VISIÓN Financiera

Edición Nro. 32 • Año 8 Guatemala - junio 2019

El camino a la innovación y su regulación

Pág.11

www.sib.gob.gt

Revista de la
SUPERINTENDENCIA DE BANCOS (SIB)

Superintendencia de Bancos
Guatemala, C. A.

Contenido

Directorio

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

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

Presentación

Actualmente la banca mundial enfrenta no solo cambios tecnológicos sino también una reinvención del sistema financiero con vistas al futuro que se observa más digital y personal. Estos cambios se estiman han derivado de la crisis económica recién pasada, la inquietud de los entes reguladores para mejorar las reservas de capital y liquidez; el incremento del índice de crimen y fraude financiero cada vez más sofisticado; y, por requerimientos de usuarios que buscan nuevos y más ágiles servicios, lo que ha abierto las puertas a la tecnología, como las *Fintech*.

En ese orden de ideas, en calidad de Superintendente de Bancos presento como tema central de esta edición el artículo denominado "El camino a la innovación y su regulación", relacionado con la implementación tecnológica; en él se exponen temas sobre estándares internacionales y el camino a la regulación *Fintech*. También comparto que la Superintendencia de Bancos ha iniciado con la creación de la Unidad de Innovación y Desarrollo (UNIDE), que tendrá por objeto investigar, estudiar y analizar los modelos de negocio innovadores en el ámbito financiero y riesgos inherentes a los mismos.

Como pluma invitada, contamos con la participación del Lic. José Rutman, Consultor Internacional, quien expone el tema "Gestión, regulación y supervisión del riesgo de crédito", en el cual desarrolla la conceptualización de la gestión del riesgo de crédito por las instituciones financieras y los desafíos que afronta la regulación y supervisión, resaltando la importancia de evaluar el marco de gestión del riesgo crediticio.

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

El Ing. Pablo Antonio Marroquín Fernández, Asesor del Despacho Central de la SIB, presenta el artículo "Gestión de crisis financieras, la experiencia del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO)", en el cual como parte de la gestión de crisis que permite reducir el costo de las mismas, hace referencia a la necesidad de fortalecer los mecanismos de cooperación e intercambio de información, cuando se produzcan eventos extraordinarios.

El Lic. Juan David Barrueto Godoy, Director del Departamento de Supervisión de Riesgos de Seguros y Otros de la SIB, nos comparte sobre los "Desafíos del uso del *Big Data* en la actividad aseguradora", la cual constituye una herramienta poderosa para las aseguradoras que permite obtener información y mejorar los procesos principales de esta industria.

Por su parte, la Lcda. Claudia María Rosales de Díaz, Inspectora del Departamento de Análisis de Transacciones Financieras de la SIB, desarrolla el tema "Importancia del equilibrio entre las medidas Anti-Lavado de Dinero/Contra el Financiamiento del Terrorismo (ALD/CFT) y la inclusión financiera" en el cual indica que dicho equilibrio se puede alcanzar a través de la adecuada implementación de la Recomendación 1, del Grupo de Acción Financiera Internacional (GAFI), Evaluación de Riesgo y Aplicación de un Enfoque Basado en Riesgo (EBR).

En la sección de tecnología, el Lic. Nefy David Morales Recinos, Profesional del Departamento de Tecnología de la Información de la SIB, presenta el artículo "Estrategia *Multicloud*", describiendo los medios sobre cómo actualmente se están implementando los servicios tecnológicos en la nube.

Finalmente, como tema de actualidad, el Lic. Carlos Humberto Martínez Molina, Inspector del Departamento de Supervisión de Riesgos de Seguros y Otros de la SIB, expone "El gobierno corporativo y la gestión de la seguridad de la información", compartiendo que la transformación digital de esta era está motivando a las entidades a desarrollar nuevas tecnologías, que mediante el gobierno corporativo requieren la implementación de políticas de seguridad que preserven y garanticen los sistemas y su información.

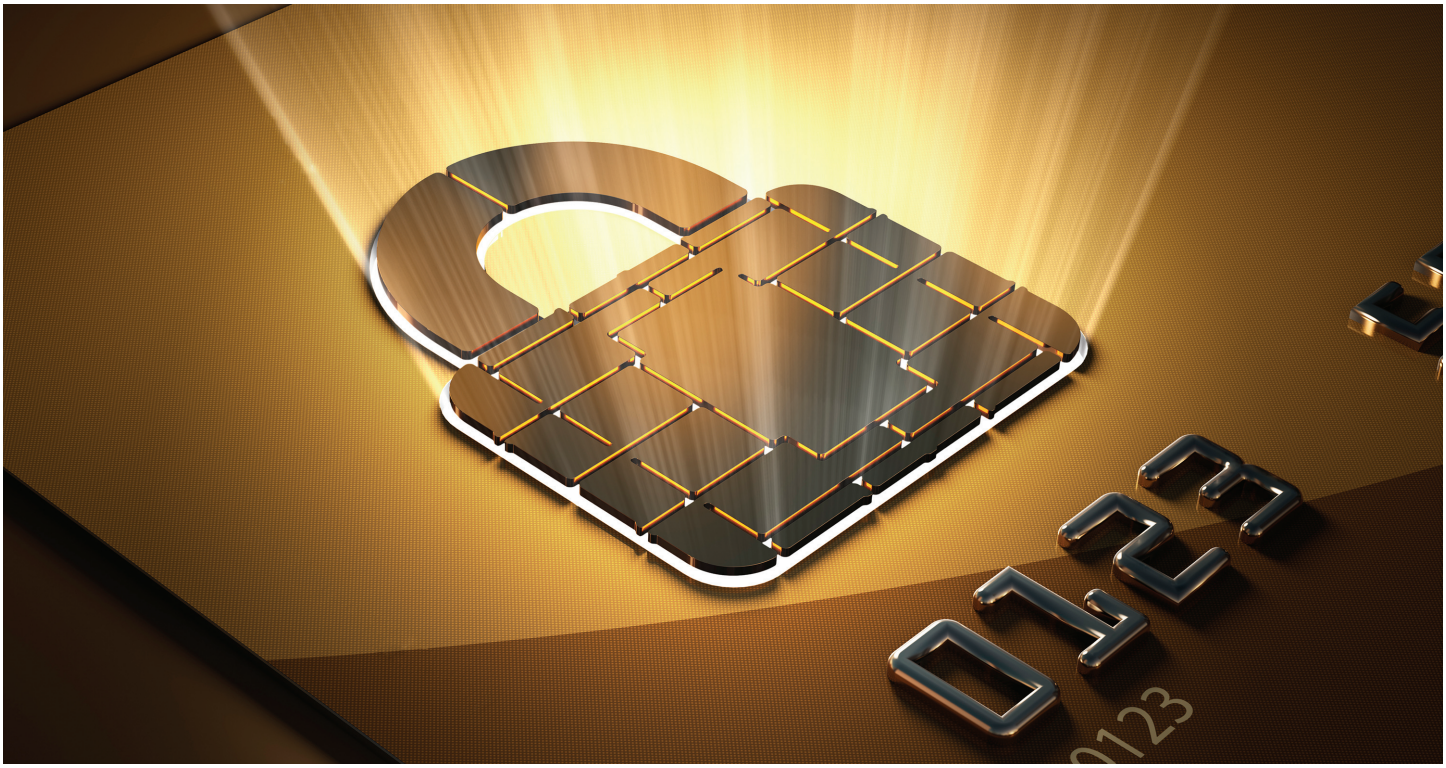
Esperamos que los temas incluidos en esta edición sean de su interés y utilidad.

Atentamente,

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Gestión, regulación y supervisión del riesgo de crédito

José Rutman*
Consultor Internacional



Algunos aspectos conceptuales

Una definición de Riesgo de Crédito (RC) posible es la brindada por el Comité de Supervisión Bancaria de Basilea (CSBB), que lo describe como *"La posibilidad de que un deudor de una institución financiera no sea capaz de cumplir con sus obligaciones de acuerdo a los términos acordados".* El RC se ve afectado por diferentes factores, tales como la capacidad individual de repago del deudor, condiciones generales de la economía (recesión, cambios en las tasas de interés), el marco legal y normativo, la calidad de las garantías, entre otros.

Si bien la actividad de intermediación financiera enfrenta varios riesgos (liquidez, crédito, operacional, mercado, tasa de interés, reputacional, estratégico, entre otros), el RC es el más relevante. Ello resulta más evidente aún en los sistemas financieros de países en desarrollo, donde la actividad de intermediación financiera clásica (captar depósitos para ser colocados en créditos) sigue teniendo un peso fundamental, dado el bajo desarrollo de otros productos y servicios financieros más sofisticados (tales como productos securitizados, derivados financieros, instrumentos valuados a precios de mercado).

Medición del riesgo de crédito

El comportamiento de las pérdidas por RC en una cartera de exposiciones crediticias puede describirse a través de una función de densidad probabilística (definida como las probabilidades que la variable en cuestión, "pérdidas por RC", pueda adoptar diferentes valores). La forma de esta función depende de varios factores, tales como: tamaño y calidad de las exposiciones, tasas de recupero, garantías, riesgo individual (idiosincrático o específico), y riesgo sistémico. Las distribuciones de retornos crediticios son fuertemente asimétricas, no respondiendo a una distribución normal. En base a ello, la

medición del RC presenta desafíos que requieren de apropiada información histórica y elementos para su adecuada interpretación.

El RC tiene, para su medición, dos dimensiones: individual (que puede ser capturado a través de sistemas de *credit scoring* / *ratings*) y de cartera (que solo puede ser incorporado al análisis a través de un enfoque de portafolio; siendo un ejemplo de ello, la metodología avanzada del CSBB conocida como *Internal Rating Based* (IRB), o modelos comerciales como KMV o *Credit Risk* +.

Un concepto ampliamente utilizado es la Pérdida Esperada (PE) de un crédito, el cual puede determinarse a partir de tres componentes: la Probabilidad de *Default* (PD), la Exposición al Momento de *Default* (EAD) y la Pérdida Dado *Default* (PDD), a través de la expresión siguiente:

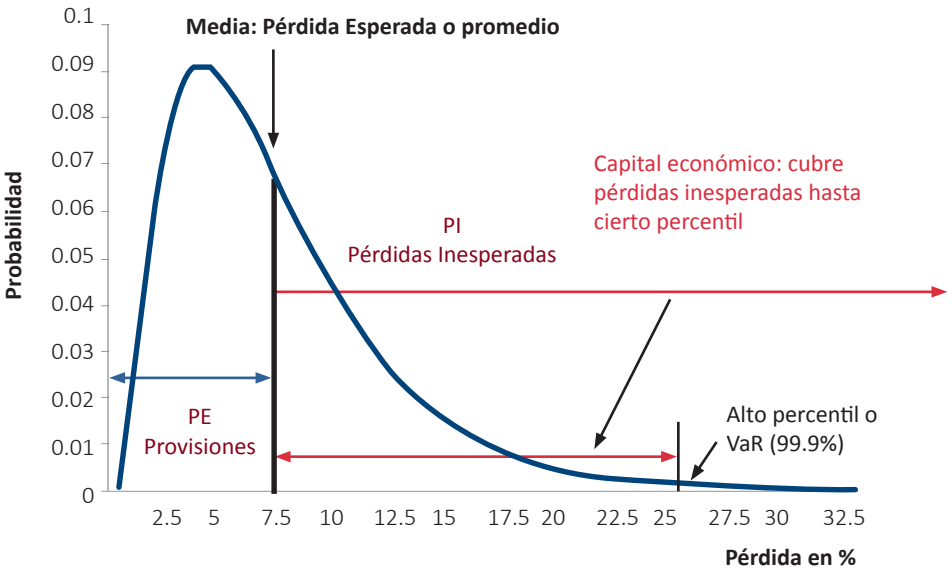
$$PE = PD \times EAD \times PDD$$

La PD de los deudores puede ser calculada a partir de metodologías históricas (predicen en base a lo sucedido en el pasado; algunos ejemplos son las calificaciones de riesgos o las matrices de transición) o metodologías prospectivas (modelos de *credit scoring* o basados en información de mercado). Respecto de la EAD, si bien en muchos casos resulta coincidente con el saldo actual de balance, hay varios rubros (tales como tarjetas de crédito, adelantos o sobregiros en cuentas corrientes, líneas financieras, entre otros) cuyos montos al momento de incurrir en *default* pueden presentar valores mayores a los registrados actualmente. Las estimaciones de las EAD se basan, generalmente, en reglas y modelos,

y están afectadas por las condiciones del mercado.

