



VISION[®]

Financiera

Edición Nro. 30 • Año 7 Guatemala - diciembre 2018

Aspectos fundamentales de la gestión del riesgo de liquidez en las entidades bancarias

Pág. 11

La gestión del riesgo de mercado como una herramienta gerencial en la banca

Pág. 8

La actividad fiduciaria y los principales riesgos asociados

Pág. 18

La incidencia de la nube en los planes de continuidad de tecnología

Pág. 25



Superintendencia de Bancos Guatemala, C. A.

Contenido

- 03 Presentación
- 04 Pluma invitada Normas Internacionales de Información Financiera (NIIF)
- 08 Artículo La gestión del riesgo de mercado como una herramienta gerencial en la banca
- 11 Tema central Aspectos fundamentales de la gestión del riesgo de liquidez en las entidades bancarias
- 15 Artículo Supervisión consolidada de grupos financieros y riesgos asociados
- 18 Artículo La actividad fiduciaria y los principales riesgos asociados
- 21 Tecnología Ciberseguridad en el sector financiero
- 25 Actualidad La incidencia de la nube en los planes de continuidad de tecnología

Directorio

Director General

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Consejo Editorial

Lic. Hugo Daniel Figueroa Estrada
Intendente de Coordinación General

Lic. Hugo Rafael Oroxóm Mérida
Intendente de Estudios y Normativa

Inga. Xiomara Noemí Cabrera de Anzueto
Directora del Departamento
de Desarrollo Institucional

Lcda. Claudia Larissa Zúñiga Aragón
Supervisora en funciones, Departamento
de Desarrollo Institucional

Oficina de Atención al Usuario

9.ª Avenida 22-00, zona 1, Guatemala, C. A.
PBX: 2429-5000 y 2204-5300
Ext. 1+2550/2551/2552 Fax: 2232-0002
Correo electrónico: info@sib.gob.gt
www.sib.gob.gt

Si requiere recibir información de la
Superintendencia de Bancos
suscríbese:



Al correo electrónico:
comunicacion@sib.gob.gt



Al teléfono: 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.

**“Usted ahorra,
los bancos cuidan su dinero,
la SIB supervisa”**

En la presente edición de la revista *Visión Financiera*, el tema central se relaciona con la gestión del riesgo de liquidez en las entidades bancarias. Conforme lo describen los tratadistas, el riesgo de liquidez consiste en la posibilidad de incurrir en pérdidas, derivado de la carencia de activos líquidos suficientes para que, en un horizonte de tiempo determinado, se pueda hacer frente a las obligaciones contraídas. Por la naturaleza de su operación de intermediación, las entidades financieras se encuentran particularmente expuestas a este riesgo, de manera individual o sistémica, ya que su actividad incluye la captación de fondos de la población, lo cual puede generar crisis originarias de eventos severos y masivos que se constituyan en requerimientos de inyección de liquidez a costos no previstos que impacten en la situación financiera de las entidades o del sistema financiero en general.

En ese sentido, el Lic. Luis Francisco Vallejo García, Inspector del Departamento de Supervisión de Riesgos Específicos de la SIB, desarrolla como tema central el artículo titulado “Aspectos fundamentales de la gestión del riesgo de liquidez en las entidades bancarias”, en el cual nos comparte la importancia de la gestión de dicho riesgo de manera prospectiva, la cual debe evaluarse en un contexto de escenarios, adoptando metodologías robustas.

Como pluma invitada, contamos con la valiosa participación del Dr. Jorge Pérez Ramírez, responsable del Programa de Asistencia Técnica del Centro de Estudios Monetarios Latinoamericanos (CEMLA), quien expone ampliamente no solo el origen, evolución e importancia de las “Normas Internacionales de Información Financiera (NIIF)”, sino también comparte su opinión sobre la



Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

adopción y desventajas en la aplicación de dichas normas en el sistema financiero guatemalteco e hipótesis fundamentales como el devengo y la empresa en funcionamiento.

Por su parte, el Lic. Edgar René Guevara Recinos, Profesional del Departamento de Normativa de la SIB, presenta el tema “La gestión del riesgo de mercado como una herramienta gerencial en la banca”, en el cual expone, en adición a la definición técnica del riesgo de mercado, las fuentes generadoras del mismo, así como los métodos de medición de dichas fuentes, concluyendo, entre otros aspectos, que las entidades bancarias deben contar con una estructura administrativa que les permita gestionar y mitigar oportunamente dicho riesgo.

