



VISION[®]

Financiera

Edición Nro. 35 • Año 9 Guatemala - marzo 2020

Retos para el ente supervisor en el 2020

Pág. 12



Cumplimiento más allá de la Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT).

Pág. 8

El seguro escolar como política pública en Guatemala

Pág. 16

Riesgo tecnológico y ciberseguridad

Pág. 25



Superintendencia de Bancos Guatemala, C. A.

Contenido

- 3 Presentación
- 4 Pluma invitada El rol de *Fintech* en la inclusión financiera
- 8 Artículo Cumplimiento más allá de la Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT)
- 12 Tema central Retos para el ente supervisor en el 2020
- 16 Artículo El seguro escolar como política pública en Guatemala
- 19 Artículo La transformación digital: beneficios y retos para el sector financiero (Parte 2)
- 22 Tecnología Seguridad de la información
- 25 Actualidad Riesgo tecnológico y ciberseguridad

Directorio

Director General

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Consejo Editorial

Lic. Hugo Rafael Oroxóm Mérida
Intendente de Coordinación Técnica

Lic. Byron Vinicio Méndez Castillo
Intendente de Estudios y Normativa

Inga. Xiomara Noemí Cabrera de Anzueto
Director
Departamento de Desarrollo Institucional

Coordinador General

Lic. Hugo Rafael Oroxóm Mérida
Intendente de Coordinación Técnica

Director de Proyecto

Lcda. Claudia Larissa Zúñiga Aragón
Supervisor
Departamento de Desarrollo Institucional

Unidad de Información Pública

9.ª Avenida 22-00, zona 1, Guatemala, C. A.
PBX: 2429-5000 y 2204-5300
Ext. 1+2560/2561/2562
Correo electrónico: info@sib.gob.gt
www.sib.gob.gt

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



Al correo electrónico:
comunicacion@sib.gob.gt



Al teléfono: (502) 2429-5000
extensiones 1+4350 o 4351

El contenido incluido en cada una de las secciones es responsabilidad exclusiva de sus autores y no representa necesariamente la opinión oficial de la Superintendencia de Bancos.

Se autoriza la reproducción del contenido de esta publicación, sin fines comerciales, citando su fuente de origen.

Esta publicación es gratuita y queda prohibida su venta.

“Trabajamos para promover la estabilidad y confianza en el sistema financiero supervisado”

Apreciables lectores:

En la edición 35 de la revista **Visión Financiera** se incluyen los principales retos que como Superintendencia de Bancos (SIB) nos hemos propuesto afrontar en el 2020 y que además están contenidos en el Plan Estratégico 2016-2021 de la Institución.

En tal sentido, seguiremos fortaleciendo la cooperación regional para la supervisión consolidada y transfronteriza de los grupos financieros, que implica estrechar el trabajo colaborativo entre entes supervisores.

Asimismo, será necesaria la revisión de los mecanismos de intercambio de información que viabilicen la efectividad de este modelo de supervisión.

La internacionalización de los mercados financieros pone de manifiesto la necesidad de avanzar en la implementación de las mejores prácticas y estándares internacionales, que incluyan las recomendaciones del Comité de Supervisión Bancaria de Basilea en torno a fortalecer la resiliencia del sistema financiero; de los Atributos Clave de Regímenes Efectivos de Resolución de



Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Entidades Financieras emitidos por el Consejo de Estabilidad Financiera (FSB, por su siglas en inglés); y, de las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) con respecto al combate del lavado de dinero u otros activos y el financiamiento al terrorismo.

Tomando en consideración los cambios en la infraestructura del sistema financiero, resulta prioritaria la revisión integral del perímetro de supervisión basado en el interés público que subyace en la naturaleza de las actividades que prestan las diferentes instituciones del sistema financiero.

Adicionalmente, la gestión de las instituciones supervisadas debe avanzar hacia esquemas prospectivos y basados en riesgos

con técnicas modernas que incluyan pruebas de resistencia y como consecuencia, de ser necesario, elaborar planes de acción para solventar las vulnerabilidades identificadas.

Finalmente, en esta edición se desarrollan temas que están vinculados al Plan Estratégico de la SIB. En tal sentido resalto la contribución de la licenciada Natalia Pinzón, Presidente de la Asociación *Fintech* de Guatemala, quien como pluma invitada expone sobre “El rol de *Fintech* en la inclusión financiera”. Asimismo, debo mencionar la colaboración de expertos de la Institución que abordan diferentes temas como el cumplimiento más allá de la prevención de lavado de dinero y financiamiento al terrorismo; el seguro escolar como política pública en Guatemala; la transformación digital: beneficios y retos para el sector financiero; seguridad de la información; y, riesgo tecnológico y ciberseguridad.

Atentamente,

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

El rol de *Fintech* en la inclusión financiera

Natalia Pinzón*

Presidente de la Asociación *Fintech* de Guatemala



***Fintech* en Guatemala**

En Guatemala, la industria *Fintech* está en un punto clave de crecimiento e innovación, liderado por múltiples emprendimientos regionales e internacionales. En noviembre de 2018, empezó la primera iniciativa para agrupar este sector bajo una entidad representativa y posteriormente se formalizó en lo que hoy es la Asociación *Fintech* de Guatemala, la cual tiene como objetivo principal agrupar a las empresas de la industria *Fintech* del

país para ofrecerle a sus miembros y al público en general, un espacio inclusivo de colaboración en el que se les permita impulsar la evolución de la industria.

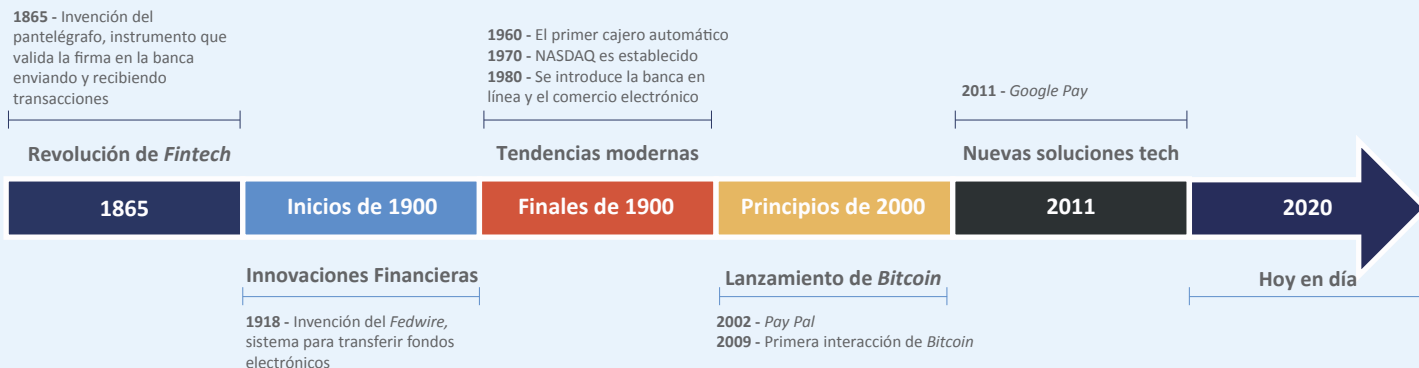
Asimismo, la Asociación *Fintech* de Guatemala confía en la colaboración entre los sectores público y privado con el objetivo de crear la estructura necesaria para el desarrollo empresarial de la industria *Fintech*, empoderando a los consumidores a través de una experiencia segura, transparente

y fácil. La Asociación comenzó con tres miembros y en el último año ha crecido hasta un total de 22, originados en varios sectores de *Fintech* pero con prevalencia en los medios de pago, remesas y préstamos. En los últimos años se ha evidenciado el crecimiento de la industria, no solo por el aumento de empresas *Fintech* en Guatemala, sino también por la presencia de instituciones bancarias, las entidades regulatorias y otros interesados en el sector.

Historia de *Fintech*

Tecnología financiera, conocida como *Fintech*, es definida por la Junta de Estabilidad Financiera como innovación en servicios financieros que puede resultar en nuevos modelos de negocio, aplicaciones, procesos o productos.

La historia de *Fintech* es más extensa de lo que muchos creen, como se muestra en el gráfico a continuación:



Tendencias globales

Este crecimiento exponencial en Guatemala es parte de una tendencia global en la evolución de la industria. El año pasado tuve la oportunidad de representar a Guatemala en la delegación del Banco Internacional de Desarrollo (BID) ante el Festival *Fintech* de Singapur. El evento fue la conferencia más grande del mundo sobre este tema, con más de 60 mil

participantes de 140 países. En la actividad se abordaron temas de innovación, tendencias tecnológicas y la importancia de la nube en el desarrollo de las *Fintech*, entre otros. Sin embargo, el punto focal fue la inclusión financiera y como a través de la colaboración inter-industrial se puede lograr un cambio significativo para los 1700 millones de adultos no bancarizados en el mundo. La colaboración inter-industrial se refiere

a la cooperación entre los jugadores clave de cada país, incluyendo las instituciones financieras, organismos internacionales, reguladores y las *Fintech* para fomentar iniciativas con el fin común de la inclusión financiera. Adicionalmente, en una reunión sostenida con la Autoridad Monetaria de Singapur (MAS), se comentó sobre la importancia de la colaboración entre los jugadores de la industria para el desarrollo de la economía de la región. Hay que resaltar algunas palabras del Ministro: «Una empresa puede ayudar a una persona; varias empresas, a un grupo de personas; pero si unimos a los jugadores clave del mercado con un fin común podemos cambiar una economía».