Finalmente, la PDD (que representa el monto que se pierde en el evento de un *default*, el cual difiere de la EAD ya que se puede cobrar; por ejemplo, de las garantías reales afectadas al crédito) se calcula utilizando modelos basados en datos históricos de recupero, incluyendo los costos en que se incurrirá para ello, así como el factor tiempo (la recuperación futura esperada -neta de los costos asociados a ella- de las exposiciones crediticias que entran en *default* deben ser traídos a "hoy", descontándolo aplicando la tasa de interés relevante –concepto de valor presente–).

Conceptualmente, las PE son las que deben ser cubiertas con las provisiones (reservas), mientras que las Pérdidas Inesperadas (PI) –que complementan las restantes pérdidas de la distribución, con un determinado nivel de confianza– son las que debieran ser cubiertas con el capital.



Fuente: Propia del autor.

A su vez, las distribuciones de pérdidas pueden ser condicionales (dada la realización de un factor sistémico; v. g. años "buenos" en los que la economía tiene buena *performance*, años "malos" en los que la economía presenta peor desempeño) o incondicionales (independiente de qué valor toma el factor sistémico, construida con información de períodos largos que incluye al menos un ciclo económico completo).

La gestión del riesgo de crédito por parte de las instituciones financieras

El primer responsable de que haya un marco apropiado para la gestión del RC es la propia Institución Financiera (IF). El marco debe abarcar una estrategia, estructura, políticas, procedimientos y sistemas que, de manera proporcionada a las características de la IF, permitan una adecuada gestión del RC. La estrategia debe ser establecida por el Consejo de Administración y contemplar políticas y procedimientos que incluyan al menos, el nivel de tolerancia al RC (en términos cuantitativos); límites prudenciales específicos de exposición al RC; lineamientos y supuestos para practicar las pruebas de tensión; desarrollo de planes de contingencia; monitoreo y análisis de las tendencias macroeconómicas, financieras, sectoriales y de mercado y su impacto en la exposición al RC; procedimientos para la aprobación, administración y recuperación de los activos crediticios; metodologías y herramientas para la identificación, medición, monitoreo, control, prevención y mitigación del RC; y, sistemas de información gerencial relacionados con el proceso de administración del RC. Asimismo, la IF debe tener claramente definidas las responsabilidades en la gestión del RC por parte de su Consejo de Administración, Comité de Gestión de Riegos, Unidad de Administración de Riesgos y Auditoría Interna.

Algunos de los aspectos que, luego de la última crisis financiera internacional, han tomado relevancia dentro de la gestión del RC son las siguientes:

a) **Un adecuado programa de pruebas de tensión** que sean lo suficientemente severas, calibradas considerando los principales factores de RC de la IF, y cuyos resultados generen acciones concretas por parte de esta).

b) **Contar con políticas apropiadas de incentivos para que el RC sea internalizado por los funcionarios y directivos de la IF**; por ejemplo, que el RC se tome en cuenta al momento de diseñar e implementar una estrategia de colocación de créditos, y no solo se centre en maximizar la colocación de los mismos.

c) **Mayor nivel de involucramiento de las autoridades superiores** de las IFs en la gestión del RC.

Los desafíos de la regulación y supervisión del riesgo de crédito

Un aspecto fundamental del RC es una adecuada valuación de los activos crediticios, aspecto que presenta un alto impacto en la solvencia de las IFs. A diferencia de lo observado en materia de cálculo de capitales mínimos (y recientemente también en liquidez), **no hay estándares internacionales cuantitativos en materia de valuación de activos crediticios**. Los Principios Básicos para una Supervisión Bancaria Efectiva del CSBB, contemplan buenas prácticas relacionadas con el RC (nro. 17) y en materia de activos dudosos, provisiones y reservas (nro. 18), mientras que otros documentos del CSBB contemplan aspectos para una adecuada gestión del RC. En los últimos años se han profundizado los acercamientos entre el CSBB y los fijadores de estándares contables para que la valuación de los activos crediticios migre desde el concepto de pérdida incurrida al de pérdida esperada.

Los marcos regulatorios deben contemplar exigencias vinculadas con una sana administración del RC complementados con criterios claros para la valuación de exposiciones crediticias (tanto dentro como fuera de balance), incluyendo aspectos referidos a la clasificación de deudas y deudores; distinción de tipos de deudores y créditos, provisionamiento mínimo; consideración de las garantías como mitigadores del RC y su impacto en el cálculo de provisiones mínimas.

Independientemente de que la normativa establezca los criterios de valuación, **debe propenderse a que las IFs desarrollen sus propias metodologías de medición del RC**, incluyendo el cálculo de la PE y sus componentes para lo cual, el primer paso, es comenzar a recolectar información relevante de manera estandarizada. Si bien ello representa un esfuerzo para las IFs que no se vería reflejado (en el corto/mediano plazo) en los requerimientos regulatorios de las provisiones mínimas, ello les permitiría una mejor medición del RC que enfrentan, además de poder ser utilizado como elemento para la valuación o "*pricing*" de los productos crediticios.

Finalmente, la supervisión del RC presenta el desafío de evaluar el marco de gestión del RC de las IFs, más allá de la verificación sobre la correcta valuación (clasificación y provisionamiento de los activos crediticios). Ello involucra comprender la estrategia que lleva adelante la IF, formarse una opinión sobre las políticas y procedimientos, así como verificar que los mismos se implementan de manera adecuada. En otras palabras, es complementar la supervisión basada en cumplimiento (*"compliance based")* con la supervisión orientada en base a riesgos (*"principle based")* que contemple los aspectos de buenas prácticas.

José Rutman

*Licenciado en Economía egresado de la Universidad Nacional de Córdoba, Argentina, con Maestría en Economía y candidato a Doctor en Economía del Centro de Estudios Macroeconómicos de Argentina (CEMA). Desde 1998 a 2010 ha sido Subgerente General del Banco Central y de la Superintendencia de Entidades Financieras y Cambiarias de Argentina, siendo representante ante el Comité de Supervisión Bancaria de Basilea. Ha efectuado consultorías para diversos organismos financieros internacionales en más de 25 países. Actualmente, es consultor internacional independiente, especializado en tópicos de regulación y supervisión financiera.

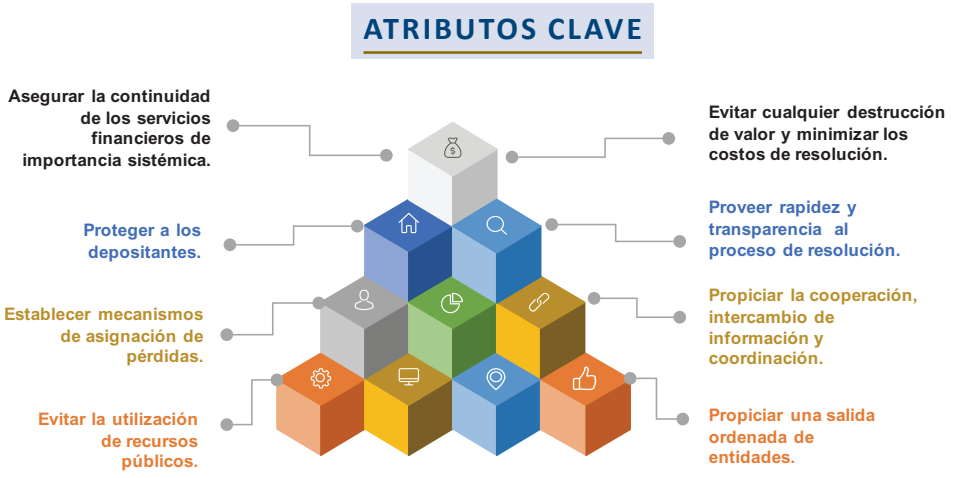
Gestión de crisis financieras,

la experiencia del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO)

Pablo Antonio Marroquín Fernández *

Los elementos más importantes que se fortalecieron después de la crisis financiera internacional fueron la implementación de acciones preventivas para reducir el riesgo de que ocurra otra crisis, así como lo referente a las medidas de gestión de crisis que permitan reducir el costo de esta. En este contexto, para salvaguardar la estabilidad financiera, el Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés) emitió el nuevo estándar internacional denominado Atributos Clave para los Regímenes de Resolución Efectiva para Instituciones Financieras[1], conocidos como Atributos Clave, en los cuales se detallan, entre otros aspectos, las herramientas de resolución que deberían estar a disposición de los hacedores de política con énfasis en las entidades financieras de importancia sistémica. Tal y como lo señala el FSB, un régimen de resolución es efectivo cuando permite la resolución de entidades financieras sin un impacto de carácter sistémico y sin exponer a los contribuyentes a las pérdidas ocasionadas por una crisis, a la vez que se protege las funciones esenciales del sistema financiero. Algunas de las características de los regímenes de resolución se muestran a continuación:

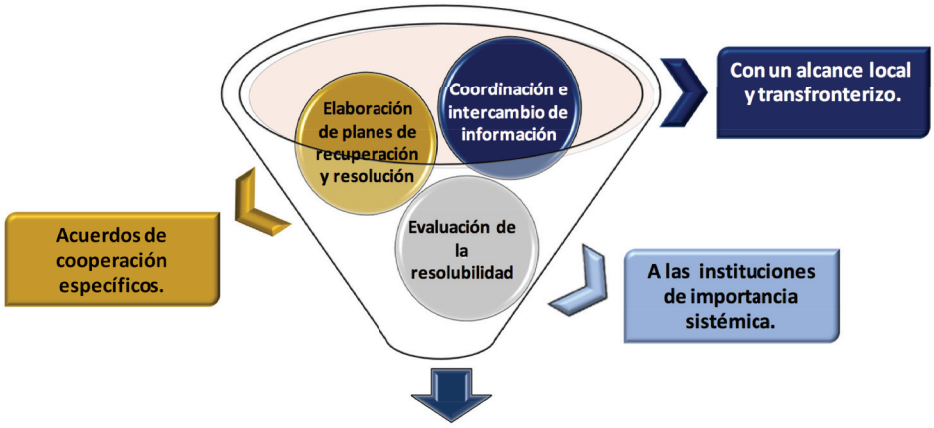
1 *"Key Attributes of Effective Resolution Regimes for Financial Institutions". FSB (2014).*



Fuente: propia del autor.