Los licenciados Ana Luisa Sical Guerra de Fernández, del Departamento “A” de Supervisión de Riesgos Bancarios, y Julio Antonio Cantoral López, del Departamento de Normativa, ambos Inspectores de la SIB, desarrollan el artículo “Supervisión consolidada de grupos financieros y riesgos asociados”, a través del cual exponen la definición de grupo financiero, los riesgos asociados y los principales retos para el supervisor bancario que, entre otros aspectos, deberá considerar la idoneidad de los administradores,

directores y accionistas de las entidades, evaluando la solvencia, honorabilidad, conocimiento y experiencia de los respectivos negocios.

La Lcda. Ana Luisa De León Enríquez, Inspectora de Riesgo Legal del Departamento de Riesgos Específicos de la SIB, desarrolla el tema “La actividad fiduciaria y los principales riesgos asociados”, en el cual nos orienta sobre cómo mitigar los riesgos asociados al negocio fiduciario.

En materia tecnológica, el Ing. Daniel Augusto Monzón Pérez, Inspector de Riesgo Tecnológico del Departamento de Supervisión de Riesgos Específicos de la SIB, presenta el artículo “Ciberseguridad en el sector financiero”, en el cual describe la definición de ciberseguridad y cómo gestionarla, además de la importancia de esta para garantizar que se alcancen y mantengan las propiedades de seguridad de los activos de la organización.

Para concluir, en la sección de actualidad el Ing. Luis César Vielman Monroy, Supervisor del Departamento de Tecnología de la Información de la SIB, expone sobre “La incidencia de la nube en los planes de continuidad de tecnología”, considerando aspectos normativos de importancia sobre el plan de continuidad de operaciones de tecnología de la información o plan de recuperación ante desastres; el diseño e implementación de servicios en la nube; y, la adopción de buenas prácticas y estándares en seguridad de la información.

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

Atentamente,

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos



Normas Internacionales de Información Financiera (NIIF)

Entrevista al Dr. Jorge Pérez Ramírez*
Responsable Técnico del Programa
de Asistencia Técnica del CEMLA

1. ¿En términos generales, qué son las NIIF?

El origen de las NIIF se encuentra en el deseo de encontrar un marco contable común para las empresas que buscan financiación en los mercados de capitales internacionales mediante la emisión de acciones, bonos o cualquier otro valor al que se pretenda, con posterioridad a su emisión, otorgar la liquidez que ofrece su negociación en una bolsa de valores. De esta manera, en junio de 1973 se creó el IASC (*International Accounting Standards Committee*), actualmente IASB (*International Accounting Standards Board*) pero, a pesar de sus esfuerzos,

durante treinta años sus normas no fueron ignoradas. No sería hasta el 2003 cuando se produce su primer reconocimiento internacional en el momento en que las autoridades de la Unión Europea (UE), en su deseo de crear un mercado único de capitales en la UE, decidieron que las normas emitidas por el IASB serían de obligado cumplimiento para entidades que tuvieran valores admitidos a negociación en cualquier bolsa europea, pero solo y únicamente para formular sus “cuentas consolidadas”.

Querría precisar dos aspectos en relación con la aplicación de las NIIF en la Unión Europea. La primera es que las normas del IASB que se aplican

en la UE deben previamente pasar por un proceso de refrendo y aprobación legal (incluida su publicación en el Diario Oficial de la UE) antes de poder ser utilizadas por una entidad europea para formular sus cuentas consolidadas. La segunda cuestión es que los estados contables individuales de las empresas europeas se formulan de acuerdo con las normas contables de cada uno de los países miembros de la UE y no de acuerdo a las NIIF, aunque en algunos de ellos las normas nacionales puedan tener disposiciones comunes o coincidentes con las NIIF.

A diferencia de lo que ocurre en los Estados Unidos de América (EE.UU.), donde las normas contables



del FASB (*Financial Accounting Standards Board*) se aplican bajo supervisión del regulador del mercado de ese país, la SEC (*Securities and Exchange Commission*), las NIIF no están adaptadas a ninguna legislación nacional (civil, mercantil, de mercado de capitales, etc.) ni a las exigencias de una autoridad reguladora de los mercados exigente y rigurosa como la SEC de los estadounidenses. Ello explica que las NIIF sean normas muy generales basadas en principios, a veces vagos e imprecisos, a diferencia de las normas FASB que son más desarrolladas, precisas, con algunas reglas y orientadas al mercado de capitales de los EE.UU., el más importante del mundo.