En Latinoamérica existen varios casos de éxito, en donde los bancos más grandes han optado por la transformación digital de sus procesos financieros. El Banco de Bogotá, por ejemplo, ha optado por una estrategia digital bastante fuerte que le ha llevado a que el 50 % de todas las cuentas de ahorro de sus clientes





organicen mesas de trabajo para alinear sus diferentes regulaciones *Fintech* de modo que se facilite la expansión de empresas *Fintech* en la región.

El rol de las *Fintech* en inclusión financiera en Guatemala

Guatemala dio el primer paso hacia la inclusión financiera cuando el Ministerio de Economía, en conjunto con la Superintendencia de Bancos (SIB) y el Banco de Guatemala, lanzaron la Estrategia Nacional de Inclusión Financiera 2019-2023 (ENIF), que busca “coordinar los esfuerzos a nivel nacional, tanto del sector público como del privado, con el objetivo de ampliar y mejorar el acceso y uso de los productos y servicios financieros a los distintos segmentos de la población guatemalteca”³. Para la Asociación *Fintech* de Guatemala fue importante haber sido incluida dentro de la estrategia y lo recibió

3 ENIF

como un valioso impulso a su misión. Si queremos una Guatemala próspera, con una economía fuerte, el cambio tiene que empezar con la colaboración. Según el reporte 2019 de la ENIF, el 56 % de la población de Guatemala no está bancarizada a pesar de ser uno de los países de Centroamérica con mayor penetración de teléfonos inteligentes (1.5 celulares por persona)⁴. A esto se suma el contraste entre la alta penetración de redes en el país y el nivel de pobreza extrema que hacen de Guatemala un candidato excelente para el fomento de la inclusión financiera a través de *Fintech*. Entre las mayores causas de la falta de bancarización global están el alto costo, el poco acceso y la falta de información de la población⁵.

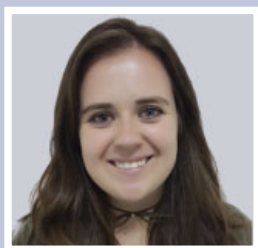
En el sistema tradicional es complejo bancarizar a personas de las que no se

- 4 Censo 2018 y <https://sit.gob.gt/download/boletin-estadistico-1er-semester-2019/wpmd-l=13429&refresh=5e2b70dcb2c111579905244>
- 5 2017 FDIC National Survey of Unbanked and Underbanked Households

tiene suficiente información, pero con el avance de la tecnología y el uso de celulares se ha vuelto cada vez más fácil perfilar a un individuo, aunque no se tenga data crediticia. Las *Fintech* permiten el desarrollo de soluciones eficientes y accesibles, estas reducen los costos de los procesos financieros actuales para poder ofrecer productos y servicios financieros a una mayor gama de clientes, especialmente a los no bancarizados y a los sub-bancarizados que están siendo desatendidos.

Conclusiones

Fomentar un ecosistema colaborativo donde los jugadores principales de la industria financiera logren trabajar juntos para un mayor desarrollo económico del país, promoviendo la inclusividad del sector financiero.



Natalia Pinzón

*Licenciada en Administración de Empresas con Especialización en Emprendimiento por Babson College, Estados Unidos de América. Participó en WINLab, una incubadora de *Startups* enfocada en mujeres. En 2017, completó el programa de *Fintech* de la Universidad de Oxford, Estados Unidos de América. Desde hace tres años gestiona proyectos de transformación digital en *Bowpi*, empresa de tecnología financiera que tiene como uno de sus pilares la inclusión financiera en Guatemala. Se considera una mujer apasionada por la inclusión financiera y actualmente es Presidente de la Asociación *Fintech* de Guatemala.

Cumplimiento más allá de la Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT)

Lic. Saulo De León Durán*

Intendente de Verificación Especial



En Guatemala, la noción de la figura de un Oficial de Cumplimiento (*Compliance Officer*) dentro de una entidad privada empezó desde que entró en vigor el Decreto número 67-2001 del Congreso de la República “Ley contra el lavado de dinero y otros activos”. El concepto y la función del Oficial de Cumplimiento proviene de una de las 40 Recomendaciones¹ del Grupo de Acción Financiera Internacional (GAFI), que refiere a

la aplicación de medidas de Debida Diligencia (*Due Diligence*) sobre el cliente con el fin de conocerlo, es decir la Política de Conocimiento del Cliente (*Know Your Customer*). Las recomendaciones del GAFI, a su vez, constituyen un mecanismo diseñado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para garantizar el cumplimiento por parte de los países de las Convenciones de Viena², de Palermo³ y de Mérida⁴.

Estas, en su orden, están enfocadas en establecer compromisos de país en la lucha contra las sustancias psicotrópicas, el crimen organizado transnacional y la corrupción.

El diseño del sistema de Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT) a nivel mundial tiene vasos comunicantes en diversos actores nacionales, públicos y privados, que buscan el cumplimiento de los estándares internacionales acordados en las convenciones mencionadas. En ese sentido, el Oficial de Cumplimiento en materia de PLD/FT resulta ser un funcionario dentro de la organización privada,

1 El GAFI formuló las 40 Recomendaciones, las cuales constituyen el marco básico de lucha contra el Lavado de Activos, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM) y han sido concebidas para una aplicación universal.

2 Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, de 1988.

3 Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, de 2000.

4 Convención de las Naciones Unidas contra la Corrupción, de 2003.

encargado de velar por el cumplimiento de la legislación, reglamentos, políticas, manuales y procedimientos aplicables para la prevención con una conexión de larga distancia con las convenciones de la Organización de las Naciones Unidas (ONU).

Evolución de la función del Oficial de Cumplimiento en materia de PLD/FT

Después de la entrada en vigor del Decreto número 67-2001, las Personas Obligadas a cumplir con la normativa PLD/FT entraron en un período de entendimiento, acoplamiento e implementación de las funciones del Oficial de Cumplimiento; ya que, no obstante sus atribuciones legales están bien definidas en la ley y el reglamento, hay ciertas características que con el tiempo se identificaron como necesarias para un adecuado desempeño, por ejemplo: jerarquía, conocimiento de la estructura y estrategia de la organización, acceso a información de todas las transacciones, conocimiento de la industria, experiencia en negociación, entre otras.

Su función de órgano de control se limitaba a tener un enfoque de cumplimiento normativo, es decir el *check list* de lo que la ley, los reglamentos y su normativo interno requería. Con el tiempo, fue evolucionando la gestión y el perfil de los Oficiales de Cumplimiento, a tal punto que en la actualidad ya está en marcha la aplicación de sistemas de Administración Basada en Riesgo del LD, que es una derivación de lo que en la gestión de empresas se denomina *Enterprise Risk Management* (ERM). Lo anterior denota que los Oficiales de Cumplimiento han desarrollado habilidades y competencias resultado de las exigencias de la compleja regulación en la materia.

Personas Obligadas registradas ante la IVE

Al 28 de febrero de 2020

Descripción	Cantidad
Agentes de Seguros Independientes	767
Almacenadoras	15
Arrendamiento de Vehículos Automotores Blindados	7
Arrendamiento Financiero	26
Aseguradoras	28
Bancos	18
Casas de Bolsa	21
Casas de Cambio	3
Casas de Empeño	1
Comercio de Joyas, Piedras y Metales Preciosos	110
Comercio de Objetos de Arte y Antigüedades	41
Compraventa de Divisas	39
Compraventa de Inmuebles	413
Compraventa de Vehículos Automotores	241
Contador Público y Auditor	237
Cooperativas de Ahorro y Crédito	408
Corredor de Seguros	72
Empresas de Canje de Cheques	1
Empresas de Transferencias de Fondos	25
Entidad Sin Fines de Lucro - Fondos del Estado	41
Entidad Sin Fines de Lucro - Fondos Extranjeros	170
Factoraje	10
Financiadoras	1
Financieras	13
Loterías, Rifas y Similares	5
Movimiento de Capitales	7
<i>Off Shore</i>	4
Operadores de Tarjeta de Crédito	3
Otras Instituciones	1
Promoción Inmobiliaria	370
Promoción Inmobiliaria o Compraventa de Inmuebles	299
Proveedor de Servicios Societarios	30
Provisión de Domicilio Fiscal	17
Servicio de Blindaje de Bienes de Cualquier Tipo	13
Tarjeta de Crédito	12
Total	3,469



Gobierno corporativo y administración integral de riesgos

El concepto y metodología aplicado a empresas de gobierno corporativo cobra relevancia a partir de los escándalos de fraudes corporativos en los años 90 y 2000 de entidades de presencia y escala mundial. Surge como una propuesta regulatoria para mitigar el típico problema de agencia de las empresas, respecto de sus relaciones entre accionistas, consejo de administración y la gerencia.

En Guatemala, lo anterior se establece como obligatorio para las entidades sujetas a la vigilancia e inspección de la Superintendencia de Bancos, en virtud de la resolución de la Junta Monetaria JM-62-2016. Con base en el artículo 57 de la Ley de Bancos y Grupos Financieros, en el que refiere a la unidad administrativa como el responsable de velar porque el personal de una entidad bancaria cumpla con la

normativa aplicable; y, a su vez, el artículo 21 de la resolución citada, desarrolla y designa a una Unidad Administrativa de Cumplimiento con funciones ahí establecidas.