Los elementos anteriores deben tener la particularidad de ser creíbles y, por consiguiente, fortalecer la disciplina de mercado y proveer los incentivos adecuados para que se propicien soluciones de mercado; todo lo anterior, en el marco de la implementación de los doce Atributos Clave esenciales, los cuales deben formar parte de los regímenes de resolución de todas las jurisdicciones. Al respecto, hay que tomar en cuenta que no todos los atributos son igualmente importantes para los sectores financieros (bancos, seguros, pensiones, etc.), ya que algunos requieren de una adaptación e interpretación específica conforme a cada sector; no obstante, el FSB emitió una guía metodológica para la evaluación de los Atributos Clave del sector bancario en las correspondientes jurisdicciones[2]. Derivado de lo anterior, en algunas plazas financieras como la Unión Europea se han actualizado los regímenes de resolución para adecuarse a los Atributos Clave y, aunque pueden existir algunas inconsistencias o desviaciones del estándar, se continúa avanzando para implementar marcos de resolución integrales[3]. En efecto, la Directiva 2014/59/EU contempla los aspectos estrechamente vinculados con los Atributos Clave.

En el marco de los Atributos Clave, en adición a la Autoridad de Resolución, los elementos más relevantes se centran en la elaboración de planes de recuperación y resolución, evaluaciones de resolubilidad, intercambio de información y cooperación transfronteriza, entre otros. En los aspectos transfronterizos se hace especial énfasis en los marcos legales y los acuerdos de cooperación transfronteriza. En este ámbito, se resaltan la relevancia de la existencia de Grupos de Gestión de Crisis (CMGs, por sus siglas en inglés), en los que deben participar y cooperar las autoridades y jurisdicciones en donde los conglomerados financieros tengan presencia regional, así como cuando se tenga una presencia sistémica. Entre los aspectos más relevantes que deben realizarse en los CMGs se incluyen:



Fuente: propia del autor.

Grupos de Gestión de Crisis

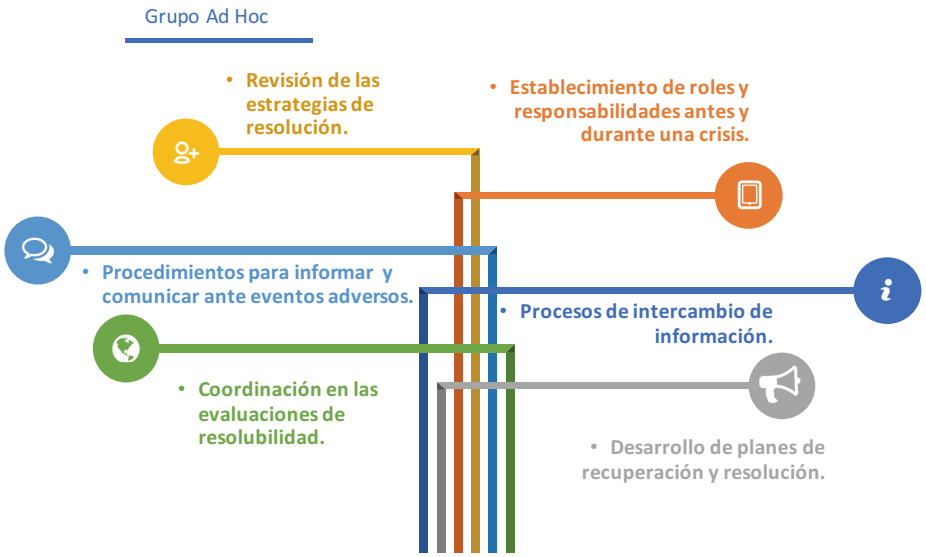
En un contexto transfronterizo caracterizado por la presencia de entidades financieras de conglomerados financieros de carácter regional, el aumento del grado de interconexiones entre los sistemas financieros, la deslocalización del capital, la internacionalización y apertura comercial e integración financiera, y el avance tecnológico en el sector financiero cobra mayor relevancia el establecimiento de grupos de gestión de crisis que, por un lado, permitan desarrollar los elementos establecidos en el nuevo estándar del FSB y, por el otro, sirvan de punto de enlace para la comunicación y la activación de protocolos de comunicación para que la supervisión sea más efectiva.

En este marco internacional, en el seno del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Entidades

2 *"Key Attributes Assessment Methodology for the Banking Sector". FSB (2016).*

3 *"Measuring the Implementation of the FSB Key Attributes of Effective Resolution Regimes for Financial Institutions in the European Union". Coleman, Nicholas, Andromachi Georgosouli and Tara Rice (2018).*

Financieras (CCSBSO), integrado por los países de Centroamérica, Panamá, República Dominicana y Colombia se ha venido impulsando la creación de grupos de gestión de crisis, en línea con lo estipulado en los Atributos Clave y con el objetivo de impulsar, desarrollar y adaptar las mejores prácticas internacionales de regulación y supervisión, sobre la base de la cooperación mutua entre sus miembros y en beneficio de la estabilidad financiera de la región. En ese sentido, el CCSBSO creó el Grupo Ad Hoc de Gestión y Resolución de Crisis cuyo ámbito de acción y, por consiguiente, su plan de trabajo multianual abarca los aspectos siguientes:



Fuente: propia del autor.

Por otra parte, el CCSBSO desde el 2007 suscribió el Memorando Multilateral de Intercambio de Información y Cooperación Mutua para la Supervisión Consolidada y Transfronteriza entre los miembros del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras, el cual fue ampliado en el 2016 y reconoce que la asistencia mutua y el intercambio de información facilitan la supervisión consolidada efectiva de las instituciones financieras pertenecientes a conglomerados o grupos financieros que operan en más de un país de la región. La creación y funcionamiento del Grupo Ad Hoc de Gestión y Resolución de Crisis complementa dichos esfuerzos al permitir, por un lado, operativizar lo establecido en el Memorando Multiraleral regional en aspectos relacionados con los protocolos de comunicación y, por el otro, fortalecer los mecanismos de cooperación, comunicación e intercambio de información cuando se produzcan eventos extraordinarios. Asimismo, permitirá cumplir con lo establecido en los Atributos Clave referentes a los grupos de gestión de crisis transfronterizos y el cumplimiento de sus principales funciones.

Este paso constituye un claro compromiso regional en la adopción de mejores prácticas y estándares internacionales relevantes para alcanzar los objetivos estratégicos contemplados en el Plan Estratégico Quinquenal del CCSBSO.

Finalmente, es importante comentar que la experiencia del CCSBSO con los dos instrumentos señalados (Memorando Multilateral y CMGs) se une a los esfuerzos pioneros realizados en otras plazas, tal es el caso de la experiencia nórdica, que constituye otro ejemplo en relación con la cooperación para la regulación transfronteriza, para la gestión y resolución de crisis[4].

4 *"Nordic experience of cooperation on cross-border regulation and crisis resolution". Report from RCG Europe Working Group (2018).*

Pablo Antonio Marroquín Fernández

*Ingeniero Químico Industrial y Licenciado en Administración de Empresas con Maestría en Finanzas por la Universidad Rafael Landívar. Ha realizado estudios de Postgrado en Gerencia Avanzada del INCAE y en Economía de Banca Central, Métodos Cuantitativos y Teoría Económica del Centro de Estudios Monetarios Latinoamericanos (CEMLA). Ha desarrollado su carrera en diferentes áreas, entre ellas la supervisión y regulación del sector financiero, el análisis de la estabilidad financiera y el diseño de políticas macroprudenciales. Es Asesor del Despacho Central de la Superintendencia de Bancos.

El camino a la innovación y su regulación

Lic. Erick Armando Vargas Sierra,
Superintendente de Bancos*

Las innovaciones tecnológicas, los cambios generacionales y la modificación en las preferencias de los consumidores ha generado la necesidad que entidades financieras tradicionales inicien un proceso de transformación digital y el surgimiento de entidades no bancarias prestadoras de servicios financieros por medios electrónicos, lo cual ha provocado el surgimiento de nuevos riesgos, los cuales deben ser estudiados, analizados, monitoreados y regulados adecuadamente sin desincentivar el desarrollo de estas. Al respecto, distintos entes internacionales han emitido documentos en los cuales hacen referencia a estas innovaciones.

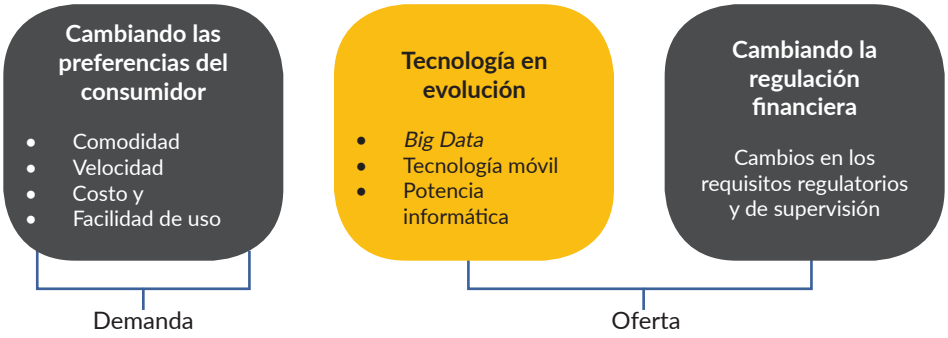
Estándares internacionales y regulación

Financial Stability Board (FSB)

El FSB emitió en junio de 2017 el documento *"Financial Stability Implications from Fintech",* en el cual se establece que con la industria *Fintech* surgen nuevas oportunidades

y riesgos para la estabilidad financiera que deben ser considerados por los entes reguladores y supervisores para promover la estabilidad financiera y fomentar la innovación responsable.

El FSB concluyó que la mayoría de las jurisdicciones encuestadas ya han tomado o planean tomar medidas regulatorias específicas para *Fintech*. El alcance y los cambios normativos planificados varían sustancialmente, dependiendo, entre otras cosas, del tamaño, de la estructura y complejidad del sector financiero, de las tecnologías de los mercados nacionales y de la flexibilidad del marco legal y regulatorio existente. En este sentido, varias jurisdicciones han implementado *Sandboxes* regulatorios y centros o aceleradores para promover la innovación y mejorar las interacciones con las nuevas empresas *Fintech*.



Fuente: Elaboración propia del autor, con información del *Financial Stabiliy Implications From Fintech. Financial Stability Board.* 2017.

Comité de Supervisión Bancaria (Basilea)

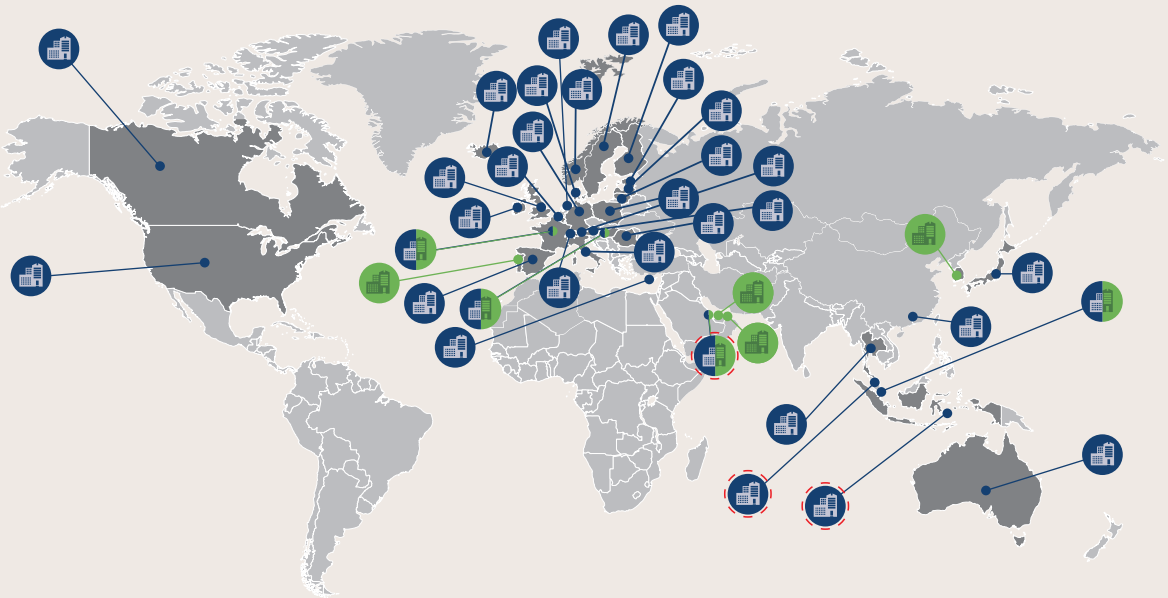
En 2018, Basilea emitió el documento *"Sound practices: implications of Fintech developments for banks and bank* supervisors", estableciendo entre sus principales consideraciones, que los supervisores deben realizar una revisión y actualización de su marco normativo, considerando las innovaciones financieras con el objeto de eliminar las barreras para estas. Asimismo, el supervisor debe desarrollar las competencias requeridas para realizar una supervisión efectiva a los desarrollos *Fintech*, evaluando la apertura de centros HUB de innovación y la implementación de *Sandboxes* regulatorios.