Por último, la esencia y relevancia de las NIIF no está en la elaboración de un balance, una cuenta de resultados, entre otros, sino en las notas que acompañan a los estados financieros. Esto con frecuencia se ignora y son muchos los que todavía confunden las NIIF con determinados criterios de valoración (valor razonable, coste amortizado), que de ninguna manera suponen una aportación original del IASB, ni tampoco del FASB, a la contabilidad como disciplina financiera. Por el contrario, son las notas lo que da valor a los estados financieros básicos (balance, cuenta de resultados, estados de cambios en patrimonio y de flujos de efectivo) presentados bajo NIIF, a fin de contribuir a que sus usuarios puedan formarse un juicio profesional y tomar

decisiones respecto de la adquisición, venta o mantenimiento de una determinada inversión (acción, bono, etc.). Las notas a los estados financieros incluyen informaciones relativas a las bases de estimación de los activos y pasivos, las políticas contables adoptadas los juicios y supuestos sobre el futuro que se han utilizado para obtener los importes mostrados y para medir la incertidumbre. Las notas son a menudo ignoradas por los lectores menos cautos porque consideran que son solo formalidades o desgloses de lo mostrado en los estados básicos. Nada más lejos de la realidad. Ocurre que la comprensión del impacto de las notas requiere de una elevada formación en finanzas, negocios y en contabilidad, sin los cuales es francamente difícil alcanzar una lectura útil y diligente de la información financiera mostrada y eso supone para algunos una importante barrera.

2. ¿Por qué son importantes las NIIF en el sistema financiero?

La adopción de las NIIF ofrece en general una oportunidad para que las empresas que lo deseen puedan financiarse en los mercados de capitales como complemento al crédito otorgado por bancos y proveedores. Los bancos, aun cuando no se financien en los mercados de capitales, obtienen su financiación básica del ahorro de los ciudadanos, ya sea mediante depósitos de dinero o cualquier otro instrumento

financiero. Los depósitos de dinero no son instrumentos negociables en los mercados de capitales ni los depositantes son acreedores comerciales, pero como acreedores financieros se encuentran alineados con los bonistas, por lo que una información que les fuera útil a estos debería serlo para aquellos. Además, una regulación contable basada en las NIIF podría serle útil al supervisor como base a partir de la cual estimar la solvencia de las entidades financieras y determinar sus requerimientos de capital. Ello es así porque se trata de una normativa que, con ciertos matices, es utilizada en algunos países para la elaboración de los “estados consolidados”, lo cual podría facilitar una cierta comparabilidad cuantitativa.

3. ¿Cómo visualiza el proceso de adopción de las NIIF para el sistema financiero en Guatemala?

El proceso de adopción de cualquier regulación internacional limita la soberanía nacional y suscita riesgos que pueden llegar a ser relevantes desde el punto de vista de la estabilidad financiera de un país. El hecho de que la crisis financiera desatada en 2007 se cebara con bancos y aseguradoras de países desarrollados que aplicaban una regulación financiera internacional supuestamente avanzada tanto en materia contable (NIIF o FASB) como prudencial (Basilea II para los bancos, Solvencia en el caso de las aseguradoras europeas), no parece una prueba edificante de la bondad que se esperaba de esas regulaciones para alcanzar la estabilidad financiera de un país. Al contrario, la crisis puso de manifiesto deficiencias notables tanto en la normativa contable (estimaciones muy deficientes en deterioros crediticios o en la consolidación de determinadas estructuras financieras) como en la prudencial, que terminaron costando dinero a los ciudadanos y en

algunos casos afectando al equilibrio presupuestario de algunos estados. Pero tampoco parece una buena política para alcanzar la estabilidad financiera cerrarse al exterior y no delegar aspecto alguno del diseño normativo contable y prudencial de un país.

Por ello, a mi juicio, si las autoridades desean contener con acierto los riesgos que plantea la integración financiera internacional, es necesario encontrar un equilibrio entre estabilidad financiera y globalización normativa. Los países en desarrollo suelen carecer de un auténtico mercado de capitales y con ello de la experiencia necesaria para adoptar regulaciones contables y prudenciales apropiadas que les defiendan de los efectos perversos de una liberalización normativa de sus sistemas financieros. Es preciso pues actuar con suma prudencia. Para ello, en el caso de la normativa contable destinada al sector financiero, lo ideal es que las autoridades elaboren normas contables propias que, inspirándose en la regulación NIIF, mantengan las mejores prácticas y reglas de la normativa nacional, como pueden ser la estimación de deterioros por riesgo de crédito en los bancos y la consolidación de cualesquiera estructura financiera que pueda terminar afectando al grupo, incluidos el riesgo reputacional, tan duro de ganar como fácil de perder.

4. ¿Qué desventajas considera que tiene el adoptar las NIIF plenas en un sistema financiero?