Adicionalmente, la resolución de la Junta Monetaria JM-56-2016 mediante la cual se publica el Reglamento de Administración Integral de Riesgos, establece una Unidad de Administración de Riesgos encargada, entre otros temas, de verificar e informar al Comité de Gestión de Riesgos, periódicamente, sobre el nivel de cumplimiento de las políticas y procedimientos aprobados para la administración integral de riesgos.

Como vemos, la designación en una figura, persona, unidad o departamento encargado de velar por el apego de determinada normativa, se ha convertido en un mecanismo de “autocontrol” efectivo y, en algunos casos, se percibe más operacional que un comité.

Foreign Account Tax Compliance Act (FATCA) y Foreign Corrupt Practices Act (FCPA)

La *Foreign Account Tax Compliance Act* (FATCA) es una ley estadounidense emitida en 2010, la cual requiere que todas las entidades financieras no establecidas en Estados Unidos de América, hagan una búsqueda en sus registros para determinar si sus clientes cumplen con las condiciones para ser considerados con una conexión con este país, como datos de nacimiento, residencia en Estados Unidos de América, reporte de intereses (activos, cuentas, bienes) en el referido país.

La *Foreign Corrupt Practices Act* (FCPA), es una ley estadounidense emitida en 1977, la cual prohíbe a las compañías establecidas en Estados Unidos de América entrar en cualquier tipo de acto catalogado como corrupción (*bribery*) hacia estados extranjeros. No obstante, aplica también para compañías y personas que directamente o por intermediarios ayuden o faciliten pagos provenientes de la corrupción en territorio estadounidense.

Respecto del FATCA, es bien conocido que las entidades financieras guatemaltecas, en su mayoría delegaron en las unidades de cumplimiento PLD, la implementación de los controles, procedimientos y mecanismos de monitoreo para su observancia y realización. A su vez, respecto de FCPA, el conocimiento, la aplicación de las medidas y su ejecución ha recaído en los despachos jurídicos asesores, sean internos o externos.

Compliance en empresas del sector real

A partir del fenómeno de la globalización de los negocios impulsado por el acceso al internet, comunicaciones electrónicas, entre otros, las empresas y compañías han ido estandarizando sus prácticas comerciales, contractuales y, en especial, en el cumplimiento de su normativa y regulación local e internacional. Lo anterior se ha llevado a cabo a tal grado que, se reconoce que las empresas que tienen adecuados controles y sistemas integrales de *compliance* son más competitivas para el comercio internacional, el acceso a créditos internacionales, iniciar relaciones comerciales (de agencia, de exportación, de representación, entre otros) con contrapartes estadounidenses o europeas.

Es interesante observar constantemente que las empresas guatemaltecas se interesan en desarrollar dentro de su estructura una Unidad de Cumplimiento, que en muchos casos abarca temas más allá de anticorrupción y prevención de LD/FT, e incorporan los conceptos de gobierno corporativo relacionados con los conflictos de interés, códigos de ética y conducta; incluso, se incorporan políticas para la administración



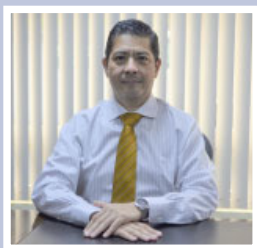
de los riesgos inherentes de la industria. Es común encontrar en la industria azucarera, inmobiliaria, *retail*, entre otras, a participantes con altos estándares y buenas prácticas en materia de *compliance* integral.

Es mi entendimiento que esto se debe a que el cúmulo de regulaciones nacionales e internacionales por cumplir y para poder participar en el concierto mundial de los negocios, hacen necesario delegar en un responsable la adecuación de políticas, procesos, métricas y procedimientos, que velen por su cumplimiento, y que el parámetro objetivo de este, se encuentre en la normativa que se genera para industrias reguladas, en este caso las entidades sujetas a la vigilancia y supervisión de la Superintendencia de Bancos. Es

decir, son varios los ejemplos de empresas que toman de base o punto de partida la reglamentación de la Junta Monetaria en materia prudencial y administración de riesgos, las cuales las adecúan para su industria o práctica comercial.

En conclusión, *compliance* en su sentido amplio y en las circunstancias actuales, se entiende por la práctica de una empresa de cualquier naturaleza, de desarrollar desde dentro de su organización un esfuerzo por adecuar sus procesos a la normativa, obligatoria o por elección, y velar por su cumplimiento mediante canales de comunicación a la administración. *Compliance* es un concepto amplio que va más allá de la prevención del LD/FT, ya que absorbe toda la regulación aplicable a la empresa.

Saulo De León Durán



*Abogado y Notario por la Universidad Francisco Marroquín, con Maestría en Administración de Empresas por el INCAE. Cuenta con especializaciones internacionales en temas relacionados con la Gestión de Riesgos en Prevención de Lavado de Dinero y Financiamiento al Terrorismo (LD/FT), Administración de Riesgos Financieros, Planeación Estratégica y Balanced Scorecard, entre otros. Posee amplia experiencia legal y bancaria, fue abogado asociado de uno de los bufetes más reconocidos en Guatemala y trabajó durante cinco años en el sector bancario ocupando diferentes cargos. Fue Coordinador del Comité de Oficiales de Cumplimiento de la Asociación Bancaria de Guatemala (ABG); lideró la defensa de Guatemala ante la Evaluación Mutua del Grupo de Acción Financiera del Caribe (GAFIC) sobre el cumplimiento de las 40+9 Recomendaciones para lo cual estableció y ejecutó una estrategia para posicionar a Guatemala como referente regional en la lucha contra el LD/FT. Ha realizado diferentes consultorías y ha sido conferencista sobre regulación financiera a nivel nacional e internacional; asimismo, fue Intendente de Verificación Especial de la Superintendencia de Bancos de marzo de 2008 a noviembre de 2010, cargo que ostenta nuevamente desde octubre de 2018.

Retos para el ente supervisor en el 2020

Lic. Erick Armando Vargas Sierra*
Superintendente de Bancos



La identificación de las principales vulnerabilidades y riesgos de las entidades financieras tanto de carácter endógeno como exógeno, que permitan el diseño y la implementación de políticas públicas para mitigarlos, es crucial para realizar una supervisión efectiva, así como para emitir regulaciones que coadyuven a que la función de intermediación se realice sin interrupciones, de tal forma que los bancos cumplan con su función en la sociedad de canalizar

los recursos de agentes superavitarios a deficitarios y, por ende, impulsar el crecimiento económico y el desarrollo del país. Adicionalmente, la naturaleza cambiante y dinámica del mercado financiero, local e internacional, hace imprescindible que el ente supervisor se ajuste continuamente mediante la identificación y determinación de las prioridades de supervisión y regulación. En ese contexto, en Guatemala dicho proceso se realiza en el marco del

plan estratégico institucional, con un horizonte multianual, que la Superintendencia de Bancos revisa todos los años y descansa, entre otros aspectos, en la misión de “Promover la estabilidad y confianza en el sistema financiero supervisado”. Para la identificación de los retos del ente supervisor hay que tomar en cuenta, por un lado, ciertas tendencias internacionales y, por el otro, el desarrollo del sistema financiero nacional.

DIAGRAMA 1



Fuente: SIB.

En relación con las tendencias internacionales y como se puede observar en el diagrama, me gustaría resaltar las que considero más importantes: i) la internacionalización del capital y la mayor interconexión del sistema financiero nacional con el resto del mundo, ii) el uso intensivo de la tecnología y el surgimiento de la omnicanalidad en el sector bancario, iii) la incorporación de nuevos jugadores no tradicionales en el sector financiero como la industria *Fintech*, que en términos genéricos se refiere a empresas emergentes que ofrecen servicios financieros específicos y las empresas *BigTech*, las cuales son firmas tecnológicas globales que agregan a su oferta de productos actuales los servicios financieros, iv) la mayor relevancia de los riesgos cibernéticos

y del cambio climático y, v) la creciente volatilidad e incertidumbre en la que están operando los mercados financieros internacionales. Todo lo anterior, conlleva retos para fortalecer la estabilidad financiera con el fin de proteger al sistema financiero de potenciales riesgos, derivados de la rapidez y escala con la que se pueden transferir los riesgos internacionales a la economía nacional. En este contexto, la velocidad del cambio tecnológico no solamente requiere nuevas habilidades, sino también un enfoque diferente de la supervisión, con mayor uso de los instrumentos y herramientas digitales, pero sobre todo descansando en una transformación digital a todo nivel.

Por otra parte, también es necesario tomar en consideración el aumento de la competencia en la industria financiera a través de la innovación, lo cual debe incentivarse, pero con el cuidado que se desarrolle un crecimiento financiero saludable, un mercado financiero eficiente con un alto grado de integridad. Además, en el mundo de hoy, principalmente centrado en datos, surge la necesidad de apuntalar la protección de estos, en particular los aspectos vinculados con las operaciones de los clientes del sistema financiero, así como la propiedad, privacidad y valor de estos en el modelo de negocios.

En el desenvolvimiento del sistema financiero nacional se debe tomar en cuenta que el mismo se encuentra en un proceso de expansión internacional y de crecimiento moderado en el mercado doméstico, se ubica entre los más rentables de la región y con un alto grado de liquidez, lo que permitirá financiar los proyectos de inversión y el consumo, además se tiene un crecimiento sostenido en las fuentes de financiamiento, principalmente locales, lo que demuestra la confianza del público en el sistema bancario tanto a nivel nacional como internacional. Por otro lado, el sistema financiero ha venido modernizándose en los últimos años con la inversión en importantes proyectos de infraestructura financiera, el desarrollo de mercados financieros alternativos, la actualización de la normativa bancaria y la incursión en modelos de negocios innovadores para propiciar la inclusión financiera y el crecimiento rentable de este.