El camino internacional a la creación de normativa para *Fintech*

Centro o punto de innovación HUB del regulador o supervisor financiero

De conformidad con Basilea, la mayoría de las autoridades supervisoras han establecido, como primer paso, un centro de innovación con el objeto de funcionar como punto de diálogo entre la autoridad supervisora o reguladora y entidades innovadoras reguladas y no reguladas.

DIFERENTES CENTROS DE INNOVACIÓN CREADOS EN EL MUNDO



Fuente: UNSGSA *FinTech Working Group and CCAF* (2019), a*nd European Supervisory Authorities* (2019)

En Latinoamérica, en el 2018 fue creado el HUB de la Superintendencia Financiera de Colombia, como unidad de innovación de la Dirección de Investigación y Desarrollo, que es el área que investiga, analiza y emite las instrucciones normativas correspondientes. El objetivo de esta unidad es tener un acercamiento con entidades innovadoras reguladas o no, para identificar barreras regulatorias, oportunidades de capacitación al sector y mapeo de nuevas tendencias innovadoras. En el caso de México se realizó un diagnóstico previo del mercado para conocer las principales entidades *Fintech* existentes y los distintos modelos de negocio innovadores que se estaban implementando, lo que motivó la emisión de la Ley para Regular las Instituciones de Tecnología Financiera en marzo de 2018. En Brasil, en 2016 fue creado su HUB de innovación, con el objeto de tener acercamiento con el mercado previo a emitir una regulación específica. En Perú, la Superintendencia de Banca, Seguros y AFP, creó en 2017 un equipo de innovación para realizar un análisis del mercado previo a emitir la ley que permita las fuentes alternas de financiamiento como el *Crowdfunding*.

Regulación *Sandbox*

Según Basilea, el término "campo de pruebas regulatorio" o "caja de arena" suele hacer referencia a ensayos de nuevos productos o servicios en un entorno regulatorio controlado, que puede abarcar a las entidades reguladas y no reguladas en función de las características de cada país. Los campos de pruebas regulatorios van más allá del diálogo y el intercambio de conocimiento inicial en el HUB, ya que implican el acompañamiento y vigilancia del supervisor durante el período de prueba, es decir, implican el uso de facultades discrecionales concedidas legalmente a la autoridad supervisora.

Es importante mencionar que no todas las empresas *Fintech* pueden optar a participar bajo un modelo de normativa *Sandbox,* sino que únicamente aquellas que cumplen con ciertos requisitos establecidos por el supervisor, quien considerará el tipo de modelo de negocio y el desarrollo de este. Dentro de la normativa *Sandbox* se establecerá el plazo; el tipo o modelo; la información que deberá compartir; y, las condiciones para que se considere un modelo exitoso o no. Por último, deberá definirse la manera de incorporarse bajo una supervisión normal al ser un modelo exitoso, o la forma de salida de la empresa para tener el menor impacto en el mercado financiero en caso no sea considerado exitoso.

A nivel internacional, se han desarrollado distintos modelos de *Sandbox*: el primero, permite realizar una prueba controlada de productos innovadores de entidades financieras tradicionales. El segundo, permite el otorgamiento de licenciamientos temporales a entidades *Fintech* con el objeto de que puedan probar productos innovadores en un ambiente controlado. Un tercero, es un *Sandbox* multi jurisdiccional o transfronterizo, el cual consiste en una unificación regulatoria entre varios países, permitiendo que una entidad reciba un licenciamiento temporal para probar sus productos.

Es preciso señalar que, para la existencia de una normativa *Sandbox,* es necesario que exista una legislación flexible para permitir este tipo de normativa y licenciamiento temporal, de lo contrario será necesario

crear la vía legal para permitir al órgano regulador emitir este tipo de normativa. Por ejemplo, en el caso de México, la Ley de Instituciones de Tecnología Financiera (conocida como Ley *Fintech*) estableció que la Comisión Nacional de Bancos y Valores podrá emitir normativa específica y temporal para modelos novedosos de entidades supervisadas o no. En el caso de Colombia, la Ley del Plan Nacional de Desarrollo, aprobada el 2 de mayo del presente año, permite a la Superintendencia Financiera de ese país emitir certificados (licenciamientos) para operar temporalmente en este tipo de entidades.

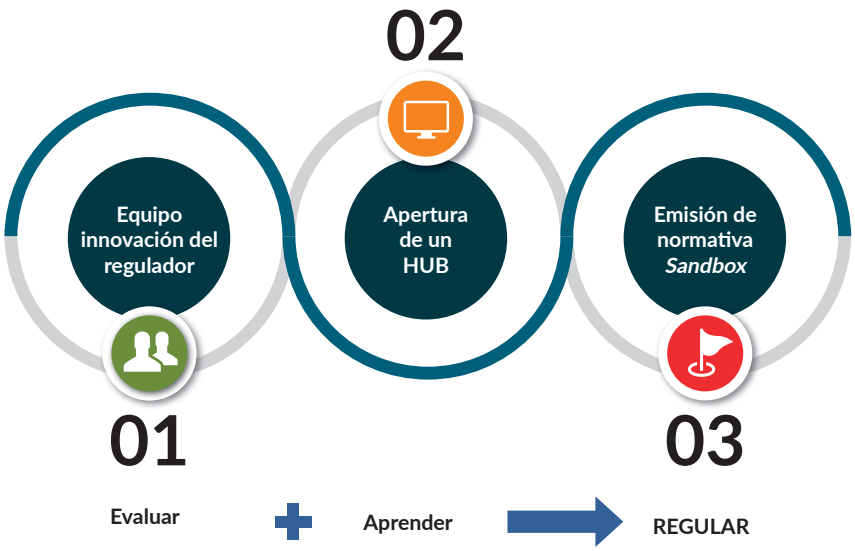
El camino a la regulación *Fintech* por la Superintendencia de Bancos de Guatemala

El Superintendente de Bancos emitió el Acuerdo Número 16-2019, por medio del cual se crea la Unidad de Innovación y Desarrollo (UNIDE), la cual depende funcionalmente de la Intendencia de Estudios y Normativa de la SIB. La UNIDE tiene por objeto investigar, estudiar y analizar los modelos de negocio innovadores en el ámbito financiero, así como los riesgos que le son inherentes, con el objeto de desarrollar los instrumentos técnicos y legales necesarios para su diagnóstico y regulación.

Entre sus atribuciones se encuentran estudiar e investigar la utilización de nuevas tecnologías para el mercado financiero regulado, la naturaleza y necesidad de regulación de productos y servicios innovadores; proponer, desarrollar y actualizar la legislación y normativa prudencial relacionadas a dichas innovaciones; y, brindar capacitación interna y externa sobre temas de innovación.

En este sentido, se tiene previsto que esta Unidad de Innovación y Desarrollo sea la encargada de la apertura del HUB de innovación de la Superintendencia de Bancos, el cual será un punto de contacto entre el órgano supervisor y las entidades *Fintech*, con el propósito de conocer sus modelos de negocio, así como los desafíos e identificar riesgos involucrados con las nuevas innovaciones, con el fin de proponer, si fuera necesario, los cambios regulatorios para preservar la estabilidad del sistema financiero supervisado, sin limitar o impedir las innovaciones financieras tecnológicas.

La Superintendencia de Bancos con la creación de la UNIDE y el lanzamiento del HUB de innovación, se convierte en la primera autoridad supervisora en Centroamérica que crea una unidad específica destinada para el desarrollo e innovación y la implementación de un punto de contacto entre el supervisor y las entidades que desarrollen modelos de negocios que apliquen tecnologías financieras innovadoras, con la intención de lograr un desarrollo tecnológico del sistema financiero y apoyar los esfuerzos nacionales de inclusión financiera.



Fuente: Elaboración propia del autor, proceso de reglamentación. *Test, learn and then regulate.*

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; pénsum 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. Actualmente, es Superintendente de Bancos de Guatemala y Presidente del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO).

Desafíos del uso del *Big Data* en la actividad aseguradora

Juan David Barrueto Godoy*

En los últimos años se han utilizado y escuchado con más frecuencia dos términos relacionados con la utilización de la tecnología en el sistema financiero y que están cambiando la forma de hacer negocios, siendo estos términos acrónimos de habla inglesa *Fintech* e *Insurtech*, correspondiendo a las palabras *Financial Technology* e *Insurance Technology*, respectivamente.

En el caso de *Insurtech*, se refiere a la tecnología aplicada a la actividad de seguros o empresas de tecnología que desarrollan tecnología aplicable a los negocios de seguros. Según estudios publicados por varias empresas, *Insurtech* abarca los conceptos siguientes:

- *Digital Platforms* (internet, teléfonos inteligentes, etc.)
- *Internet of Things - IoT*
- *Telematics / Telemetry*
- *Big Data y Data Analytics*
- *Comparators*
- *Machine Learning - ML y Artificial Intelligence - AI*
- *Distributed Ledger Technology – DLT*

El presente artículo se enfoca en *Big Data*, entendiendo como tal, a un gran volumen de datos estructurados o no, con los que puede contar un negocio, ya sea por que los recolecte directamente o porque los obtenga de otra fuente de información[1].

Algunos estudios señalan que *Big Data* se fundamenta en las **"5 V"**, **volumen** (gran cantidad de datos), **velocidad** para accederlos y procesarlos, **valor** para el negocio, **variedad** de datos por las fuentes utilizadas y **veracidad**.

Fuente: Propia del autor.

De conformidad con lo publicado el 6 de febrero de 2019, por la revista *Latino Insurance on line*, el volumen de información que existe actualmente es elevado. Una investigación de Domo en 2017 reveló que cada minuto se postean en el mundo 456,000 *tweets*, se realizan más de 3,600,000 búsquedas en *Google* y se visualizan más de 4,146,000 videos en *YouTube*. Por otra parte, según el estudio *Data Age* 2025, realizado por *International Data Corporation* (IDC), el volumen de datos total a nivel mundial aumentará 10 veces para 2025. El 90% de los datos de los que se dispone hoy han sido generados en los últimos dos años y, en 2019, las empresas generarán el 60% de la información a nivel mundial.

En la actividad aseguradora los datos pueden ser de utilidad en varios procesos, es decir en el diseño de productos a ofrecer, selección de riesgos, tarificación o determinación de la prima, ventas cruzadas, predicción de reclamos y detección de fraudes, lo que permite generar productos personalizados y automatizar los distintos procesos, aumentando la penetración del seguro y la rentabilidad de este tipo de empresas.