El IASB, como órgano productor de las normas contables NIIF, está continuamente mejorando y adaptando sus propias normas. Aplicar directamente sus normas sin someterlas a un proceso legal y normativo nacional no resulta muy apropiado, entre otras cosas porque puede dar lugar a una inseguridad jurídica que de ninguna manera es deseable, y aún menos

para el caso de entidades sometidas a supervisión prudencial como son los bancos y aseguradoras. El mecanismo utilizado por el que la Unión Europea adopta y exige las NIIF es el camino a seguir cuando se dispone de un mercado de capitales mínimamente desarrollado y profundo, pero existen otras fórmulas válidas.

Las NIIF fueron diseñadas para ser aplicadas por cualquier tipo de empresa que se financie en los mercados de capitales, pero no se adaptan apropiadamente a las características específicas de entidades o sectores concretos. De manera particular y relevante para los países, ese es el caso para los bancos y entidades de crédito y depósito. Por ejemplo, someter al mismo proceso de evaluación del riesgo de crédito a un préstamo que se encuentre en el balance de una compañía agrícola que al de la cartera crediticia de un banco supone ignorar no solo el muy distinto peso relativo de estos activos en los balances de ambos grupos de compañías, sino además las distintas consecuencias del deterioro crediticio en una y otra entidad dado el elevado nivel de endeudamiento de un banco respecto al de cualquier compañía no financiera. Y todo ello agravado por los efectos provocados sobre la estabilidad financiera de un país por el colapso de un banco, frente al de cualquier otra entidad no financiera. Es preciso pues actuar con exquisita prudencia y sensatez.

5. ¿Por qué considera que debe prevalecer la hipótesis del devengo al estimar el resultado del ejercicio?

La preparación de estados financieros no es un fin en sí misma, sino que su justificación se encuentra en la relevancia de la información facilitada. Esta información está sujeta a limitaciones

e imperfecciones que son fruto de las convenciones en que se basa el registro inicial y la valoración posterior de una determinada transacción económica.

La primera convención es la denominada “empresa en funcionamiento”, que supone asumir que (salvo evidencia en contrario) la entidad continuará operando con normalidad en el futuro previsible y que por ello las normas contables no tienen por objetivo determinar el valor de liquidación de la compañía. Como el resultado definitivo de cualquier negocio solo se puede conocer liquidándolo (como hacían las primeras formas societarias en el Medioevo) y este momento es incierto, los inversores no pueden esperar a ello para conocer el resultado de su inversión, por lo que es necesario establecer un plazo periódico y arbitrario de rendición de cuentas que convencionalmente se ha venido aceptando de un año.

La segunda convención es consecuencia de la primera y es conocida como el criterio de “devengo” o “acumulación”. La necesidad de rendición periódica de cuentas requiere determinar el resultado del período fijado. Como señalaba antes, únicamente con la liquidación de la entidad sería posible conocer con absoluta certidumbre el resultado obtenido, pero lo normal es que la entidad no se liquide sino que continúe funcionando. Ello requiere estimar qué parte del resultado se ha obtenido o, dicho de otra manera, la variación del patrimonio neto entre el inicio y el fin del período no motivadas por aportaciones o retiros de sus propietarios (accionistas, etc.).

La contabilidad esencialmente trata de medir la diferencia entre los costes incurridos (como esfuerzo realizado) y los ingresos obtenidos (como éxito del esfuerzo realizado), es decir la variación del patrimonio neto o diferencia entre

el valor de los activos y el importe de las deudas a lo largo de un período. Los conceptos de cobro, pago, ingreso, gasto, correlación de ingresos y gastos son fundamentales en la preparación de estados financieros, sin que se les otorgue la misma importancia en la teoría económica, razón por la que quizás algunos economistas tienen dificultades para comprender el significado completo del término “devengo” y “acumulado”. Para el poco experto, como regla simple, coste y gasto significan dinero entregado e ingreso y resultado significan dinero recibido. Las ideas de “devengo” y “correlación” o “compensación” son bastante más profundas. La contabilidad no trata de correlacionar el dinero cobrado con el recibido, sino el esfuerzo realizado con el logro obtenido, el servicio entregado con el servicio recibido, el precio pagado con el precio recibido, y ello requiere encontrar bases sólidas de asociación entre el presente y el futuro. Todo esto es lo que comprende los conceptos de “ingreso”, “coste” y “devengo contable”.