DIAGRAMA 2



Fuente: SIB.

En este entorno, como se aprecia en el diagrama 2, uno de los retos que enfrentará el ente supervisor en el 2020 es el fortalecimiento de la supervisión consolidada y transfronteriza que implica estrechar el trabajo colaborativo a nivel regional, continuar ampliando y mejorando los colegios de supervisión, así como utilizar los instrumentos legales actuales que permitan ser más eficaces en el intercambio de información. Sin duda, en el contexto de la incursión de nuevos participantes o competidores en el sistema financiero, será crucial trabajar con autoridades de jurisdicciones con las que se ha tenido muy poco intercambio de información o con entidades que sencillamente no existían hace unos años. En cualquier caso, la actualización de los mecanismos de intercambio de información, cooperación y coordinación regional, así como las herramientas, metodologías

y modelos con el componente transfronterizo representan un desafío importante por lo que las acciones de la Superintendencia de Bancos requerirán contemplar este aspecto en toda su dimensión y en el que estamos inmersos como país.

Otro de los aspectos de mayor relevancia y desafío para el ente supervisor es el diseño e implementación de mejores prácticas y estándares internacionales, tales como: a) la aplicación gradual de medidas de política macroprudencial que permitan fortalecer la resiliencia del sistema financiero y de los mercados financieros ante eventos adversos y contar con colchones de capital para hacer frente a los mismos, así como suavizar el ciclo de crédito que coadyuve a la mitigación de los riesgos; b) la implementación de los Atributos Clave de Regímenes Efectivos de Resolución de Entidades Financieras que permitan asegurar, en lo posible, la continuidad de las funciones y procesos críticos del

sistema financiero y proteger los recursos del público, de tal forma que se vayan incorporando nuevas herramientas a la red de seguridad financiera, tanto local como regionalmente, derivadas de las lecciones de las crisis financieras internacionales; y c) las recomendaciones del Grupo de Acción Financiera Internacional (GAFI), con respecto al combate del lavado de activos y financiamiento al terrorismo, por lo que, para el país sigue siendo una prioridad la lucha contra este flagelo, en donde el rol de las entidades financieras es el elemento esencial que implica el involucramiento tanto del sector público como del privado para continuar avanzando en la estrategia nacional.

Adicionalmente, debe evaluarse periódicamente el perímetro regulatorio en línea con las nuevas prácticas. En Guatemala, es crucial abordar un esquema integral que permitiría apoyar el crecimiento del crédito y, en general, el uso de los productos y servicios financieros. Este elemento toma más relevancia al tomar en cuenta los cambios potenciales en el sistema financiero dado el incremento en la competencia en la industria financiera, la cual se orientará a la implementación de modelos de negocios con el fin de cumplir con las crecientes expectativas de sus clientes a la vez que se cumple con la regulación, lo cual irá acompañado de un cambio cultural para optimizar los canales de comercialización y la experiencia bancaria en un mundo digital.

En cuanto a la supervisión macroprudencial, el enorme desafío consiste en transitar a una supervisión prospectiva basada en técnicas modernas y avanzadas de medición de riesgos, en particular, utilizar herramientas como las pruebas de resistencia para evaluar la resiliencia de las entidades bancarias y el análisis de redes que permitan vincular la supervisión microprudencial con



la macroprudencial, priorizar e implementar medidas, mitigadores e instrumentos macroprudenciales como los requerimientos de capital de conservación, los colchones de capital contracíclicos y el capital por riesgo sistémico a efecto de disminuir la prociclicidad de la regulación y proteger la solvencia de las entidades bancarias en todo el ciclo financiero, así como los nuevos indicadores de liquidez sugeridos por el Comité de Supervisión de Basilea que permitan identificar los activos líquidos de alta calidad no comprometidos que poseen las entidades para hacer frente a las salidas netas de efecto en un horizonte de tiempo determinado, aspectos incluidos en la reforma denominada Basilea III. De igual forma es importante completar la transición hacia los requerimientos de capital por los distintos riesgos que enfrente el sector financiero. También es necesario continuar modernizando la supervisión y regulación del sector asegurador para fortalecer el margen de solvencia y la adecuada gestión de las reservas técnicas, entre otros aspectos. Asimismo, habrá que ir trazando la ruta para que la gestión y regulación de las aseguradoras sea prospectiva y basada en riesgos. Adicionalmente, si bien hemos iniciado la transición a un

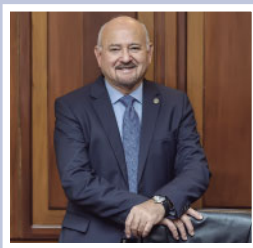
nuevo marco contable, es necesario continuar desarrollando los elementos esenciales para que el régimen de provisiones tome en consideración la metodología de las pérdidas esperadas.

En este orden de ideas, es fundamental continuar aumentando las capacidades de la Superintendencia de Bancos, aspecto crucial para la transformación de la supervisión (prospectiva y basada en riesgos), que coadyuve a promover la estabilidad financiera. Por otra parte, a lo interno es necesario continuar diseñando e implementando la transformación digital en la institución enfocada cada vez más en la gobernanza de datos y la seguridad de la información. Es importante hacer notar que el supervisor y regulador debe adaptarse a la nueva dinámica del sector financiero y, si bien debe enfocarse en la gestión de los riesgos y el gobierno corporativo de las entidades, también debe hacerse un esfuerzo por comprender y evaluar las nuevas tecnologías que están surgiendo en el sistema financiero a efecto de balancear un crecimiento mediante la innovación sin poner en riesgo la estabilidad financiera; todo lo anterior seguramente requerirá ajustar en algunos aspectos la regulación

financiera incluyendo, como se indicó, a nuevos actores, productos, servicios y operaciones con el objetivo de estrechar la colaboración de todos los jugadores del sector financiero.

Finalmente, en el contexto de la implementación de la Estrategia Nacional de Inclusión Financiera en el país, es relevante apuntalar la educación financiera, el diseño de un marco efectivo de protección al usuario de servicios financieros y todo lo que conlleva al fortalecimiento de las mipymes y otros sectores como el de vivienda. Lo anterior permitirá mejorar las condiciones de acceso y uso de los servicios financieros, facilitando los pagos mediante la interoperabilidad y el dinero electrónico, así como procurando nuevos mecanismos de ahorro y cobertura de seguros. Además, no hay que olvidar la importancia que tiene, en general, el desarrollo de la infraestructura y los mercados financieros. En ese sentido, es importante continuar impulsando el desarrollo integral de las centrales de riesgos y modernizar el sistema de pagos, así como desarrollar el mercado de valores para el surgimiento de vehículos de inversión alternativos.

Lic. Erick Armando Vargas Sierra



*Contador Público y Auditor por la Universidad de San Carlos de Guatemala, Abogado y Notario por la Universidad Mariano Gálvez de Guatemala; pónsum cerrado en las Maestrías de Derecho Penal y Consultoría Tributaria; y, Posgrado en Derecho Procesal Civil y Mercantil. Posee especializaciones en las áreas de Gestión y Administración Integral de Riesgos y Operaciones de Banca Central por el Centro de Estudios Monetarios Latinoamericanos (CEMLA). Como catedrático universitario ha impartido cursos de Auditoría, Finanzas, Economía, Contabilidad y Estadística en la Universidad de San Carlos de Guatemala, Universidad Francisco Marroquín, Universidad Mariano Gálvez, Universidad Mesoamericana y Universidad Panamericana. Cuenta con más de 40 años de experiencia profesional en el sector financiero, ha desarrollado su carrera en diferentes entidades nacionales e internacionales, tales como, la Superintendencia de Bancos, CARE Guatemala, Banco Centroamericano de Integración Económica (BCIE) y como auditor interno corporativo en tres grupos financieros guatemaltecos, Expresidente del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO). Actualmente, es Superintendente de Bancos de Guatemala.

El seguro escolar como política pública en Guatemala

Héctor Antonio Espina Lima*



El seguro como mecanismo de protección, es importante para la economía de un país porque protege contra pérdidas o daños al patrimonio del sector agrícola, comercial, industrial, de servicios y otros, lo cual optimiza su capital de trabajo, con el fin principal de evitar que las pérdidas impidan la continuidad de las empresas o que con el fallecimiento y enfermedades del asegurado la familia se vea

imposibilitada de atender sus necesidades y obligaciones.

Según la Asociación Guatemalteca de Instituciones de Seguros (AGIS), en Guatemala el índice de penetración del seguro (primas netas sobre el Producto Interno Bruto -PIB-) es del 1.2% a diciembre de 2019. Dicho porcentaje ubica a nuestro país con la más baja penetración del seguro en Centroamérica, y una de las más bajas a nivel latinoamericano.

El bajo índice de penetración representa que la brecha de protección del seguro¹ es significativa. De acuerdo con la información publicada en septiembre de 2019 por el Servicio de Estudios de la Fundación Mapfre: “El Mercado Asegurador

¹ Brecha de protección del seguro: Según Diccionario de Fundación Mapfre, representa la diferencia entre la cobertura de seguros que es económicamente necesaria y beneficiosa para la sociedad, y la cantidad de dicha cobertura efectivamente adquirida.

Latinoamericano en 2018”, Guatemala tenía una brecha de aseguramiento de Q38.7 millones, lo cual equivale a 5.5 veces el mercado asegurador real al cierre de ese año, por lo que se tiene un potencial de crecimiento interesante para lograr que dicha brecha se reduzca o desaparezca.