Tradicionalmente a la actividad aseguradora se le ha denominado como un mercado de oferta, es decir, que los productos se diseñan conforme características definidas por la aseguradora y en formatos estandarizados para grupos de personas; asimismo, previo a la negociación de un producto de seguros, se requiere que el mismo sea aprobado o registrado por el órgano supervisor, tal es el caso de Guatemala, según lo dispuesto en el artículo 36 de la Ley de la Actividad Aseguradora. Para el diseño y aprobación o registro de productos de seguros, se requiere contar con datos estadísticos que permitan realizar la mejor estimación de la siniestralidad esperada, conocida como prima de riesgo y que constituye la base para la prima de tarifa, es decir la que se le cobrará al cliente, generalizando o definiendo la prima para un grupo de asegurados con características similares. En consecuencia, a mayor volumen de datos y veracidad de estos, mejor será la tarificación y reducirá la exposición al riesgo de suscripción inherente a la aseguradora, entendiéndose como dicho riesgo a la probabilidad de pérdidas derivado de que la siniestralidad ocurrida sea superior a la esperada o estimada al momento de diseñar el producto.

En tales circunstancias, ***Big Data* se ha convertido en una herramienta poderosa para la actividad aseguradora, toda vez que le permite a las aseguradoras obtener información que facilita y mejora el proceso de suscripción de riesgos, permitiendo que el mercado de seguros se convierta en un mercado de demanda, donde los productos son diseñados acorde a las necesidades y perfil de riesgo de los clientes**. Al respecto, a nivel mundial existen seguros expedidos conforme la demanda del cliente, considerando el perfil de riesgos de cada posible asegurador, para tarificarlo en función del nivel de riesgo individual y no como parte de una media. Adicionalmente, los seguros cubren el tiempo de uso, el comportamiento de quien usa el bien asegurado, por ejemplo la forma de conducir, o tomando en cuenta

1 *Report of the 24th A2ii, IAIS Consultation Call "Supervising Insurtech" – (21 september 2017). Access to Insurance Initiative – International Asocciation of Insurance Supervisors.*

los hábitos de vida de la persona, medidos a través de dispositivos que calculan el nivel de actividad física de las personas aseguradas.

En virtud que todo el historial de consumo de una persona, sus hábitos, su comportamiento al usar el bien asegurado, sus preferencias, historiales médicos y otra información, es almacenada en grandes cantidades, esto se puede considerar *Big Data*, lo cual facilita y mejora la medición e identificación de los riesgos, para una mayor gestión del riesgo de suscripción y mejorar la rentabilidad de las aseguradoras; sin embargo, las expone a otros desafíos que hay que tomar en cuenta, entre los que destacan los siguientes:

a. **Privacidad de la información.** Previo a usar cualquier información se debe contar con los derechos legales para poder acceder a ella, sin que ninguna persona pueda reclamar su privacidad.

b. **Saturación de información.** Para optimizar el uso de la información, dado su volumen y variedad, se debe contar con mecanismos adecuados de análisis, a efecto que no se acumule información sin ninguna utilidad que represente altos costos para la aseguradora o que solo cause distorsión en el proceso de análisis requerido.

c. **Plataforma tecnológica.** Las aseguradoras deben contar con la infraestructura tecnológica adecuada, que le permita obtener, procesar, almacenar, transmitir, comunicar y disponer de la información que almacena *Big Data*, para dar viabilidad a los procesos del negocio. En este aspecto debe tomarse en cuenta, la obsolescencia acelerada a la que está sujeta la tecnología y que podría afectar la utilización del *Big Data*.

d. **Seguridad de la información.** Se deben implementar medidas que garanticen la confidencialidad, integridad y disponibilidad de los datos para que la utilización de grandes volúmenes de información, por medio de *Big Data*, no haga vulnerable a la aseguradora de ataques cibernéticos que conlleven la pérdida, extracción y corrupción de la información almacenada.

e. **Relaciones con terceros.** Para el aprovechamiento de economías de escala y por la especialización que requiere el uso de *Big Data*, generalmente involucra a empresas especializadas en este tema, lo que hace conveniente que las aseguradoras cuenten con políticas, procedimientos y controles adecuados que permitan la gestión de los riesgos inherentes a la tercerización de servicios, con el propósito de garantizar la disponibilidad de los servicios continuamente y debiendo observar los accesos que requieren los reguladores a la información relacionada con las entidades supervisadas.

Estos desafíos y otros que surjan, deben ser abordados por las aseguradoras como parte de la gestión del riesgo operacional, a tenor de lo dispuesto en el artículo 29 de la Ley de la Actividad Aseguradora, el cual establece que las aseguradoras deben contar con procesos integrales que incluyan la administración del riesgo operacional, entre otros, que contengan sistemas de información y de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir la exposición al riesgo citado, siendo responsabilidad del consejo de administración de cada entidad, velar porque se implementen y encuentren en adecuado funcionamiento los procesos integrales a los que se ha hecho referencia.

Referencia: Seminario Regional ASSAL - IAIS y Cumbre Insurtech

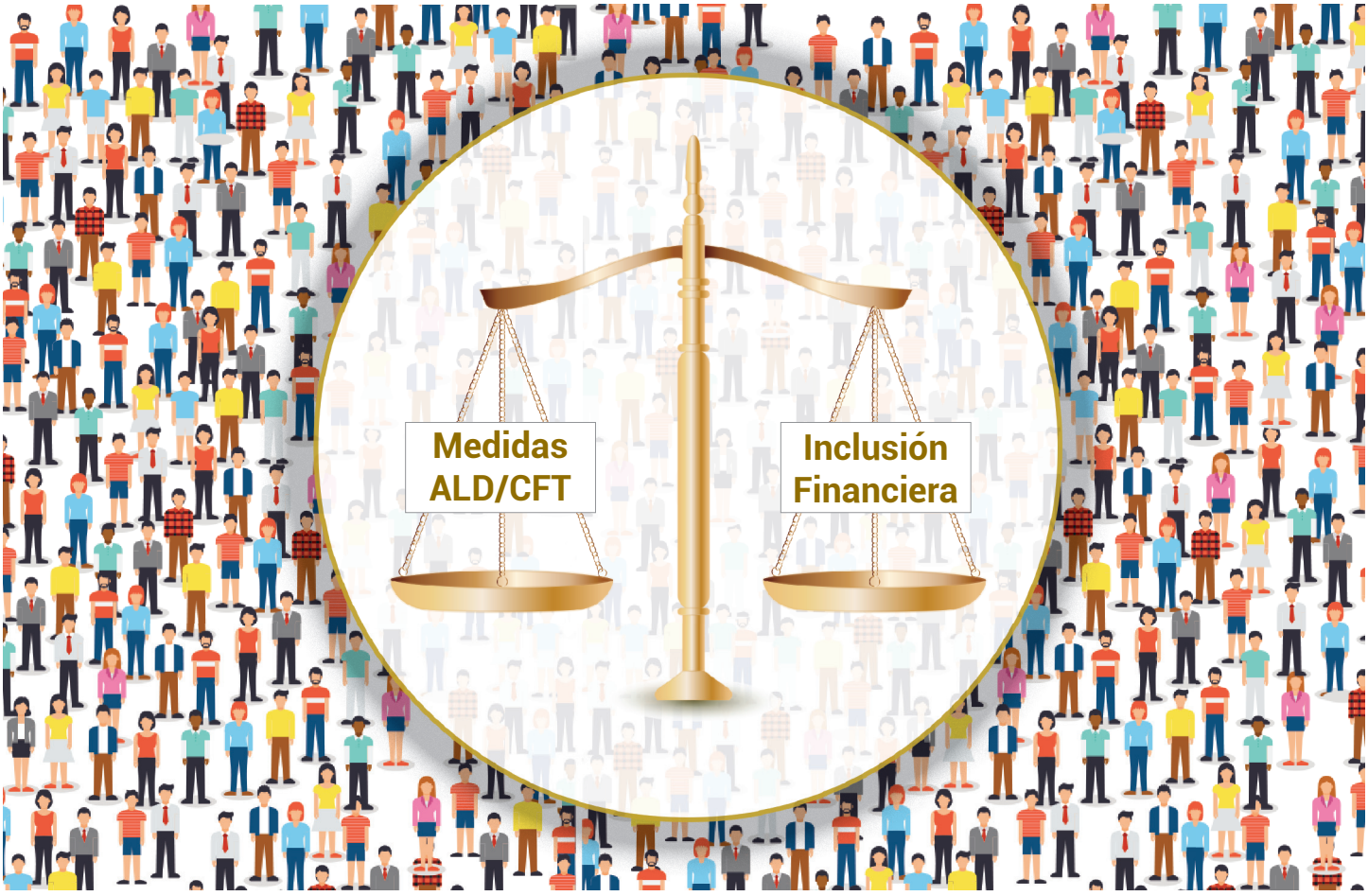
Juan David Barrueto Godoy

*Contador Público y Auditor egresado de la Universidad de San Carlos de Guatemala. Maestría en Administración de Empresas con especialización en Finanzas, con mención honorífica *Magna Cum Laude* por la Universidad Francisco Marroquín de Guatemala y Máster Universitario en Gestión y Técnica de Seguros, por la Universidad Pontificia de Salamanca, España. Ha realizado estudios de especialización en el extranjero en temas relacionados con: supervisión de riesgos de seguros, supervisión bancaria, supervisión y evaluación de riesgos del sistema financiero; y, operaciones de banca central, entre otros. Ingresó a la Superintendencia de Bancos en 1995 y ha desempeñado los puestos de Inspector, Supervisor de Área y Director en varios departamentos relacionados con la labores de supervisión de riesgos. Actualmente, tiene a su cargo la coordinación de la supervisión de las aseguradoras, el banco central y otras entidades. Es Director del Departamento de Supervisión de Riesgos de Seguros y Otros de la Superintendencia de Bancos.

Artículo

Importancia del equilibrio entre las medidas Anti-Lavado de Dinero/Contra el Financiamiento del Terrorismo (ALD/CFT) y la inclusión financiera

Claudia María Rosales Flores de Díaz*



¿Existe correlación entre las medidas Anti-Lavado de Dinero/ Contra el Financiamiento del Terrorismo y la inclusión financiera? ¿Por qué debe haber un equilibrio entre ambos? Aparentemente son ajenos entre ellos, pero al profundizar en su estudio resulta evidente su relación.

El lavado de dinero consiste en el encubrimiento del origen ilegal de recursos generados en actos delictivos, con el fin de disfrutar sus beneficios sin atraer la atención hacia la actividad o a las personas involucradas. Este impacta la economía y la sociedad de cada nación, generando distorsiones en los mercados, debilitamiento de las instituciones financieras, riesgos para la reputación del país, violencia, aumento de la corrupción, entre otros.

Además, sus efectos negativos tienen alcance mundial; quienes blanquean dinero y financian el terrorismo se aprovechan de la complejidad del sistema financiero global y de las

diferencias que existen entre las leyes y los sistemas nacionales ALD/CFT (Fondo Monetario Internacional, 2016).

Por ello, en 1989 se creó el órgano intergubernamental denominado Grupo de Acción Financiera Internacional (GAFI), cuyo objetivo es *"fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación y otras amenazas a la integridad del sistema financiero internacional" (Financial Action Task Force, 2012).* En 1990 se emitieron las recomendaciones originales del GAFI que incluyen medidas ALD/CFT y cuya versión vigente fue aprobada en 2012.