El “devengo contable” hace referencia al momento en que los eventos económicos han de ser reconocidos en los estados financieros. Reconocer los eventos en términos de movimientos de efectivo (cobro/pago) no muestra el resultado de un negocio puesto que no relaciona el valor recibido con el esfuerzo realizado. Un devengo inadecuado puede dar lugar, por ejemplo, a un reconocimiento anticipado de ingresos (antes de que haya una certeza razonable en cuanto a que vayan a ser efectivamente



recibidos) o a un diferimiento indebido de gastos o de pérdidas. Ambas posibilidades son muy graves puesto que el resultado de una entidad es la diferencia entre sus ingresos y sus costes (gastos y pérdidas). El devengo contable requiere reconocer un ingreso cuando haya un incremento de expectativas racionales de recibir dinero (u otro activo) relacionado con un incremento de activos o reducción de pasivos, además que su importe pueda ser razonablemente estimado; y, ello con independencia de que se haya recibido o no el dinero u otro activo. Por su parte, debe reconocerse un coste (gasto o pérdida) cuando surgen expectativas de salidas de dinero o se haya producido una reducción de valor de un activo (pérdida por deterioro o menor valoración otorgada por el mercado), y su importe pueda ser medido con fiabilidad, y ello con independencia de que se haya entregado el dinero u otro activo.

Uno de los aspectos críticos de la contabilidad bancaria es el reconocimiento de la incertidumbre respecto de la cobrabilidad de los préstamos otorgados, es decir si se están reconociendo con suficiente puntualidad las pérdidas o si por el contrario se están enmascarando dentro del balance, por ejemplo refinanciando u otorgando alargamientos de pagos a prestatarios en dificultades. Del mismo modo, políticas crediticias laxas o poco rigurosas pueden suponer un mal devengo de las pérdidas crediticias, difiriéndolas hacia ejercicios futuros en lugar de ser incluidas en el año de otorgamiento del préstamo. Buena parte de estas prácticas contables y crediticias fueron abono que contribuyó a la germinación de la crisis financiera desatada en 2007 y que finalmente explotó en septiembre de 2008 con el colapso del banco Lehman Brothers en los EE.UU.



Jorge Pérez Ramírez

³Doctor en Economía con premio extraordinario de doctorado; es el Responsable Técnico del Programa de Asistencia Técnica del Centro de Estudios Monetarios Latinoamericanos (CEMLA) para el fortalecimiento del marco regulatorio contable de los bancos centrales y entidades supervisadas del sistema financiero. Destacado ponente y conferenciante en seminarios, talleres y encuentros tanto universitarios como de capacitación de altos cargos de los bancos centrales y supervisores latinoamericanos. También es autor de trabajos y libros sobre contabilidad, derivados e historia de la banca y de la medición de riesgos como *“Vidas paralelas: la banca y el riesgo a través de la historia”*, *“Banca y Seguros. Capital y Contabilidad”*, *“Del Oráculo de Delfos a la Torre de Basilea”*, entre otros.

La gestión del riesgo de mercado como una herramienta gerencial en la banca

Edgar René Guevara Recinos*



“

La gestión de riesgo de mercado requiere de un análisis integral, dinámico y complementario que permita identificar, medir, gestionar y mitigar las fuentes generadoras de riesgo inherente, lo cual constituye un reto importante para las entidades bancarias.”

La idea de riesgo aparece siempre asociada a la posibilidad de desviación en la consecución de un rendimiento u objetivo

previamente establecido, esto es una variación, una divergencia entre un valor estimado *a priori* y el realmente alcanzado¹. En ese sentido, aplicado a las entidades bancarias, el Comité de Supervisión Bancaria de Basilea, en adelante el Comité, define el riesgo de mercado como “la posibilidad de sufrir pérdidas en posiciones dentro y fuera de balance a raíz de oscilaciones en los precios de mercado”²; cabe comentar

que dichas pérdidas pueden reflejarse en una disminución de ingresos o de patrimonio³.

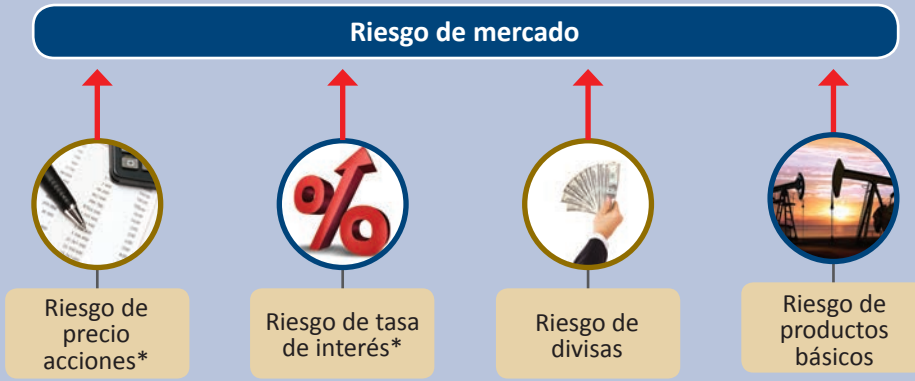
De acuerdo con el Comité, pueden clasificarse como fuentes generadoras de riesgo de mercado las siguientes:

1 Feria Domínguez, José Manuel (2005). *El Riesgo de Mercado su medición y control*. España.

2 Convergencia Internacional de medidas y normas de capital. Marco revisado. Junio 2006

3 Para el caso de Guatemala el Reglamento para la Administración del Riesgo de Mercado, emitido por la Junta Monetaria mediante resolución JM-119-2016, define el riesgo de mercado como “la contingencia de que una institución incurra en pérdidas como consecuencia de movimientos adversos en precios en los mercados financieros. Incluye los riesgos de tasa de interés y cambiario”.