Según la publicación el mercado potencial de seguros en Guatemala (medido como la suma del mercado real y la brecha de protección del seguro) se ubicó en Q45.7 millones, equivalente a 6.5 veces el mercado a diciembre de 2018; por lo que es un reto importante para el país incrementar la penetración del seguro, lo cual implica fomentar su cultura y crear opciones o modalidades que permitan cubrir riesgos específicos, procurando el acceso a más personas a los beneficios que se obtienen en la contratación de un seguro.

En Guatemala, con el objetivo de ampliar y mejorar el acceso a los seguros para los distintos segmentos de la población de acuerdo a sus necesidades, en conjunto, el Ministerio de Economía, el Banco de Guatemala y la Superintendencia de Bancos, a finales del 2019 implementaron la Estrategia Nacional de Inclusión Financiera 2019-2023 (ENIF), que incluye dentro de sus cuatro áreas temáticas, una específica para seguros, cuyo objetivo es ampliar el alcance y profundización, la cobertura, los canales de distribución y la diversificación del seguro, así como desarrollar nuevos productos.

En términos generales, se considera que el concepto de inclusión financiera abarca el proceso mediante el cual la sociedad tiene acceso a los diferentes servicios financieros (crédito, ahorro, seguros, sistemas de pagos y pensiones, entre otros), y a mecanismos de educación financiera,



con el propósito de mejorar sus condiciones materiales de bienestar. En el caso de la actividad aseguradora, la inclusión financiera se concentra en el acceso a grupos específicos de la sociedad de aquellos productos que permiten la protección de la vida, la salud y el patrimonio por medio de los procesos de ahorro y compensación de daños implícitos en los productos de seguros.

Otro de los factores que puede influir en el aumento de la penetración del seguro es la implementación de políticas públicas o de Estado² que se utilicen como instrumento para solucionar el problema de la falta de acceso a los beneficios de los seguros por alguna parte de la población y lograr una protección igualitaria y, por ende, disminuir la brecha de protección.

Algunos países en Latinoamérica, como Perú y México, instituyeron como

política pública o de Estado, un seguro escolar que garantiza la atención médica gratuita por accidentes que sufran los estudiantes en las instalaciones de los centros educativos públicos o en camino a ellas, excluyendo a los alumnos de los centros educativos privados, basados en la idea de que en los primeros estudian niños y jóvenes de las familias más pobres del país y, por ende, con una alta vulnerabilidad ante gastos imprevistos derivado de accidentes escolares.

Las coberturas tradicionales que se otorgan en el seguro escolar de Perú y México, son principalmente, atención médica por accidente, atención quirúrgica o dental en los establecimientos, hospitalización, medicamentos y productos farmacéuticos, rehabilitación física, prótesis y aparatos ortopédicos y su reparación; sin embargo, no están cubiertos accidentes que pudieran haber sido provocados por los mismos estudiantes, enfermedades comunes, o eventualidades producidas en períodos vacacionales o fines de semana.

2 Políticas Públicas o Políticas de Estado: Son conjuntos de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas de interés nacional que se consideran prioritarios y que trascienden períodos de gestión de gobiernos, por ejemplo: el desempleo, la inseguridad ciudadana, la escasez de vivienda, la inmigración, el medio ambiente, entre otros.



Actualmente, en Guatemala no existe un seguro escolar en beneficio de los alumnos de los centros educativos públicos, por desconocimiento de la mayoría de los padres de sus beneficios y porque su situación económica no les permite pagar las primas que cobran las aseguradoras, lo cual provoca que su contratación no sea un asunto prioritario dentro de la economía familiar. Los padres de los alumnos de los centros educativos privados contratan voluntariamente pólizas colectivas de accidentes personales que cubren lesiones corporales sufridas durante el ejercicio de las actividades relacionadas con el centro educativo. Según registros

de la Superintendencia de Bancos, los principales beneficios para los estudiantes son: a) asistencia médica; b) asistencia quirúrgica; c) gastos de hospitalización; d) invalidez total y permanente por enfermedad no preexistente; y, e) ambulancia.

Según información publicada en periódicos y entrevistas a los Ministros de Educación y de Salud Pública y Asistencia Social, el Gobierno de Guatemala, presidido por el Doctor Alejandro Eduardo Giammattei Falla, congruente con la estrategia de inclusión financiera, tiene planificado contratar un seguro escolar que otorgue cobertura médica por

accidentes que sufran los estudiantes de los centros educativos públicos, lo cual se considera una política pública de gran trascendencia a nivel nacional, ya que, no solo incrementará la penetración del seguro en Guatemala, sino que, lo más importante, permitirá a los padres y a las autoridades de educación y salud, tener la seguridad y tranquilidad de que los estudiantes se encontrarán asegurados contra accidentes que pudieran sucederles durante el desarrollo de sus actividades educativas, lo que motivará a los padres a inscribir a sus hijos en el ciclo escolar y reducirá el riesgo de abandonar sus estudios por problemas relacionados con la salud.



Héctor Antonio Espina Lima

*Contador Público y Auditor por la Universidad de San Carlos de Guatemala; Máster en Gestión y Técnica de Seguros por la Universidad Pontificia de Salamanca, España, y del Centro Universitario MAPFRE de Estudios de Seguros; y, Maestría en Administración Financiera por la Universidad Mariano Gálvez de Guatemala. Delegado por la Superintendencia de Bancos de Guatemala para el intercambio de experiencias relacionadas con la actividad aseguradora en varios países latinoamericanos; con participación en seminarios organizados por la Asociación Internacional de Supervisores de Seguros (IAIS, por sus siglas en inglés); Asambleas Anuales de la Asociación de Superintendentes de Seguros de América Latina (ASSAL), Colegios de Supervisores de Seguros; seminarios organizados por la Agencia Española de Cooperación Internacional (AECI); Programa de Liderazgo para Seguros realizado por el Toronto Center; y, congresos realizados por reaseguradores. Tiene más de 28 años de experiencia en supervisión del sistema asegurador guatemalteco. Es Supervisor del Departamento de Supervisión de Riesgos de Seguros y Otros de la Superintendencia de Bancos.

La transformación digital: beneficios y retos para el sector financiero

(Parte 2)

Jorge Luis Hernández Rodríguez*



La tecnología que está haciendo posible la transformación digital de los servicios financieros

Sin mencionar las monedas virtuales, innumerables aplicaciones, desarrollos tecnológicos e innovaciones han surgido en los servicios financieros, que han dado lugar a una mejor experiencia para los clientes en los productos y servicios de la banca y han tenido impacto en la inclusión financiera. A continuación, algunas tecnologías que están transformando el sector financiero¹:

Tendencia tecnológica	Descripción
Inteligencia Artificial (IA)	Sistemas informáticos que realizan funciones que precisan capacidades humanas. La IA puede hacer preguntas, formular y probar hipótesis y tomar de forma automática decisiones basadas en análisis avanzados de conjuntos de datos muy amplios.
Machine Learning (Aprendizaje automático)	Es un método para diseñar reglas de resolución de problemas que mejoran automáticamente con la experiencia. Los algoritmos de aprendizaje automático otorgan a los ordenadores la capacidad de aprender sin que sea necesario especificarles todo el conocimiento que necesitarían para realizar una tarea deseada, así como de estudiar y construir algoritmos que pueden extraer enseñanzas de datos y experiencias y hacer predicciones basadas en ellos.
Interfaz de Programación de Aplicaciones (API, por sus siglas en inglés)	Constituye un conjunto de normas y especificaciones que los programas de <i>software</i> aplican para comunicarse entre ellos y que facilitan su interacción.
Internet de las Cosas (IoT, por sus siglas en inglés)	Es la interconexión de dispositivos físicos, vehículos, edificios y otros objetos que tienen integrados dispositivos electrónicos, <i>software</i> , sensores e interruptores, así como la conectividad de la red que permite que estos objetos recojan e intercambien datos y envíen, reciban y ejecuten órdenes.
Macrodatos o Big Data	Representan grandes volúmenes de datos que pueden ser generados, analizados y, cada vez más, utilizados por herramientas digitales y sistemas informáticos. Estas funciones se basan en la mayor disponibilidad de datos estructurados, la capacidad para procesar datos no estructurados, las mayores funcionalidades de almacenamiento de datos y los avances en potencia informática.
Blockchain (Tecnologías de registros distribuidos)	Constituyen un medio para registrar información a través de un libro contable o registro distribuido, es decir, una copia digital de datos en múltiples ordenadores. Estas tecnologías permiten que los nodos de una red propongan, validen y registren de forma segura cambios de estado (o actualizaciones) en un registro sincronizado que está distribuido por todos los nodos de la red.
Computación en la nube	Alude al uso de una red en línea (nube) de procesadores de alojamiento para incrementar la escala y la flexibilidad de la capacidad computacional. Este modelo, permite el acceso en red, a demanda y de forma sencilla, a un conjunto compartido de recursos informáticos configurables (como redes, servidores, instalaciones de almacenamiento, aplicaciones y servicios), que pueden liberarse rápidamente con un esfuerzo mínimo de gestión y escasa interacción con el proveedor de servicios.

1 Documento: Buenas prácticas - Implicaciones de los avances en Tecnofinanzas (*Fintech*) para los bancos y los supervisores bancarios. Comité de Supervisión Bancaria de Basilea, febrero 2018.