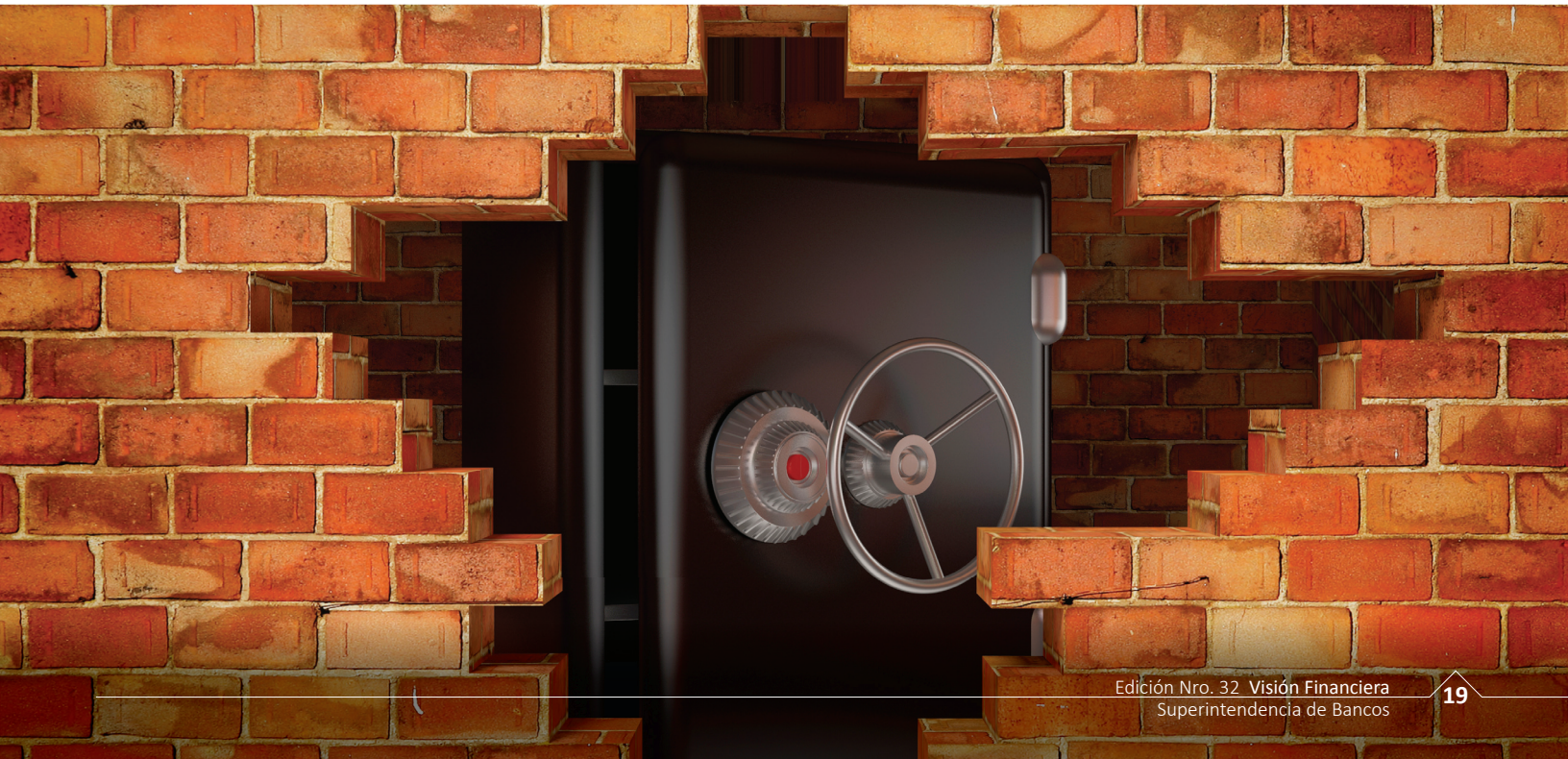
Las Recomendaciones del GAFI son aplicadas por los países debido a su carácter de estándar internacional, lo cual da lugar a que se lleven a cabo evaluaciones mutuas que consisten en la verificación del nivel de implementación de las medidas ALD/CFT, y son relevantes, ya que permiten identificar aspectos de mejora tanto específicos del país, como generalizados entre naciones.

En las evaluaciones realizadas del 2005 al 2011 sobresalió que los países introdujeron requerimientos uniformes en sus sistemas ALD/CFT, es decir, incorporaron requisitos que aplican para todos, independientemente de su riesgo (*Financial Action Task Force*, 2017).

Asimismo, según Koker & Isern 2009, se ha identificado una aplicación inadecuada de las normas internacionales ALD/CFT; por ejemplo, la exigencia de conservar copias impresas de la verificación de la identidad de los clientes, los registros de las transacciones y documentos que comprueben el domicilio de los mismos; *"El documento nacional de identidad no es un requisito previo para contar con un marco eficaz de lucha contra el Lavado de Dinero (LD) y el Financiamiento del Terrorismo (FT), pero la ausencia de documentación de identidad confiable o de fuentes accesibles para verificar la identidad de las personas complica el proceso de debida diligencia con los clientes, aumenta los costos para el cumplimiento de los requisitos y menoscaba la eficacia de las medidas contra el LD y el FT" (de Koker & Isern, 2009).* En consecuencia, las instituciones financieras se preocupan por su rentabilidad y su reputación, dando como resultado *De-risking*[1] y a la vez exclusión financiera.

Es preciso comprender que la inclusión financiera se refiere al acceso que tienen los grupos vulnerables y desfavorecidos a una gama adecuada de servicios financieros convenientes, seguros y asequibles (*Financial Action Task Force*, 2017). Su importancia radica en la influencia que tiene, por ejemplo: en el crecimiento económico a largo plazo de forma sostenida de los países; en la disminución de los índices de pobreza e informalidad; y, en el aumento del recaudo fiscal sin afectar el nivel agregado de consumo y de ahorro (FELABAN, 2018). Asimismo, el

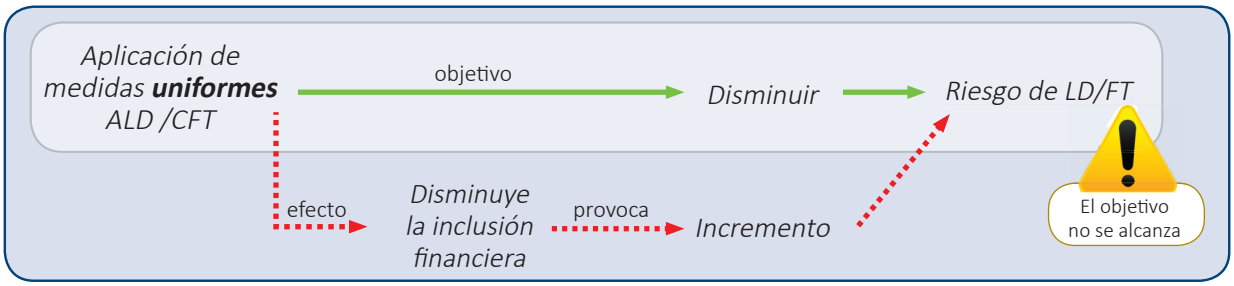
1 *De-risking*: se refiere al fenómeno que consiste en que las instituciones financieras prefieren evitar el riesgo y derivado de ello terminan o restringen las relaciones con los clientes, en lugar de implementar un Enfoque Basado en Riesgo. (*Financial Action Task Force*, 2014)



Banco Mundial ha calificado el tema como un elemento clave para reducir la pobreza e impulsar la prosperidad gracias a su aporte a 7 de los 17 Objetivos de Desarrollo Sostenible[2].

El *De-risking* es de crucial importancia para el GAFI por dos razones principales: 1) puede introducir riesgo y opacidad en el sistema financiero, ya que la terminación de las relaciones con los clientes provoca que las personas utilicen canales menos regulados o no regulados; y, 2) es esencial para su mandato asegurar que el estándar global ALD/CFT sea comprendido correctamente e implementado de forma acertada (*Financial Action Task Force*, 2014).

Entonces, para definir el problema es necesario identificar tres variables que interactúan entre sí: las medidas ALD/CFT, el riesgo de LD/FT y la inclusión financiera, observándose que con las medidas uniformes implementadas, se espera disminuir el riesgo de LD/FT; no obstante, las medidas limitan la inclusión financiera, y cuando esto sucede, el riesgo aumenta, razón por la cual no se alcanza el objetivo original.



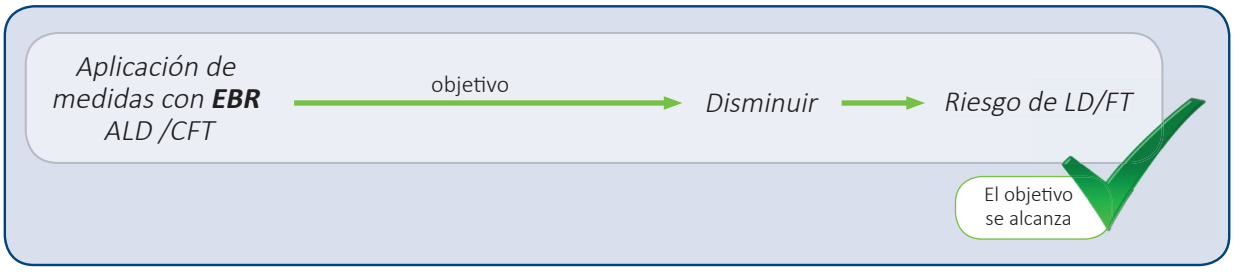
Fuente: Elaboración propia del autor.

Lo anterior ocurre debido a que las medidas uniformes limitan a las personas vulnerables el acceso a servicios y productos financieros, provocando exclusión financiera, la que aumenta el riesgo de LD/FT porque las regulaciones son aplicables a menos individuos; la información disponible para monitoreo, análisis y persecución es menor; y, se desarrollan mercados informales.

De la misma manera, las estrategias para la inclusión financiera también podrían tener efectos nocivos en el riesgo de LD/FT en caso de no haberlo considerado en su diseño, ya que se pueden crean medios que faciliten a los criminales la colocación y estratificación de los fondos.

Además, es importante aclarar que, tanto las medidas ALD/CFT como la inclusión financiera buscan el mismo objetivo último, que es el bienestar social; así pues, debe existir un equilibrio entre las medidas y la inclusión financiera.

Este se alcanza a través de la adecuada implementación de la Recomendación 1: *Evaluación de Riesgo y aplicación de un Enfoque Basado en Riesgo (EBR)*, ya que indica que los países deben aplicar medidas intensificadas donde haya mayor riesgo, y del mismo modo, en caso de riesgos bajos se deben permitir medidas simplificadas; es decir que, la intensidad de las medidas ALD/CFT dependen del nivel y la naturaleza del riesgo (*Financial Action Task Force*, 2017). Esto evita que los requerimientos difíciles de cumplir sean aplicados innecesariamente a personas vulnerables, de ahí que no se ocasiona un impacto perjudicial en la inclusión financiera, por consiguiente, tampoco en el riesgo de LD/FT.



Fuente: Elaboración propia del autor.

2 Los Objetivos de Desarrollo Sostenible son una iniciativa impulsada por Naciones Unidas para dar continuidad a la agenda de desarrollo tras los Objetivos de Desarrollo del Milenio, son un llamado universal a la adopción de medidas para poner fin a la pobreza, proteger el planeta y garantizar que todas las personas gocen de paz y prosperidad.