FUENTES GENERADORAS DE RIESGO DE MERCADO



Fuente: Elaboración propia del autor con base a criterios emitidos por el Comité de Supervisión Bancaria de Basilea.

*Títulos valores clasificados en la cartera de negociación.

En cuanto a los riesgos inherentes a los precios de las acciones y a instrumentos relacionados con los tipos de interés ilustrados en el esquema anterior, es importante indicar que no todos los títulos valores que poseen las entidades bancarias están sujetas a riesgo de mercado, únicamente se considera que están afectos a este tipo de riesgo aquellos títulos valores que la entidad tiene predestinados para negociar en el mercado, clasificados dentro de la cartera de negociación (*trading book*); mientras que no se considera que estén afectos a riesgo de mercado aquellos títulos valores que la entidad pretende mantener hasta su vencimiento, clasificados dentro de la cartera bancaria (*banking book*).

Por otra parte, en cuanto al riesgo inherente de divisas y de productos básicos⁴, estos aplican a las posiciones que las entidades mantienen en moneda extranjera y en productos básicos, ya sea en el mercado al contado, a plazo o en derivados.

A continuación se desarrollan las fuentes de riesgo de mercado indicadas anteriormente y se describen algunos

métodos relacionados con la medición de las mismas.

1. Riesgo de precio acciones: este riesgo corresponde a la posibilidad de que una entidad incurra en pérdidas por mantener títulos valores de renta variable, entre ellos, acciones y derivados sobre estas o índices bursátiles, debido a fluctuaciones de los precios de las mismas. Gran parte del riesgo inherente al precio de las acciones está relacionado con instrumentos derivados de acciones, en los cuales los cambios en las cotizaciones de dichos precios están íntimamente relacionados con sus activos subyacentes⁵; por lo tanto, la medición del riesgo de mercado de este tipo de instrumentos se vuelve más compleja para las entidades debido a que no depende únicamente de su riesgo *per se*, sino depende en gran medida del riesgo del activo subyacente.

2. Riesgo de tasas de interés: los riesgos de tasa de interés en la cartera de negociación se relacionan con la posibilidad de incurrir en pérdidas debido a la dificultad de trasladar las

variaciones en las tasas de mercado a las tasas de los productos. Existen varias metodologías para la medición de la exposición al riesgo de tasa de interés, entre las cuales se pueden indicar las siguientes:

- **Método de vencimientos:** es empleado especialmente para medir el impacto de cambios en tasas de interés sobre el margen financiero, entendiéndose como tal al costo de intermediación de las entidades, es decir la diferencia entre lo que los bancos cobran a sus clientes que solicitan recursos y lo que pagan a sus depositantes. Dicho método consiste en distribuir, a partir de datos agregados del balance, los títulos valores por bandas determinadas según las fechas de vencimiento o renovación, utilizando el valor nominal.
- **Método de duración:** calcula el tiempo promedio ponderado de recuperación de cada título valor, a partir de operaciones individuales, utilizando el valor presente de cada instrumento financiero para medir el impacto sobre el valor patrimonial de la entidad.
- **Valor en riesgo (VAR, Value at Risk):** utiliza volatilidades de tasas de interés para medir posibles cambios en el valor de los instrumentos financieros, incorporando correlaciones entre tasas y precios. Se basa en un enfoque de portafolio, sustentado en la diversificación para disminuir el riesgo. La mayoría de estos métodos no necesariamente asumen distribuciones normales, puesto que se basan en modelos *risk metrics*, los cuales se construyen a partir de una gran cantidad de simulaciones que permiten establecer la distribución de probabilidad que mejor se ajusta al comportamiento de los datos y medir los cambios de valor del portafolio con base a estimaciones de pérdida esperada y niveles de confianza.

4 Acorde con el Comité de Supervisión Bancaria de Basilea, un producto básico (o materia prima) es cualquier producto físico negociado o negociable en un mercado secundario, como por ejemplo productos agrícolas, minerales (incluido el petróleo) y metales preciosos, sin incluir el oro.

5 Un activo subyacente es aquel cuyo valor sirve de referencia para establecer el precio de un instrumento financiero derivado, entre ellos, futuros, opciones, *swaps*.

