos virtuales en múltiples tipos, sin que importen las tarifas de conversión que den lugar a explicaciones comerciales lógicas. Los activos virtuales permiten realizar transferencias a múltiples proveedores registrados o que operan en otras jurisdicciones lo que eleva contingencias como la falta de relación de domicilios donde reside el cliente o donde realiza sus transacciones.

Experiencias internacionales revelan que los activos virtuales han sido utilizados a través de compras de grandes cantidades de estos, por parte de varias personas en los que en la mayoría compartieron una misma dirección de residencia y la tendencia es dada a que las transacciones se realizaron desde un mismo protocolo de internet (IP). En estos casos el dinero fiduciario para la compra de activos virtuales es ingresado en efectivo a distintas cuentas constituidas en instituciones financieras dando lugar a una posible esquematización de uso de "mulas" por parte de los lavadores de dinero para el blanqueo de sus ganancias ilícitas.

Operaciones relativas a los usuarios

No es secreto el hecho de que el crimen organizado utiliza y crea plataformas en redes sociales como medio para el reclutamiento de personas "mulas" (las personas creen estar realizando una actividad para la cual fueron reclutados; sin embargo, el lavador disfraza la actividad criminal que realizará el reclutado, haciéndolas en muchos casos víctimas de la propia red criminal) para lograr el objetivo de lavar ganancias procedentes de actividades ilícitas. Puede darse el caso de que cuentas constituidas en instituciones financieras realicen operaciones incompatibles con el perfil del titular de la cuenta; por ejemplo, que un joven universitario reciba múltiples depósitos de naturaleza comercial de distintas personas y que posteriormente el mismo utilice los recursos depositados para transferirlos inmediatamente hacia cuentas de proveedores de activos virtuales para compra de estos, transfiriéndolos posteriormente a otras jurisdicciones.

Favorecimiento del anonimato

Las características inherentes y las vulnerabilidades asociadas a las tecnologías de los activos virtuales aumentan el anonimato, lo que en ocasiones obstaculiza la detección de actividades delictivas, lo anterior hace que los activos virtuales sean atractivos para las organizaciones criminales para el ocultamiento y almacenamiento de sus recursos. Por eso, es preciso prestar especial atención a aquellas situaciones en las que un activo virtual que opera en una cadena de bloques pública y transparente pase a un intercambio centralizado e inmediatamente después este se convierta a una criptomoneda que propicia el anonimato o es catalogada como privada. Por su parte aquellos clientes que operen con proveedores de servicios de activos virtuales (VASP, por sus siglas en inglés)[2] no registrados, sin licencias de sus sitios web de intercambio (*peer to peer*), así como usuarios que ingresen a plataformas de VASP usando direcciones de IP asociadas a una red oscura o *softwares* de similar naturaleza que permitan comunicaciones anónimas, por ejemplo, accesos a través de mecanismos *proxies* que censuren o supriman los nombres de dominio así como sus propietarios, podrían constituir una mayor exposición a riesgos asociados al lavado de dinero o financiamiento del terrorismo.

Cabe resaltar que, existen posibilidades de que una gran cantidad de carteras de activos virtuales pueden haber sido constituidas como carteras pantalla, con el propósito de que las mismas sean utilizadas por diferentes usuarios desde una misma dirección de IP, con el fin de ocultar su relación entre sí.

Finalmente, resulta de vital importancia la implementación de un enfoque basado en riesgos de forma oportuna, dadas las distintas situaciones que pueden implicar el uso de activos virtuales en actividades de lavado de dinero o financiamiento del terrorismo, prestando especial atención en la consideración de aplicación de medidas de debida diligencia intensificadas en cuyo caso se identifiquen exposiciones a riesgos mayores, tomando en cuenta el propósito de la relación comercial que el cliente desea establecer con la PO, tipo de producto o servicio contratado, el perfil económico financiero que se establezca para el cliente, así como la congruencia que exista entre estos.