¿Cuáles son las implicaciones de la transformación digital para la banca y para los organismos supervisores?

La transformación digital para la banca implica beneficios y retos, tal es el caso de los riesgos asociados que las entidades deben gestionar. Dentro de los riesgos que enfrentan las entidades bancarias y financieras se encuentran los siguientes²:

Riesgo estratégico: se deriva de la probabilidad de pérdida en las posiciones de mercado de una entidad y como consecuencia en su rentabilidad, debido al surgimiento de nuevos actores en el mercado financiero que ofrecen servicios innovadores a sus clientes, no incluidos actualmente, estos nuevos actores en el perímetro regulatorio y su imposibilidad de poder competir con estos o realizar alianzas que les permitan permanecer en el mercado.

Amplificación del riesgo operacional: como consecuencia de una mayor exposición en los procesos e interdependencia entre los sistemas de información, tanto propios como de terceros; así como los derivados de la inadaptabilidad de las infraestructuras tecnológicas a nuevos entornos tecnológicos.

Riesgo de externalización: por las pérdidas monetarias o en la reputación en que podría incurrirse al suscribir convenios con terceros, derivados de alianzas estratégicas o la utilización de proveedores de servicios, en virtud que, los responsables directos ante los usuarios son las entidades bancarias o financieras.

2 Documento: Buenas prácticas - Implicaciones de los avances en Tecnofinanzas (*Fintech*) para los bancos y los supervisores bancarios. Comité de Supervisión Bancaria de Basilea, febrero 2018.

Mayores dificultades en el cumplimiento de disposiciones sobre *Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)*³: como consecuencia del surgimiento de productos y servicios innovadores derivados de la transformación digital y la interacción con nuevos entes prestadores de estos que no estén del todo dentro del perímetro regulatorio, lo que trae consigo, una mayor exposición para las entidades bancarias y financieras ante el uso de estas para realizar actividades delictivas en el ámbito de prevención del lavado de dinero y financiamiento al terrorismo, así como mayor dificultad en el cumplimiento de sus obligaciones derivadas de la ley y reglamentación sobre la materia.

Riesgo de cumplimiento relativo a la privacidad de los datos⁴: el riesgo de incumplimiento de las normas de privacidad de los datos puede aumentar con el desarrollo de técnicas de macrodatos (*Big Data*), la mayor externalización por acuerdos con empresas *Fintech* y la consiguiente competencia por la titularidad de la relación con el cliente.

Riesgo cibernético: proviene de la amenaza continua y la escala industrial sobre los activos digitales, las operaciones y la información corporativa, por parte de terceros⁵.

Riesgo de liquidez y volatilidad de las fuentes de financiación bancaria: la utilización de productos innovadores derivados de la transformación digital de la banca, permite a los usuarios dinamizar la inversión de sus recursos

3 Documento: Buenas prácticas - Implicaciones de los avances en Tecnofinanzas (*Fintech*) para los bancos y los supervisores bancarios. Comité de Supervisión Bancaria de Basilea, Página 26, febrero 2018.

4 Buenas prácticas - Implicaciones de los avances en Tecnofinanzas (*Fintech*) para los bancos y los supervisores bancarios. Comité de Supervisión Bancaria de Basilea, página 26, febrero 2018.

5 Buenas prácticas en gestión de riesgos - la fábrica de pensamiento Instituto de Auditores Internos de España – Ciberseguridad una guía de supervisión. Octubre 2016.

al trasladarlos fácilmente y en tiempo real a cuentas o fondos especializados de inversión, lo cual puede incidir en la volatilidad de las fuentes de fondeo de los bancos, exponiéndolos al riesgo de liquidez. Por su parte, los órganos reguladores y supervisores en su afán de preservar la estabilidad financiera a nivel global, están ejecutando iniciativas a efecto de normar y supervisar dichas tendencias, sin limitar la innovación y desarrollo del mercado.

En tal virtud, cada vez se hace necesaria la adopción y constante actualización, por parte de la banca y entidades financieras, de sanas prácticas de gobierno corporativo, que incluyan mecanismos de mitigación y control de riesgos, tanto para los riesgos tradicionales como para los riesgos emergentes inherentes a las innovaciones.

Adicionalmente, es importante que la banca y entes supervisores, implementen mecanismos adecuados de gobernanza de la información, para tener data de calidad en tiempo real y clasificación de la criticidad de esta, además disponer de un gobierno de la seguridad de la información con la participación de un CISO (*Chief Information Security Officer*) que proponga la estrategia de seguridad de la organización y que permita implementar la transformación digital, especialmente las tecnologías disruptivas con un adecuado apetito al riesgo y las medidas de seguridad pertinentes.

En el ámbito organizativo, no solo las entidades bancarias y financieras están formando cuadros de personal con perfil especializado en estas tendencias, tales como *data science* (científico de datos), tecnólogos, matemáticos, etc., sino también los entes supervisores deben rediseñar sus metodologías de supervisión y ajustar y dinamizar el perfil del personal que forma parte de sus cuadros técnicos, así como sus estructuras organizacionales tal y como lo aconseja el Comité de Basilea.

Primeros pasos del país sobre la transformación digital en el sector financiero

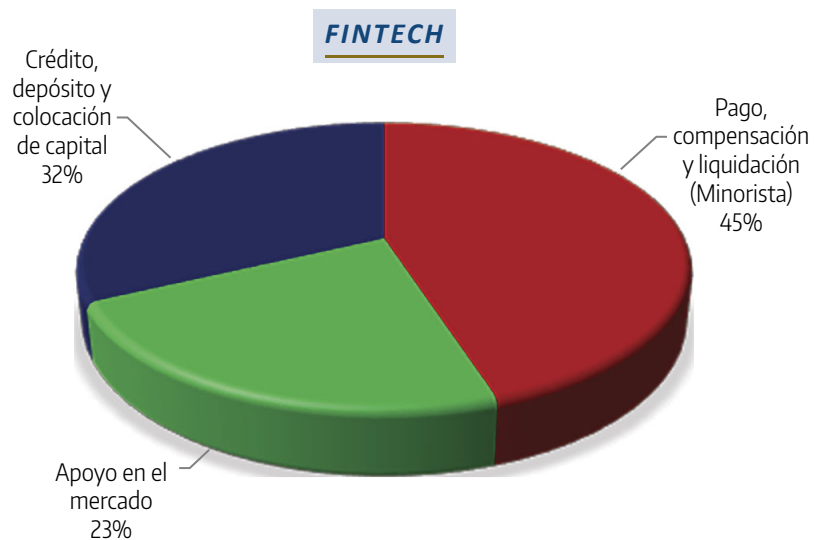
El tema sobre transformación digital en los servicios financieros, está siendo abordado por órganos internacionales especializados en la regulación y supervisión de los mercados financieros, así como empresas especializadas en el tema. En Guatemala, la banca está reaccionando ante esta tendencia, iniciando algunos con la elaboración e implementación de planes de transformación digital, y otros con la incorporación de nuevos productos, estrategias y tecnologías innovadoras, entre las cuales se pueden citar las siguientes:

- Inteligencia artificial (*Chatbots*).
- Pagos a través del celular con tecnología NFC⁶ (tarjetas con *Contactless*).
- Uso de *Machine Learning* para analizar comportamientos de los clientes.
- Utilización de los móviles para realizar operaciones sin consumo de datos.
- Alianzas estratégicas con *Fintech*.
- Utilización de redes sociales (atención de usuarios).

Por su parte, la Superintendencia de Bancos (SIB) consciente de la evolución tecnológica, cuenta con un espacio

⁶ NFC (*Near Field Communication*): es un conjunto de protocolos de comunicación que permiten a dos dispositivos, uno de los cuales es generalmente un dispositivo portátil tal como un teléfono inteligente, para establecer la comunicación a una distancia de 4 cm del uno al otro.

denominado “**SIB Innovation HUB**”, el cual es un punto de encuentro entre la institución y las *Fintech*, que permite conocer los desarrollos actuales y futuros de estos, así como facilitar la comprensión del marco jurídico financiero vigente.



Fuente: SIB.

Desde julio 2019 a la fecha, se han inscrito 26 *Fintech*, clasificadas de acuerdo a la matriz del Comité de Basilea, tal y como se observa en la gráfica anterior.

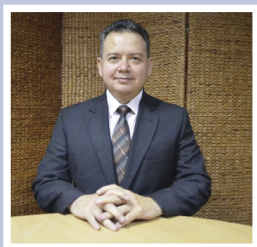
Ante el espacio concedido por el ente regulador, la respuesta de las *Fintech* en un corto tiempo en Guatemala es bastante positiva para impulsar la transformación digital en el sector financiero.

Para finalizar, se exponen las reflexiones siguientes:

- La transformación digital se extiende por todos los sectores, afectando tanto al mundo virtual como al contexto real. Es un motor de cambio definitivo e imparable.

- “*La transformación digital es un viaje y no un destino*”, es decir, es un megaproceso de mejora continua.
- El colocar al cliente en el centro es uno de los elementos clave de la transformación digital.
- El lograr el cambio de cultura tradicional por la digital, es uno de los principales retos de toda organización que desea transformarse digitalmente.
- La transformación digital más que un factor tecnológico, es una estrategia y cultura digital.

⁷ Eva Sánchez-Caballero Jiménez, *Business Development Manager BIS Sales and Sales Support* de Canon España.