3. Riesgo de divisas: este se asocia directamente con el riesgo cambiario y se define como la posibilidad de que una entidad incurra en pérdidas debido a fluctuaciones del precio de las divisas en los mercados financieros. En ese sentido, para poder estimar el riesgo inherente, es importante cuantificar la exposición que una entidad puede tener frente a una o varias monedas determinando, si en términos netos se trata, de una posición acreedora, es decir posee más activos que pasivos, o bien de una posición deudora, que en este caso significará que tiene más pasivos que activos.

4. Riesgo de productos básicos: este riesgo es intrínseco al riesgo de precios y corresponde a las pérdidas que puede tener una entidad debido a la variación de precios de los productos básicos, suele ser más complejo y volátil que el asociado a las divisas o a los tipos de interés, debido a que los mercados de productos básicos pueden resultar menos líquidos que los de tipos de interés o divisas, por lo que los cambios en la oferta y la demanda pueden tener un efecto más profundo en los precios y en la volatilidad. De manera similar al riesgo de acciones, el riesgo inherente al precio de productos básicos está íntimamente relacionado con instrumentos derivados, por lo que la sensibilidad al riesgo depende también del comportamiento de activo subyacente.

Cabe comentar que, para la medición de las fuentes generadoras de riesgo de mercado indicadas anteriormente, el Comité desarrolla una serie de metodologías que pueden consultarse, principalmente, en los documentos *Convergencia internacional de medidas y normas de capital (2006)* y *Requerimientos mínimos de capital por riesgo de mercado (2016)*.

Como se puede observar, las fuentes generadoras de riesgo de mercado son múltiples y cada una de ellas requiere de un tratamiento distinto, lo cual constituye un reto importante, en cuanto a gestión, para las entidades bancarias. En ese sentido, el Banco Interamericano de Desarrollo y Grupo Santander en el documento *Gestión de Riesgos Financieros, un enfoque práctico para países latinoamericanos (1999)*, propone tres pasos para tener una visión completa del riesgo de mercado.

- 1 Identificación de las fuentes de riesgo:** requerirá un conocimiento profundo de todos los productos en que la entidad está operando y de los nuevos en los que tenga planificado operar.
- 2 Mapa de posiciones:** muestra la sensibilidad del valor de la cartera ante variaciones en el valor de cada una de las fuentes generadoras de riesgo de mercado por separado. Permitiría calcular rápidamente la repercusión sobre la cuenta de resultados de un movimiento en el mercado.
- 3 Mapa de pérdidas y ganancias:** se basa en un análisis integral que parte del mapa de posiciones indicado anteriormente, suponiendo determinados comportamientos

e interrelaciones de las fuentes generadoras de riesgo de mercado con el propósito de estimar el comportamiento total de la cartera. El resultado final es la obtención de un conjunto de escenarios posibles que tendrían asignada una probabilidad de ocurrencia.

De esta cuenta, una vez aplicados los pasos anteriores, es importante que la entidad posea una adecuada estructura administrativa que permita medir, monitorear, controlar, prevenir y mitigar el riesgo adecuadamente, para lo cual es crucial que esta establezca políticas, procedimientos y sistemas, contenidos en un manual de administración de riesgo de mercado, el cual debe ser aprobado y actualizado por el órgano de dirección superior de la entidad. Asimismo, es importante establecer un comité y una unidad de riesgos, que cuenten con funciones y actividades claramente establecidas, dentro de un contexto de un adecuado gobierno corporativo.

Finalmente, se puede concluir que: a) la gestión de riesgo de mercado requiere de un análisis integral, dinámico y complementario que permita identificar y medir las fuentes generadoras de riesgo inherente; b) la entidad bancaria debe contar con una adecuada estructura administrativa que permita gestionar y mitigar el riesgo de mercado; y, c) es recomendable que al momento de diseñar metodologías para medir y gestionar el riesgo de mercado se considere la interrelación que puede tener con otros tipos de riesgos, principalmente, de liquidez, de crédito y operacional.



Edgar René Guevara Recinos

*Ingeniero Industrial por la Universidad de San Carlos de Guatemala y Master en Finanzas por la Universidad Rafael Landívar. Egresado del Programa de Estudios Superiores Mención en Economía y Finanzas del Banco de Guatemala, el Centro de Estudios Monetarios Latinoamericano (CEMLA) y la Universidad Rafael Landívar. Posee experiencia en regulación de mercados financieros y análisis de esquemas y marcos legales de protección al usuario de servicios financieros. Es Profesional del Departamento de Normativa de la Superintendencia de Bancos.

Aspectos fundamentales de la gestión del riesgo de liquidez en las entidades bancarias

Luis Francisco Vallejo García*



Definiciones

Liquidez

Es la capacidad de una institución bancaria para cumplir sus compromisos y obligaciones a un costo razonable.