2 *Virtual Assets Services Provider*

Lcda. Karen Celenia Pivaral Rodríguez
Inspector del Departamento de Prevención y Cumplimiento de la SIB

Administradora de Empresas egresada de la Universidad Mariano Gálvez de Guatemala, con Maestrías en Administración de Negocios, Desarrollo y Evaluación de Proyectos; y, Dirección Financiera títulos otorgados por las universidades Mariano Gálvez de Guatemala y Da Vinci de Guatemala, respectivamente. Posee experiencia en supervisión de entidades financieras, desarrollo e implementación de metodologías para supervisar y administrar los riesgos de Lavado de Dinero y Financiamiento del Terrorismo (LD/FT), ha sido certificada como Profesional Internacional Experto en Sistemas de Prevención AML/CFT por WCA. Docente en la Facultad de Ciencias Administrativas y Comerciales de la Universidad Da Vinci de Guatemala.

Estafas o fraudes por medios tecnológicos *Phishing*

Lic. Hugo Gerardo Cervantes Grajeda

Las estafas o fraudes por medios tecnológicos consisten en engañar a las personas para obtener algún beneficio para el atacante, en la mayoría de los casos dinero o datos personales de las víctimas. Estos delitos los realizan haciendo uso de redes públicas como es el caso de internet, infraestructuras internas en las organizaciones, redes sociales, correo electrónico, teléfono o cualquier otro dispositivo electrónico que transporte o almacene información. Estas estafas o fraudes, afectan a individuos, empresas, entidades de gobierno o cualquier organización, y pueden causar graves pérdidas económicas, robo de información, daños a la reputación, entre otros. Dentro de estas estafas, se identifican actividades falsas como: préstamos, tiendas en línea, alquileres, soporte técnico, ofertas de empleo, chantajes con supuesta información personal (perfiles), compraventa de productos, entre muchos más. Para que los delitos o fraudes cibernéticos se concreten, se requiere hacer uso de la ingeniería social, siendo la técnica más utilizada el *phishing*.

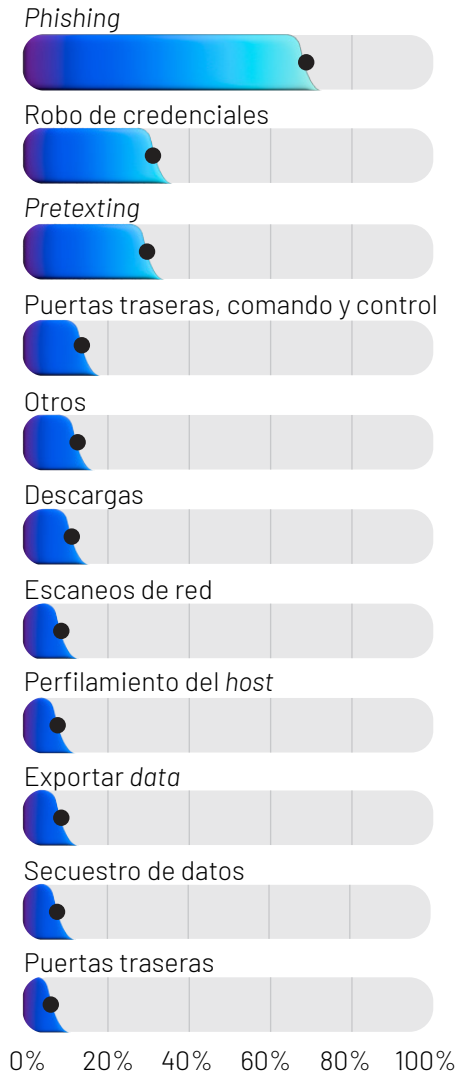
El Instituto Nacional de Normas y Tecnología estadounidense (NIST, por sus siglas en inglés), define *phishing* como:

> *Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza*[1]

Es razonable que esta definición describa los datos de cuentas bancarias como confidenciales, ya que el sector financiero y sus usuarios son los objetivos más atractivos para los cibercriminales para ejecutar este tipo de ataques e intentos de fraude, como lo demuestra el más reciente informe sobre las investigaciones de fugas de datos publicado por la empresa Verizon[2], estableciendo como una de sus principales conclusiones, que el principal motivador de los ataques externos es el financiero; también menciona que en el 82% de las fugas de datos interviene el factor humano, asimismo indica que el *phishing* sigue siendo el método de ataque preferido por los cibercriminales haciendo uso de la ingeniería social, reflejando que los ataques de *ransomware* (secuestro de datos) han aumentado un 13% en los últimos cinco años, dicho ataque inicia generalmente con correos maliciosos.