Jorge Luis Hernández Rodríguez

*Contador Público y Auditor egresado de la Universidad de San Carlos de Guatemala, con Maestría en Informática con Énfasis en Banca Electrónica por la Universidad Mariano Gálvez de Guatemala. Posee Certificación del Programa de Transformación Digital y reconocimiento “*Fire Hydrant Award*” otorgados por el Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés). Ha participado en programas de tecnología de la información en diferentes países; desarrollo de habilidades gerenciales; e, innovación tecnológica, entre otros. Con experiencia en supervisión del riesgo tecnológico y ciberseguridad. Es Supervisor del Departamento de Supervisión de Riesgos Específicos de la Superintendencia de Bancos.

Seguridad de la información

Israel Ebenezer Mendoza Bautista*



Siendo la información uno de los principales activos para las organizaciones, velar por su seguridad es de gran importancia, por lo que es esencial independientemente del giro del negocio que se trate. Algunas veces se confunde la seguridad de la información con la protección de los datos tangibles, como: contratos, documentos financieros, planes estratégicos, entre otros, pero no se consideran los activos intangibles, como: la reputación de la empresa o negocio, el valor que tiene

la información contenida en bases de datos o en computadoras, licencias de *software*, procesos, personas y aquellos activos que poseen valor y están en torno al negocio día a día.

Por lo tanto, es importante conocer los fundamentos de la seguridad de la información y a partir de allí tener un modelo de negocio que incluya la protección de la información. En primera instancia, la seguridad de la información se define como: *preservación de la confidencialidad,*

*integridad y disponibilidad de la información*¹.

Preservación de la confidencialidad, integridad y disponibilidad de la información

1 ISO IEC 27000:2014, *Overview and vocabulary*.



¿Qué es integridad de la información?

Es transferir la información de un lugar a otro; por ejemplo, se consulta una cuenta bancaria de un usuario, la información debe estar en tiempo real y no estar alterada, debe ser la misma desde la última vez que hubo una modificación autorizada. *La integridad de la información es la propiedad de exactitud de la información*².

¿Qué es confidencialidad de la información?

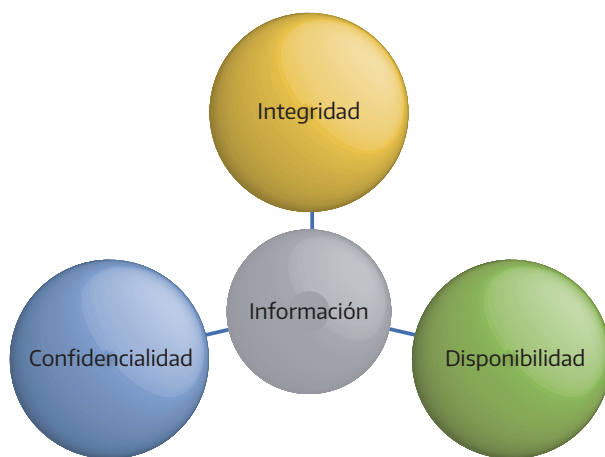
Es cuando esta puede ser restringida a todos los niveles. No todos los usuarios deben tener acceso a cierto tipo de información; por ejemplo, los datos de accionistas de una empresa

o del personal. *La confidencialidad es la propiedad de que la información no esté a disposición o se divulgue a personas, entidades o procesos no autorizados*³.

¿Qué es disponibilidad de la información?

Es disponer de datos en el momento que el negocio lo necesite; por ejemplo, se requiere de inventarios actualizados en una cadena de tiendas de artículos, por lo que es indispensable que estos estén disponibles en todo momento. *La disponibilidad de la información es la propiedad de ser accesible y utilizable a pedido de una entidad autorizada*⁴.

SEGURIDAD DE LA INFORMACIÓN



Fuente: propia del autor.

2,3,4 Ibid.

La seguridad de la información se basa en que esta es considerada como un activo que tiene valor y que requiere protección apropiada, contra la pérdida de disponibilidad, confidencialidad e integridad. Si lo que se desea es proteger su disponibilidad, se debe asegurar que sea accesible y utilizable cuando se necesite.

Actualmente ha tomado auge el término ciberseguridad el cual ISACA (Information Systems Audit and Control Association) lo define como una “capa de protección para los archivos de información, buscando que los sistemas de información puedan prevenir, actuar antes, durante y después de un ataque para reducir el riesgo de pérdida de información”. Deloitte expone en su informe “Tendencias de Ciberseguridad en América Latina, junio 2018”, que en los últimos años ha habido cambios significativos en temas de ciberseguridad y que las organizaciones han aumentado sus inversiones en este rubro debido a las brechas de seguridad que han descubierto.

El 18 de febrero de 2020, Prensa Libre de Guatemala publicó un artículo en el que un especialista en seguridad informática, Dmitry Bestuzhev, comenta que el país ocupa el lugar 111 en el conteo mundial con relación a la seguridad informática. Expuso que “El 20.1 por ciento de los usuarios nacionales están en riesgo de ser atacados por piratas virtuales. En este año ya se han registrado 1 millón 251 mil 424 incidentes de vulnerabilidad de cualquier tipo en el país”. También indicó que las infecciones de seguridad, código malicioso o virus se propagan y comparten por medio de memorias USB. Se estima que a la fecha han ocurrido 3 millones 133 mil 185 incidentes causados por

USB conectados a computadoras o laptops. Bestuzhev, comenta, “Esto quiere decir que el 38.6% de los usuarios guatemaltecos de memorias USB corren el riesgo de que se vulnere su seguridad”.

Sin embargo, aunque existen amenazas y riesgos asociados por ataques informáticos, la seguridad de la información puede gestionarse eficazmente mediante estándares y normas como ISO27000, ISO20000, COBIT, ITIL, entre otras. De acuerdo con las necesidades de la empresa, no es suficiente una solución de antivirus para mitigar los ataques cibernéticos,

sino también considerar sistemas antispam, prevención de intrusos IPS (Intrusion Prevention System), antimalware, filtrados de contenido de Internet, protección perimetral con *Firewalls*, segmentación de redes, entre otros. Además, es necesario tener controles, procesos y personas calificadas para gestionar los servicios de seguridad para mitigar los riesgos.

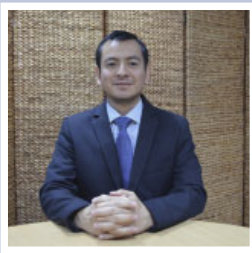
Seguridad de la información y ciberseguridad en Guatemala

Actualmente en Guatemala, existe un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-gt), el

cual es gestionado por el Ministerio de Gobernación; sin embargo, aunque el equipo ya está formado y ha colaborado con asuntos en materia de seguridad informática e información, hay carencia de legislación sobre la delincuencia cibernética; según el Observatorio de la Ciberseguridad en América Latina y el Caribe (www.observatoriociberseguridad.com), Guatemala no cuenta con una legislación integral sobre la delincuencia cibernética, por lo que el sistema judicial tiene dificultades para procesar los casos de esta índole.

En ese sentido, algunas instituciones guatemaltecas han comenzado a tomar medidas precautorias con la finalidad de proteger sus activos de información, lo cual contribuye a gestionar de mejor forma la seguridad de la información.

Aún falta mucho camino por recorrer, así como leyes que regulen la ciberseguridad en Guatemala, sin embargo, la cultura ha evolucionado y ya existen programas de concientización en materia de ciberseguridad y capacitación de personal en seguridad de la información, así como implementación de estándares y normas en tecnología. Actualmente, el sector financiero cuenta con el Reglamento para la Administración de Riesgo Tecnológico JM-102-2011, el cual considera los controles mínimos que deben cumplir las entidades para gestionar la seguridad de la información.



Israel Ebenezer Mendoza Bautista

*Ingeniero Electrónico por la Universidad de San Carlos de Guatemala, Maestría en Finanzas Avanzadas por la Universidad del Valle de Guatemala; y, Maestría en Negocios Electrónicos por la Universidad Galileo. Posee experiencia en Estándares de Gestión de Seguridad de la Información como ISO27000, ITIL, Seguridad Informática, Gestión de Servicios de Seguridad en materia Tecnológica, Mesa de Ayuda y Procesos de Servicios de Atención y Soporte a Usuarios. Es Profesional del Departamento de Tecnología de la Información de la Superintendencia de Bancos.

Riesgo tecnológico y ciberseguridad

César Fernando Mejía del Pinal*
Billy Fernando Marroquín Alvarado**



El uso de la tecnología ha crecido en los últimos años, debido al surgimiento de nuevas soluciones que cubren necesidades cada vez más complejas de las organizaciones. Dicha situación ha creado una correlación muy fuerte entre el éxito de una empresa y el uso adecuado de sistemas e infraestructura tecnológica; sin embargo, la dependencia de la tecnología aumenta el riesgo tecnológico inherente y, consecuentemente, la preocupación de las organizaciones, personas independientes y entes reguladores, lo cual ha requerido la creación de estructuras adecuadas con personal especializado, tanto para gestionar los recursos tecnológicos, como para minimizar los riesgos que asumen los mismos.

Derivado de lo anterior, uno de los temas que ha tenido mayor relevancia en los últimos años es

la ciberseguridad. En efecto, los marcos de gestión del riesgo de esta han fortalecido aspectos que ya se gestionaban en el riesgo tecnológico; no obstante, conforme a las lecciones aprendidas, tratan de enfocarse en las brechas que han generado mayor impacto financiero y reputacional en diferentes organizaciones a nivel internacional.

En ese sentido, las tendencias para la gestión del riesgo de ciberseguridad dedican sus esfuerzos a la protección y respuesta ante ataques a los sistemas e infraestructura de Tecnología de la Información (TI), a través de los canales externos que en conjunto se han denominado como “el ciberespacio”.