Por tal motivo, se han identificado retos para lograr ese balance. En el informe de CENFRI 2018, se analizan, entre otros aspectos, los siguientes:

- Dificultades para la adopción del EBR derivado de las limitaciones establecidas en el marco regulatorio; así como del eslogan "cero tolerancia al incumplimiento", utilizado en el pasado por las instituciones financieras y los supervisores, ya que en un amplio sentido puede interpretarse como "cero tolerancia al riesgo".
- Los extensos períodos de tiempo requeridos para modificar el marco normativo ALD/CFT, ya que implica continuar con la legislación vigente a pesar de sus falencias.

Llegados a este punto, es posible comprender que la relación existente entre las medidas ALD/CFT y la inclusión financiera se debe a la influencia nociva que cada una puede ejercer sobre la otra; pero también se comprende que ambas buscan el bienestar social, por lo que para lograr este objetivo es necesario encontrar y mantener un equilibrio entre ellas.

Claudia María Rosales Flores de Díaz

*Licenciada en Contaduría Pública y Auditoría con Maestría en Administración Industrial, ambos títulos otorgados por la Universidad Rafael Landívar. Posee experiencia en temas de Lavado de Dinero y Financiamiento del Terrorismo. Es Inspectora del Departamento de Análisis de Transacciones Financieras de la Intendencia de Verificación Especial (IVE) de la Superintendencia de Bancos..

Estrategia *Multicloud*

Nefy David Morales Recinos*

En la actualidad hablar de servicios tecnológicos hospedados en la nube ya no es una tendencia, tampoco se trata de hablar del futuro, hoy por hoy es una estrategia implementada por algunas organizaciones debido a que brinda diversas ventajas competitivas. Por ello, muchas organizaciones ya no están invirtiendo en la adquisición de equipos de cómputo o construcción de centros de datos, en su lugar están implementando sus servicios tecnológicos en la nube. Una publicación del 24 de agosto de 2018 por IDC[1], proyecta para Latinoamérica un crecimiento del 38.6% en la adopción de cómputo en la nube para el 2019.

¿Qué es la nube?

"La nube o cloud es un conjunto de diferentes tipos de hardware y software que funcionan colectivamente para ofrecer aspectos de la informática como ***servicio en línea*** *al usuario final. La computación cloud se trata del uso de hardware y software para proveer un servicio en red (típicamente, Internet)", (Lenovo, 2019).*

1 *International Data Corporation (IDC),* es una firma mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo. http://www.idclatin.com/releases/news.aspx?id=2388 https://www.idc.com/getdoc.jsp?containerId=prUS44971119

Los principales tres tipos de nube son: pública, privada e híbrida.

Nube pública

Es una infraestructura tecnológica compartida propiedad de un proveedor de nube, se sustituye el paradigma de adquirir *hardware* y *software* por la contratación de servicios. Para este tipo de nube la gestión de infraestructura física es responsabilidad de quien ofrece el servicio. Los requerimientos de las compañías son estipulados a través de acuerdos de nivel de servicio con el proveedor de nube. Entre los principales beneficios de esta modalidad se encuentran la escalabilidad, el pago únicamente por lo utilizado y ahorro en los costos de mantenimiento y reparación de los equipos de cómputo.

Nube privada

Este tipo de nube es suministrada por infraestructura que es propiedad de la organización, siendo esta la única responsable de su administración y mantenimiento. A diferencia del tipo anterior, en este, el reto es la gestión de la capacidad tecnológica, por ende las compañías deben prever cierta holgura en la adquisición de tecnología por lo que la subutilización de la infraestructura tecnológica es muy común, los recursos son escasos y la implementación de nuevos proyectos puede que no sea oportuna.

Nube híbrida

Como su nombre lo sugiere, este modelo es la combinación de la nube pública y privada. Al utilizar este tipo, las organizaciones pueden aprovechar las capacidades de cada tipo de nube para potenciar la flexibilidad y la escalabilidad.

Los principales modelos del servicio de nube son los siguientes:

- ***Software* como Servicio (SaaS).** El acceso a este tipo de servicios es por medio de un navegador *web*, no requiere la instalación de aplicaciones de escritorio, la disponibilidad del servicio es responsabilidad del proveedor en nube y la gestión de accesos recae sobre la organización.
- **Plataforma como Servicio (PaaS).** Proporciona a las organizaciones una plataforma para la creación y hospedaje de *software*, siendo el proveedor de la nube el encargado de la gestión de red, almacenamiento, virtualización, sistema operativo y las herramientas de desarrollo.
- **Infraestructura como Servicio (IaaS).** Provee los componentes de infraestructura tales como, procesamiento, almacenamiento, red y virtualización; el mantenimiento de los equipos de cómputo físicos es responsabilidad del proveedor de nube y el *software* es administrado por la empresa que contrata el servicio.

Uno de los retos principales para quienes gestionan la tecnología es decidir qué tipo y modelo de implementación de nube se utilizará, por temas de escalabilidad, costos asociados en mantenimiento de *hardware*, tiempo requerido para gestionar los equipos físicos de cómputo, el tipo de servicio tecnológico que se quiere brindar, etc.

La nube pública es una alternativa a considerar, debido a que se pueden obtener beneficios como el crecimiento de los recursos de cómputo a demanda de una forma oportuna, reducción en el tiempo de implementación de nuevas soluciones tecnológicas respecto a la utilización de infraestructura propia, entre otras; según IDC, para el 2023 el 60% de implementaciones de infraestructura tecnológica a nivel mundial se hará sobre la nube pública.

Algunos de los principales proveedores de nube son, *Google Cloud*, *Amazon Web Services*, *Microsoft Azure*, *Oracle Cloud*, *IBM Cloud*. Cada proveedor ofrece de forma particular el servicio de cómputo en la nube, ya sea por la ubicación donde se encuentran sus centros de datos, por la cantidad de servicios que brindan, o por el cumplimiento de estándares internacionales, entre otros.

En el momento que una organización decida utilizar la computación en la nube se enfrentará a la disyuntiva sobre qué proveedor puede responder a sus necesidades particulares como empresa o incluso por cada uno de los servicios tecnológicos que se estén considerando, por lo que el resultado del análisis que se realice puede determinar que la estrategia a utilizar sea *Multicloud*.

¿Qué es *Multicloud*?

Es una forma de adoptar la nube con el objetivo de aprovechar lo mejor de cada proveedor. Las organizaciones optan por el uso de distintos proveedores en la nube para soportar diferentes aplicaciones y hacer uso de la solución que mejor se adapte a sus necesidades.

Ventajas

- Oportunidad de aprovechar lo mejor de cada proveedor de nube.
- Agilidad en el aprovisionamiento de infraestructura.
- Distribución del riesgo.
- Alta disponibilidad y mayor resiliencia.

Desventajas

- Gestionar con más de un proveedor de nube los diferentes contratos de servicio.
- Complejidad en la administración de infraestructura.

Al decidir la adopción de *Multicloud* es necesario la creación de un entorno de gobernanza, capaz de enmarcar toda la operación tecnológica de la organización, por lo que es preciso el establecimiento de procesos y procedimientos que permitan la gestión tecnológica transversal de las diferentes soluciones de nube que se contraten.

Otro aspecto importante es lograr una adecuada interconectividad entre los servicios, ya que estos por estar alojados en diferentes nubes requieren que la comunicación fluya adecuadamente para evitar que exista latencia significativa.

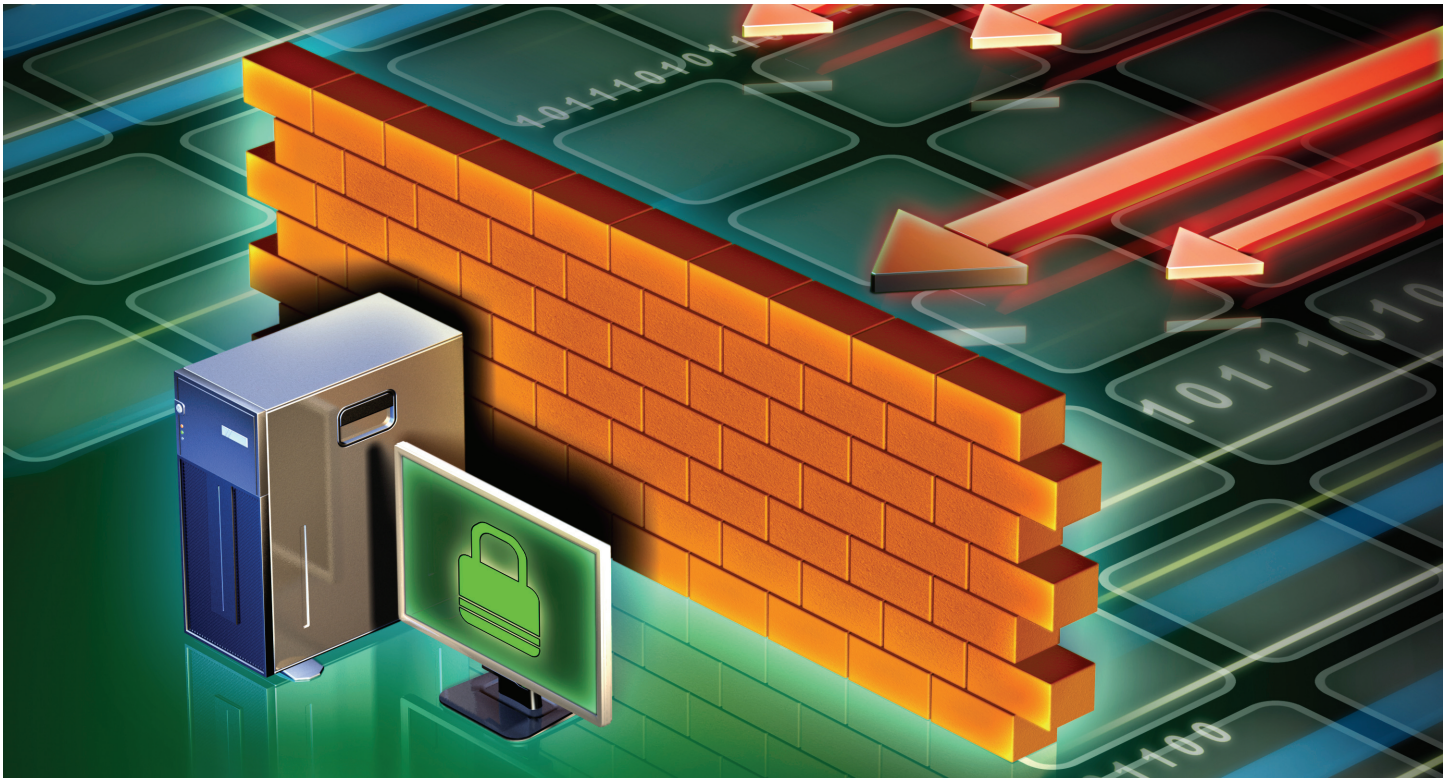
Por último, al momento de migrar o planear la implementación de servicios en la nube es importante que las organizaciones realicen un análisis integral para decidir qué tipo o modelo de nube le conviene utilizar dependiendo de los servicios tecnológicos que requieran implementar.

Nefy David Morales Recinos

*Licenciado en Administración de Sistemas de Información por la Universidad Mariano Gálvez de Guatemala. Certificado como Auditor Líder ISO/IEC 27001:2005, participación en la implementación de Sistemas de Gestión ISO/IEC 20000-1:2011 e ISO/IEC 27000:2013. Posee experiencia en manejo y administración de bases de datos, infraestructura tecnológica y migración de servicios tecnológicos a nube. Es Profesional del Departamento de Tecnología de la Información de la Superintendencia de Bancos.