Adicionalmente al *phishing*, la ingeniería social cuenta con otros tipos de ataque, cada vez mejor elaborados, difíciles de prevenir y detectar, por ejemplo los siguientes: estafas dirigidas a empleados clave o de alto nivel desde direcciones de *email* que parecen ser legítimas para estafar a otros miembros de la organización; intentar redirigir a los usuarios a un sitio web falso para robar datos personales como usuario, contraseñas, preguntas de seguridad, etc.; suplantación de identidad, a diferencia del *phishing* normal, el atacante ya tiene conocimiento previo de la víctima que lo hace más peligroso; fraude dirigido específicamente a directores ejecutivos o financieros pretendiendo obtener autorizaciones falsas sobre grandes transferencias o sumas de dinero; violación a la seguridad física accediendo a un área no autorizada aprovechando la cortesía humana; uso de mensajes de texto falsos para descarga de *malware* u otro *software* malicioso; llamadas telefónicas falsas o mensajes de voz tratando de obtener información sensible y útil para el atacante.

MÉTODOS EMPLEADOS EN ATAQUES CON INGENIERÍA SOCIAL



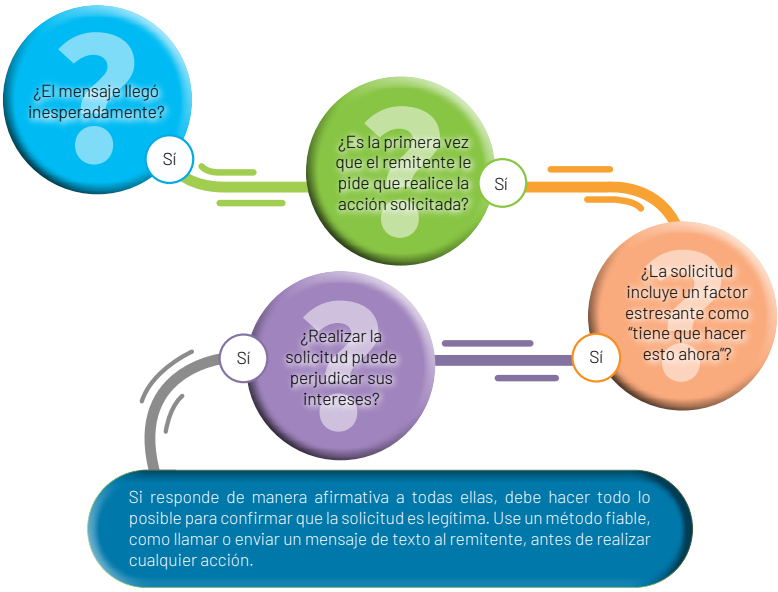
Fuente: *Data Breach Investigations Report (DBIR) 2022.*

Como se mencionó, las formas, medios y técnicas para realizar este tipo de ataques son muchas, lo cual nos lleva a la siguiente pregunta: ¿qué debemos hacer para protegernos? En ediciones anteriores de esta revista[3] menciona que el actual Reglamento para la Administración del Riesgo Tecnológico, Resolución JM-104-2021, aprobado por la Junta Monetaria, cuenta con los requerimientos mínimos regulatorios

1 *Phishing, https://csrc.nist.gov/glossary/term/phishing*
2 *2022 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/*
3 Revista Visión Financiera - SIB Edición 45, https://www.sib.gob.gt/web/sib/comunicacion_institucional/revista-vision_financiera

para encaminar y direccionar a las entidades financieras supervisadas a la implementación de controles y medidas para identificar, proteger, detectar, responder y recuperarse ante un eventual ataque cibernético, a través de prácticas esenciales como: protección a través del control y autorización de acceso, programas de capacitación y concientización, adecuada gestión de la infraestructura tecnológica, identificación de capacidades internas, plan de respuesta a incidentes, adecuados contratos con los proveedores de servicios, identificación de oportunidades de mejora, entre otras. Adicionalmente, dicha normativa se vale de estructuras establecidas en las entidades financieras, como el Consejo de Administración, el Comité y Unidad de Gestión de Riesgos; asimismo en aspectos de ciberseguridad es necesario que las entidades supervisadas cuenten con al menos un CISO (*Chief Information Security Officer*), un SOC (*Security Operation Center*), y un CSIRT (Equipo de Respuesta a Incidentes de Seguridad). La adopción y cumplimiento de estas medidas por parte de las entidades propician un ecosistema financiero con niveles de ciberriesgo aceptables; sin embargo, es importante recordar que no es suficiente contar con toda esta cadena de protección, ya que en todos los casos de ingeniería social o *phishing* está involucrado el factor humano, siendo este el más vulnerable.