En este orden de ideas, en el ámbito de ciberseguridad han surgido términos ya existentes, tal el caso de incidentes, ataques y resiliencia, a los cuales se les

han antepuesto el acrónimo “ciber”, para referirse a un subconjunto específico de ciberseguridad; aunque, se considera que la gestión del riesgo de ciberseguridad debe incorporarse dentro de la gestión del riesgo tecnológico, ya que existe un enfoque holístico que permite centralizar los esfuerzos y crear estrategias integrales.

Como se indicó, el término de ciberseguridad ha tenido relevancia, inclusive ha llevado a organizaciones internacionales como el Consejo de Estabilidad Financiera (*FSB, por sus siglas en inglés*) a definir un glosario para estandarizar los términos relacionados con la ciberseguridad, mismo que se conoce como *Cyber Lexicon*.¹

1 Cyber Lexicon: <https://www.fsb.org/wp-content/uploads/P121118-1.pdf>

Siendo este tema de alta importancia a nivel mundial, entidades de todos los países han llevado a cabo esfuerzos para establecer estrategias con el fin de gestionar y adoptar mejores prácticas en materia de ciberseguridad. En

octubre 2019, se llevó a cabo el seminario Riesgo Tecnológico y Ciberseguridad, coordinado por la Asociación de Supervisores Bancarios de las Américas (ASBA) en Brasil, en el cual fueron expuestos temas

relevantes como: figuras clave de la organización para la seguridad de la información; riesgos críticos para la estabilidad financiera; controles para ciberseguridad; y, cadenas de subcontratación y migración de servicios hacia la nube.

FIGURAS CLAVE DE LA ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN



1) Es responsable de definir, aprobar y supervisar la implementación, entre otros, de la estrategia global del negocio, las políticas principales y la estrategia de riesgos.

2) Su función principal es supervisar y velar que las estrategias definidas en la empresa se cumplan, siendo este el cargo más alto dentro del organigrama de una organización porque es el responsable final de las acciones que se llevan a cabo dentro de la empresa, de su desempeño y su eficiencia.

3) Establece la dirección estratégica de Tecnología de la Información, garantizando una operatividad de TI adecuada (incluyendo políticas y procedimientos) y se asegura de que los planes de TI estén alineados con los del negocio.

4) Esta figura es parte importante en una organización, ya que es quien desarrolla políticas, procedimientos y estándares que garantizan la seguridad, confidencialidad y privacidad de la información, además de monitorear, reportar y desarrollar estrategias para prevenir incidentes de seguridad, apoyando también a la elaboración de programas de concientización sobre seguridad de TI, trabaja directamente con los dueños de la información para garantizar que los activos de información tengan una adecuada clasificación de seguridad e inventario.

Riesgos clave para la estabilidad financiera

Pérdida de confianza: el robo de información podría causar una considerable pérdida de confianza, que en escenarios extremos, podría llegar a precipitar el pánico de los depositantes o incluso una crisis bancaria de mayor alcance.

Pérdida de fondos: los atacantes podrían llegar a acceder a las cuentas del depositante y sustraer sumas importantes de fondos, que podrían llegar a afectar la solvencia de una institución financiera y, un incidente de este tipo, podría socavar la capacidad de una institución para cumplir con sus

obligaciones contractuales y causar una gran interrupción en el mercado.

Controles para ciberseguridad

La ciberseguridad es un tema de actualidad en un proceso en evolución continua, por lo que es importante que las instituciones tengan controles que mitiguen los riesgos a los que están expuestos. Entre otros, los controles de ciberseguridad más importantes se encuentran descritos en el diagrama de la página siguiente.

Asimismo, como parte de las experiencias compartidas por el Banco de España, se abordó la preocupación que conllevan las cadenas de subcontratación y migración de servicios hacia la nube, ya que cada

vez más las entidades financieras han optado por trasladar servicios a terceros, con lo cual existen tres aspectos importantes que deben ser abordados por las entidades y entes supervisores, siendo los siguientes:

1) Concentración de servicios críticos en un proveedor

Preocupación / situación detectada: dependencia de la capacidad de dicho proveedor para la continuidad de servicios de la entidad.

Posibles soluciones: iniciativas de regulación para proveedores de servicio; así como, seguimiento continuo a través de las entidades supervisadas, sobre el cumplimiento de las medidas mínimas requeridas para prestar el



servicio. También debe evaluarse que las entidades cuenten con planes de contingencia relacionados con sus proveedores.

2) Cadenas de subcontratación

Preocupación / situación detectada: existen escenarios en los que los terceros subcontratan, parcial o totalmente, los servicios que prestan a las entidades financieras. En los contratos se crea un compromiso legal directamente con la entidad contratada, que incluye requerimientos regulatorios y salvaguardas; sin embargo, las entidades subcontratadas por parte del proveedor no quedan sujetas a los mismos compromisos establecidos con el tercero.

Posibles soluciones: previo a contratar los servicios de un proveedor, se debe conocer la cadena de subcontrataciones y determinar si cumplen con los requisitos mínimos; adicionalmente, se deberá obtener asesoría legal para incorporar dentro de los contratos cláusulas para no permitir la subcontratación en el tiempo u obligar a las entidades subcontratadas a cumplir con los mismos requisitos establecidos, notificando también cualquier cambio en la cadena de subcontratación.

3) Migración de servicios críticos hacia la nube

Preocupación / situación detectada: la nube crea condiciones

de alta disponibilidad en las infraestructuras tecnológicas para los diversos servicios que brindan las instituciones financieras, puesto que la información puede estar distribuida en diferentes países; aunque la jurisdicción y acceso a dicha información por parte del supervisor puede ser compleja.

Posibles soluciones: implementar o actualizar la normativa local para que los temas de nube tengan el alcance para los entes supervisores y que en este proceso también se pueda incluir contratos que tengan cláusulas en sintonía con las regulaciones específicas de cada país.



César Fernando Mejía del Pinal

*Licenciado en Administración de Sistemas de Información con Maestría en Administración de Negocios con Especialización en Desarrollo y Evaluación de Proyectos, ambos títulos otorgados por la Universidad Mariano Gálvez de Guatemala. Certificado Auditor Líder de la Norma ISO/IEC 27001:2013. Posee experiencia en el ámbito tecnológico enfocado en temas de seguridad informática. Es Profesional del Departamento de Tecnología de la Información de la Superintendencia de Bancos.

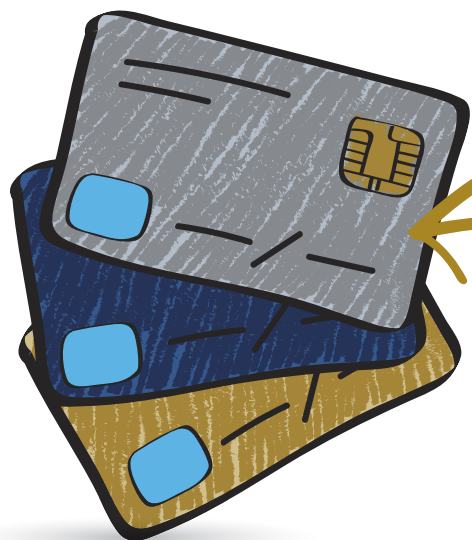


Billy Fernando Marroquín Alvarado

**Licenciado en Administración de Sistemas con especialización en Administración de Base de Datos, Magister Scientiae en Tecnologías de Información, Posgrado en Administración de Redes y Seguridad de la información, títulos otorgados por la Universidad Galileo. Auditor de Sistemas Certificado por ISACA (CISA); posee experiencia en temas relacionados con auditoría de sistemas, evaluación de la gestión de riesgo tecnológico y seguridad en entidades del sector financiero, empresas de telecomunicaciones y firmas de auditoría. Es Inspector del Departamento de Supervisión de Riesgos Específicos de la Superintendencia de Bancos.

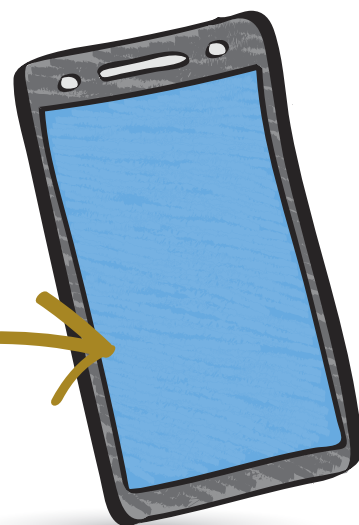
LA SUPERINTENDENCIA DE BANCOS RECOMIENDA REDUCIR, EN LO POSIBLE, EL USO DE DINERO EN EFECTIVO

La Superintendencia de Bancos comprometida con el bienestar de la sociedad guatemalteca y en apoyo a las medidas implementadas por el Organismo Ejecutivo para contener la propagación del Coronavirus (COVID-19), a la población recomienda:



Uso de otros medios de pago, como tarjetas de débito o crédito.

Uso de medios digitales como aplicaciones móviles, banca en línea, transferencias electrónicas, entre otros.





La Superintendencia de Bancos se suma a este esfuerzo de país.
¡JUNTOS SALDREMOS ADELANTE!



Superintendencia de Bancos
Guatemala, C. A.

 SIB Guatemala  @sib_guatemala  SuperBancosGuatemala

 sib_guatemala  Superintendencia de Bancos (SIB)

Visite:
www.sib.gob.gt 