El gobierno corporativo y la gestión de la seguridad de la información

Carlos Humberto Martínez Molina*



En esta época en donde se está desarrollando la cuarta revolución industrial[1], la era de la inteligencia artificial, está claro que dependemos en gran medida de la tecnología de la información y de las telecomunicaciones.

La transformación digital es el método por el cual las organizaciones empresariales, de gobierno o entidades no lucrativas conducen cambios en sus modelos de negocio y de los ecosistemas mediante la utilización de las competencias digitales.

La dependencia de las organizaciones para realizar sus transacciones por medio de plataformas digitales las ha hecho propensas a ataques cibernéticos, en los cuales, la denegación de servicio, robo de datos, recursos monetarios, pérdida de propiedad intelectual, entre otros, hace necesaria la protección de los activos en el ciberespacio, mediante una política y estrategia de seguridad de la información y de ciberseguridad. En ese contexto, es importante que las organizaciones empresariales, de gobierno o entidades no lucrativas, establezcan un adecuado control de su información para preservar su confidencialidad, integridad y disponibilidad. Cabe indicar que la existencia de un gobierno corporativo

1 El concepto Cuarta Revolución Industrial fue acuñado por Klaus Martin Schwab, fundador del Foro Económico Mundial en el contexto de la edición del Foro Económico Mundial 2016. La primera, utilizó el agua y el vapor para mecanizar la producción. La segunda, usaba energía eléctrica para crear la producción en masa. La tercera, la electrónica y la tecnología de la información para automatizar la producción. Ahora, una cuarta basada en la tercera, la revolución digital que se está produciendo desde mediados del siglo pasado, se caracteriza por una fusión de tecnologías que está difuminando las líneas entre las esferas física, digital y biológica. (www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-*what-i t-means-and-how-to-respond*/)

eficiente es un elemento esencial para el funcionamiento efectivo de cualquier institución, así como para la correcta gestión de los riesgos. Por ello, se considera que junto con la calidad de la gestión y el control interno son elementos que mitigan los riesgos, incluyendo los ciberataques, los cuales, mediante la política, estrategia y roles, deben centrarse en prevenir y no solo en detectar. Por lo tanto, el gobierno corporativo debe tener la capacidad de gestionar y dirigir iniciativas digitales, realizar innovación disruptiva en su industria, proporcionando mayor agilidad y valor competitivo al negocio.

En tal sentido, es recomendable que la estructura organizacional de la seguridad de la información corporativa sea liderada por el *CISO* (*Chief Information Security Officer*), cuya función, entre otras, es gestionar la seguridad de la información de la organización y su alineación con los objetivos del negocio; bajo su liderazgo deberían existir, entre otras, áreas como: *Governance & Risk*, encargada del manejo de políticas, procedimientos y administración de riesgos de ciberseguridad; *Strategic Change Program*, encargada de participar en los procesos de cambios en infraestructura y sistemas de información para velar por la continuidad de la seguridad; *Cyber Threat Intelligence*, encargada de analizar tendencias y amenazas para tomar decisiones anticipadas relacionadas con ataques cibernéticos; *Cyber Assurance Testing*, encargada de realizar pruebas de seguridad y de vulnerabilidades en equipos, procesos y personas; *Security Operation*, encargada del manejo y gestión del SOC (*Security Operation Center*) para monitorear la seguridad de la red de la organización e Internet; y, *Group Data Protection Officer*, encargada de definir la clasificación de información e implementación de controles para prevenir la modificación o divulgación no autorizada de información.

Dentro de la estructura de la organización, se recomienda crear comités de apoyo al consejo de administración que se encarguen de la toma de decisiones y que escalen según los niveles de criticidad; estos comités tienen que tener las competencias necesarias para dar recomendaciones sobre riesgos tecnológicos incluyendo seguridad de información y ciberseguridad; evaluar la eficiencia del área de tecnología y el programa de administración del riesgo operacional; supervisar los programas para asegurar que los controles sean manejados y gestionados; asimismo, implementar y mantener el programa que asegure cubrir los objetivos para la ciberseguridad y que estos estén alineados a la estrategia de la entidad.

En este sentido, se esperaría que las organizaciones empresariales, de gobierno o entidades no lucrativas cuenten con un marco para la gestión integral de la seguridad de la información formalmente establecido, que proporcione una visión completa de lo que se entenderá por ciberseguridad, estableciendo los lineamientos para identificar, proteger, detectar, responder y recuperar la información, definiendo las políticas, procesos, procedimientos y controles para su cumplimiento. La implementación de dicho marco de gestión requerirá que las organizaciones antes indicadas cuenten con una cultura de gestión de riesgos y de control interno sólida, cuya promoción estará a cargo de las máximas autoridades de la institución.

Además, debe fomentarse el cumplimiento de normas éticas que promuevan la integridad del personal en la realización de sus actividades diarias; para lograrlo se recomienda el entrenamiento continuo del personal en seguridad de la información y privacidad, programas de concientización y simulaciones de *phishing*[2], entre otras.

2 El *phishing* es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima. (https://www.segu-info.com.ar/malware/phishing.htm)

Las políticas de seguridad deben ser conocidas por todo el personal de una organización mediante un programa permanente de concientización. En el contenido de los documentos deben estar claramente establecidos: el objetivo, los responsables de cumplimiento y las medidas que se aplicarán en caso de incumplimiento.

Con el fin que las entidades del sistema financiero supervisado en Guatemala cuenten con políticas para la gestión de la seguridad de la información, la Junta Monetaria emitió el Reglamento para la Administración del Riesgo Tecnológico, contenido en la Resolución JM-102-2011. Esta normativa, entre otros aspectos, establece los lineamientos mínimos que dichas entidades deben observar en la organización para la administración del riesgo tecnológico; en la infraestructura de Tecnologías de la Información (TI), sistemas de información, bases de datos y servicios de TI; seguridad de la tecnología de información; continuidad de operaciones de TI; y, procesamiento de información y tercerización.

Como complemento y para reforzar la gestión de riesgos, la Junta Monetaria emitió la Resolución JM-62-2016, Reglamento de Gobierno Corporativo, el cual busca promover que los bancos y las empresas que integran los grupos financieros, implementen prácticas sanas y eficientes, conforme los estándares internacionales en la materia, para coadyuvar a la gestión efectiva de sus actividades, al fortalecimiento de los niveles de confianza del mercado, a la protección y trato equitativo de los intereses de accionistas, depositantes y clientes en general y a la estabilidad del sistema financiero; asimismo, para que los bancos y grupos financieros cuenten con sólidas políticas y procesos en materia de gobierno corporativo que abarquen, entre otros aspectos, la dirección estratégica, la estructura de grupo y organizativa, el entorno de control, las atribuciones del consejo y la alta dirección, así como las retribuciones. Estas políticas y procedimientos deben estar en consonancia con el perfil de riesgo y la importancia sistémica del banco.

En conclusión, la transformación digital en esta nueva era, está motivando a las entidades a desarrollar nuevas tecnologías para acoplarse a los requerimientos del mercado, lo cual los hace más vulnerables ante los ataques cibernéticos que de igual manera se hacen cada vez más comunes, por lo que la seguridad de la información retoma un papel de vital importancia, la cual no está supeditada a la información de tecnología solamente, sino que incluye toda la información que genera la organización, incluyendo la de su personal, lo cual requiere la implementación de un eficiente gobierno corporativo y políticas de seguridad que se desarrollen con el fin de preservar los sistemas y garantizar la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las normas y las responsabilidades en todos los niveles de la organización.

Carlos Humberto Martínez Molina

*Contador Público y Auditor *Master of Business Administration Minor in finance*, ambos títulos otorgados por la Universidad Francisco Marroquín. Ha participado en diversos diplomados relacionados con banca central, inversión de portafolios, mercado de derivados y *commodities* del Centro de Estudios Monetarios Latinoamericanos (CEMLA), Banco de España, *Federal Reserve Bank of New York y Securities and Exchange Commission*. Posee experiencia en auditoría de estados financieros, evaluaciones de control interno, supervisión basada en riesgos de bancos, financieras, banca central y portafolios de inversiones. Es Profesional del Departamento de Supervisión de Riesgos de Seguros y Otros de la Superintendencia de Bancos.

LA SUPERINTENDENCIA DE BANCOS
INFORMA QUE:

En Guatemala solamente las entidades aseguradoras autorizadas conforme la ley y supervisadas por la Superintendencia de Bancos, pueden vender pólizas de seguros.

COMPAÑÍAS DE SEGUROS AUTORIZADAS*

1. Departamento de Seguros y Previsión de El Crédito Hipotecario Nacional de Guatemala
2. Seguros G&T, S. A.
3. BMI Compañía de Seguros de Guatemala, S. A.
4. Seguros Universales, S. A.
5. ASSA Compañía de Seguros, S. A.
6. Pan-American Life Insurance de Guatemala, Compañía de Seguros, S. A.
7. Ficohsa Seguros, S. A.
8. Aseguradora General, S. A.
9. Seguros El Roble, S. A.
10. Aseguradora Guatemalteca, S. A.
11. Aseguradora Confío, S. A.
12. Aseguradora La Ceiba, S. A.
13. Aseguradora de los Trabajadores, S. A.
14. Columna, Compañía de Seguros, S. A.
15. MAPFRE | Seguros Guatemala, S. A.
16. Seguros Agromercantil, S. A.
17. Aseguradora Rural, S. A.
18. Departamento de Fianzas de El Crédito Hipotecario Nacional de Guatemala
19. Afianzadora Guatemalteca, S. A.
20. Afianzadora G&T, S. A.
21. Aseguradora Fidelis, S. A.
22. Aseguradora Solidum, S. A.
23. Fianzas El Roble, S. A.
24. Seguros Privanza, S. A.
25. Seguros Confianza, S. A.
26. Aseguradora Solidaria, S. A.
27. Afianzadora de la Nación, S. A.
28. Bupa Guatemala, Compañía de Seguros, S. A.

*Al 31 de mayo de 2019. Para más información visite nuestro sitio web: www.sib.gob.gt

Contrato de seguro.

El contrato de seguro es el acuerdo por el cual una persona traslada a la aseguradora un riesgo (posibilidad de que ocurra o no un acontecimiento), que no depende de su voluntad y que puede causarle daños personales o materiales. En caso de ocurrir, la aseguradora está obligada, de conformidad con las condiciones pactadas en el contrato de seguro (póliza de seguro) a indemnizar, reparar o compensar al asegurado o beneficiario. Las condiciones generales del seguro, deben estar registradas en la Superintendencia de Bancos.

Al respecto, el artículo 874 del Código de Comercio de Guatemala, prescribe que por el contrato de seguro, el asegurador se obliga a resarcir un daño o a pagar una suma de dinero al realizarse la eventualidad prevista en el contrato, y el asegurado o tomador del seguro, se obliga a pagar la prima correspondiente.

Delito de intermediación de seguros.

El artículo 92 de la Ley de la Actividad Aseguradora, establece que comete delito de intermediación de seguros toda persona individual o jurídica, nacional o extranjera, que vende o coloca contratos de seguros en Guatemala, de aseguradoras no autorizadas para operar en el país.

Delito de colocación o venta ilícita de seguros.

El artículo 93 de la citada ley, establece que comete delito de colocación o venta ilícita de seguros, toda persona, nacional o extranjera, que por sí misma o a través de otras, coloque o vende seguros en territorio guatemalteco, sin estar autorizada para actuar como aseguradora en el país, independientemente de la forma jurídica de formalización, del nombre o la denominación que se le de a la negociación o transferencia del riesgo asegurable, de la instrumentación o registro contable.