CONSIDERACIONES SOBRE FRAUDES O ESTAFAS

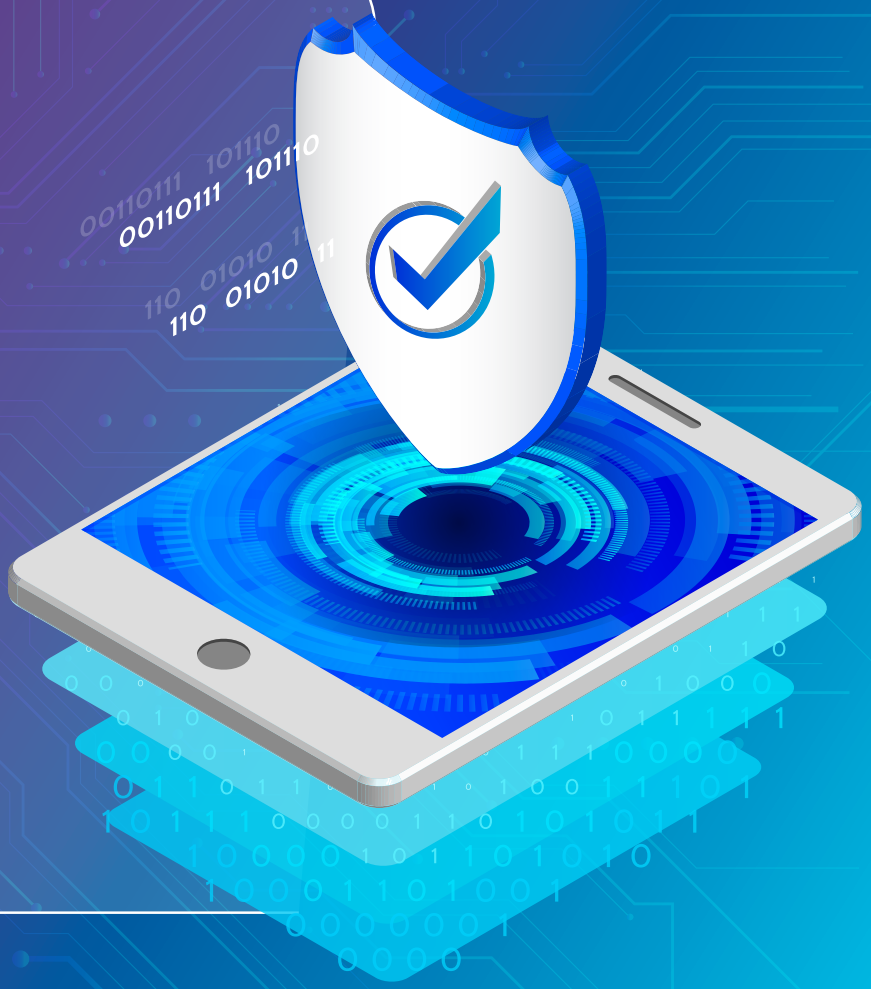


Fuente: *KnowBe4.*

SUGERENCIAS PARA NO CAER EN ESTAFAS O FRAUDES

No abra, ni descargue archivos adjuntos sospechosos o inesperados, valide antes de hacer clic, deténgase, observe y piense; no comparta información personal o financiera a través de ningún medio, hágalo solo en sitios seguros, verifique que este inicie con https://; mantenga actualizados y protegidos sus dispositivos; ante cualquier duda consulte y comuníquese inmediatamente con su soporte técnico.

Finalmente, lo expuesto evidencia la relevancia del factor humano, esto debe llevar a las entidades financieras u otras organizaciones a reflexionar que el comportamiento humano es algo sumamente complejo de gestionar, ya que involucra conductas, emociones, reacciones y estas están influenciadas por factores psicológicos, sociales y culturales, y se vuelve preponderante que existan programas formales de concientización y capacitación que incluyan campañas con contenido adecuado a cada grupo objetivo en concordancia a su contexto y circunstancias. El usuario debe conocer exactamente cómo reaccionar y a dónde acudir, aprender a reconocer correos electrónicos o actividad sospechosa. La ciberseguridad y sus riesgos, incluidas las estafas y el *phishing* son responsabilidad de todos, nuestro actuar e interés al respecto promoverá y aportará a su entidad u organización niveles de ciberriesgo aceptables.



Lic. Hugo Gerardo Cervantes Grajeda
Analista de Ciberseguridad, Departamento de Tecnología de la Información de la SIB

Licenciado en Telecomunicaciones egresado de la Universidad Francisco Marroquín, con Maestría en Reingeniería y Tecnologías de Aseguramiento, así como Maestría en Informática Forense, ambos títulos otorgados por la Universidad Galileo. Cuenta con las certificaciones de Auditor Líder ISO 27001:2013 e ITIL. Posee experiencia en diseño y gestión de servicios tecnológicos e infraestructura, implementación de sistema de gestión basado en las normas ISO27001 e ISO20000, gestión de soluciones y servicios de ciberseguridad en el sector bancario e implementación de proyectos relacionados. Actual Coordinador del Comité de Ciberresiliencia por el Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO). Apoya en el desarrollo de actividades estratégicas y al fortalecimiento de capacidades internas de la SIB.

Pagos digitales y sus riesgos

Ing. Mario César Rodas Portillo

Históricamente los medios de pago han estado vinculados por el uso de dinero en efectivo. Desde la acuñación de las primeras monedas, el efectivo le ha dado consistencia al intercambio de bienes y servicios, siendo por mucho tiempo el predominante en el comercio mundial; sin embargo, la revolución tecnológica ha acelerado el proceso de sustitución del dinero por otros medios de pago.

Desde la introducción de la tarjeta de crédito en la década de 1950, se habilitaron nuevas formas de pago que han tomado auge con la ampliación de la cobertura de Internet y, especialmente durante los últimos años, tanto la banca en línea como los aplicativos móviles (Apps), han ayudado a consumidores y a comerciantes a migrar hacia los pagos digitales a través de las tarjetas de crédito, tarjetas de débito, transferencias electrónicas de fondos y dinero electrónico; en este contexto es de resaltar que los dispositivos inteligentes han apoyado el uso de estos servicios y al aumento de la participación de terceros como proveedores de servicios de pago.

Conforme se han ampliado las oportunidades para realizar compras por medios digitales, también se han incrementado las formas de cometer actos que exponen la seguridad de los consumidores y de los comerciantes ya que estos, en muchos casos, utilizan canales de comunicación informales como las redes sociales, aplicativos de mensajería instantánea u otros, en donde la exposición a los riesgos es mayor.

Dentro de los diferentes riesgos en el uso de pagos digitales, el más relevante es el denominado fraude en línea, mediante el cual se utiliza información robada o falsa, ocasionando pérdidas para los consumidores y comerciantes. En muchas ocasiones, el robo de datos se debe a la falta de seguridad con que se gestionan los mismos, lo que pone en riesgo la privacidad de los usuarios, al punto de comprometer datos sensibles.

Otro riesgo para considerar es la interrupción en el servicio de transmisión de información mediante el cual se realizan los pagos, esta puede ocasionarse por fallas en el suministro de energía eléctrica o en los sistemas de telecomunicación, así como por acciones vandálicas que pueden causar retrasos e inclusive la imposibilidad de consumar el proceso de las transacciones.

La pérdida o robo de dispositivos inteligentes genera un riesgo significativo para los propietarios y usuarios, en virtud que la mayoría consigna, dentro del dispositivo, sus contraseñas para el ingreso a la banca en línea y aplicativos comerciales, con lo cual se facilita el robo y mal uso de los recursos contenidos dentro de las cuentas del dispositivo.

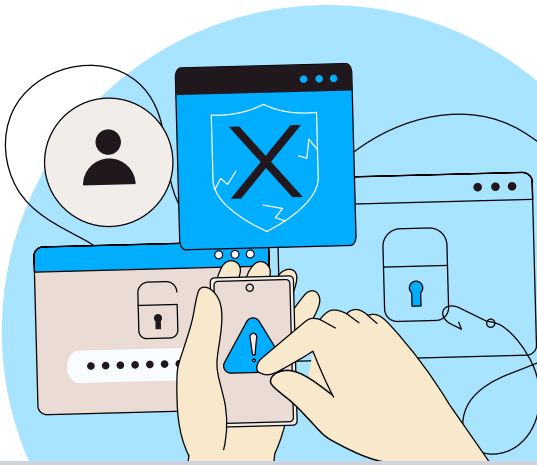
> Conforme los riesgos expuestos, es importante concientizar a los usuarios que utilizan sistemas de pagos electrónicos, a fin de que los mismos tomen las medidas de protección adecuadas, como: utilizar métodos de pago seguros, navegar en sitios web confiables y actualizar el *software* de seguridad informática en sus dispositivos tecnológicos.

En virtud de lo anterior, la Superintendencia de Bancos consciente de las innovaciones tecnológicas y los riesgos asociados a los sistemas de pago, propuso a la Junta Monetaria el Reglamento para la Administración del Riesgo Tecnológico, contenido en la Resolución JM-104-2021, el cual establece entre otros aspectos, que las instituciones que realicen operaciones y presten servicios financieros a través de canales electrónicos deberán implementar, como mínimo, mecanismos para la protección y control de la infraestructura de TI, los sistemas de información y las bases de datos considerando la gestión de la ciberseguridad; y, programas de educación y divulgación de información para clientes.

En adición a lo anterior, la citada resolución establece que las instituciones deben implementar medidas de seguridad en el intercambio de información, respaldadas por un certificado digital, cifrado de datos u otros mecanismos que permitan garantizar la autenticidad, confidencialidad, integridad y disponibilidad de la información; así como registros y bitácoras de las transacciones efectuadas.

Es importante recalcar que la educación financiera y tecnológica juega un papel trascendental para mitigar los riesgos relacionados a los pagos digitales; razón por la cual, el usuario de los sistemas de pagos digitales debe tener presente los procedimientos de autenticación existentes, es decir, establecer mecanismos que permitan dar certeza que el usuario es quien dice ser y que el mismo es el dueño de la información financiera que será utilizada, esto se logra mediante la utilización de contraseñas u otros factores de autenticación.

Finalmente, los medios de pago han evolucionado en el tiempo y en la actualidad ofrecen mecanismos digitales que facilitan la velocidad y la seguridad en los mismos, estos seguirán su transformación conforme la tecnología lo permita y la sociedad se adapte, debiéndose garantizar por todos los participantes, en la cadena de pagos digitales, la eficiencia de los sistemas para apoyar la actividad económica a bajo costo y que permita el acceso universal para la inclusión financiera.



Ing. Mario César Rodas Portillo
Profesional del Departamento de Normativa de la SIB

Ingeniero Administrativo egresado de la Universidad Galileo; es Magíster en Economía y Finanzas por la Universidad Rafael Landívar y egresado del Programa de Estudios Superiores del Banco de Guatemala. Posee más de seis años de experiencia en seguridad de la información e innovación y desarrollo. Es Miembro Titular de la SIB ante la Mesa Técnica de Pagos de la Estrategia Nacional de Inclusión Financiera (ENIF).

EL QUE PRESTA SU CUENTA PUEDE IR PRESO SIN DARSE CUENTA

Si prestas tu cuenta bancaria o tu nombre, puedes involucrarte en un delito sin saberlo.

DENUNCIAS POR EXTORSIÓN AL 1574

Para más información ingresa a: www.mp.gob.gt

#NoPrestoMiCuenta **#YoDenuncioExtorsión1574**

MP MINISTERIO PÚBLICO

GOBIERNO de GUATEMALA MINISTERIO DE GOBERNACIÓN

COALICIÓN POR LA SEGURIDAD CIUDADANA

CIEN FUNDESA

SIB Superintendencia de Bancos Guatemala, C. A.

ABG ASOCIACION BANCARIA DE GUATEMALA

Con el apoyo de todos los bancos del sistema