Mantener a un nivel adecuado la liquidez depende de la capacidad de los bancos para atender los flujos de efectivo, esperados e inesperados, sin afectar de manera adversa las operaciones ordinarias ni su situación financiera.

La liquidez de un banco proviene de diversas fuentes activas y pasivas, tales como activos fácilmente convertibles en efectivo, flujos de operación netos, así como de captación de fondos a través de depósitos y préstamos, entre otros.

Riesgo de liquidez

De conformidad con el Comité de Supervisión Bancaria de Basilea, existen dos tipos de riesgo de liquidez, de fondos y de mercado.

Riesgo de liquidez de fondos: es el riesgo de que una entidad no sea capaz de hacer frente eficientemente a flujos de caja previstos e imprevistos, presentes y futuros, sin que se vea afectada su operativa diaria o su situación financiera.

Riesgo de liquidez de mercado: es el riesgo de que una entidad no pueda liquidar fácilmente una posición a precios de mercado a causa de la ausencia de mercados especializados

o de distorsiones en el mercado existente.

Por su parte, la Oficina del Contralor de la Moneda de los Estados Unidos de América (OCC, por sus siglas en inglés) lo define como el riesgo de que la situación financiera o la solvencia de una institución sean afectadas en forma adversa, derivado de una incapacidad, real o percibida, para cumplir con sus obligaciones.

Gestión del riesgo de liquidez

Las repercusiones inmediatas y graves de la liquidez insuficiente hacen que el riesgo de liquidez y su gestión sean elementos clave en la estructura general de una entidad bancaria, más aún si se tiene en cuenta que, según lo establecido en el artículo 75 de la Ley de Bancos y Grupos Financieros, la cesación del pago de las obligaciones

por parte de un banco o una sociedad financiera constituye causal para que la Junta Monetaria suspenda de inmediato sus operaciones.

En ese sentido, una adecuada gestión del riesgo de liquidez debe considerar, entre otros aspectos, lo descrito a continuación.

- Gobierno corporativo adecuado y participación de la gerencia.
- Estrategias, políticas, procedimientos y límites apropiados para administrar y controlar el riesgo de liquidez, en situaciones normales y en condiciones de estrés.
- Sistemas apropiados de medición y monitoreo del riesgo de liquidez.
- Gestión activa de la liquidez intradía.
- Mantener una mezcla razonablemente diversa de fuentes de financiamiento.
- Niveles adecuados de valores altamente líquidos, sin restricciones, que pueden ser utilizados para cumplir necesidades de liquidez en situaciones de estrés.
- Planes de contingencia para afrontar eventos adversos de liquidez.



Fundamentos para la gestión del riesgo de liquidez

La administración de la liquidez implica estimar las necesidades de efectivo, presentes y futuras, a costos razonables; por lo que al establecer e implementar sus planes, los gestores bancarios deben considerar la variedad de fuentes disponibles.

Adicionalmente, los gestores deben evaluar otros factores como la sensibilidad de sus proveedores de fondos, los instrumentos de financiamiento que utilizan, la relación de los costos de financiamiento con el rendimiento de sus activos y cualquier restricción regulatoria o de mercado sobre el financiamiento; asimismo, deben estar alertas a los riesgos que surgen de las concentraciones en fuentes de financiamiento.

Al respecto, el autor Leonard M. Matz, en su obra *“Liquidity Risk Management”*, señala que el riesgo de liquidez posee determinadas características fundamentales que deben considerarse para su adecuada gestión, entre las que destacan las siguientes:

1. La gestión del riesgo de liquidez, como en todos los riesgos, debe ser prospectiva

Las metodologías de medición del riesgo de liquidez basadas únicamente en información del pasado, tal como indicadores históricos, tienden a ser limitadas.

Los indicadores históricos proveen información útil para fines de comparación con otras entidades, o bien, pueden funcionar como una herramienta de análisis de tendencias; sin embargo, los análisis basados en proyecciones constituyen una mejor

herramienta para la medición del riesgo de liquidez.

En consecuencia, un proceso adecuado de medición del riesgo de liquidez debe incluir, entre otros aspectos, métodos robustos para proyectar flujos de efectivo generados por los activos, pasivos y operaciones fuera de balance, en diferentes horizontes de tiempo.

El análisis de proyecciones de flujos de efectivo, consiste básicamente en comparar la cantidad de efectivo que podría estar disponible dentro de un horizonte de tiempo determinado, con la cantidad de efectivo requerida dentro del mismo período. La diferencia entre esas dos cantidades constituye la brecha de liquidez que debe gestionarse.

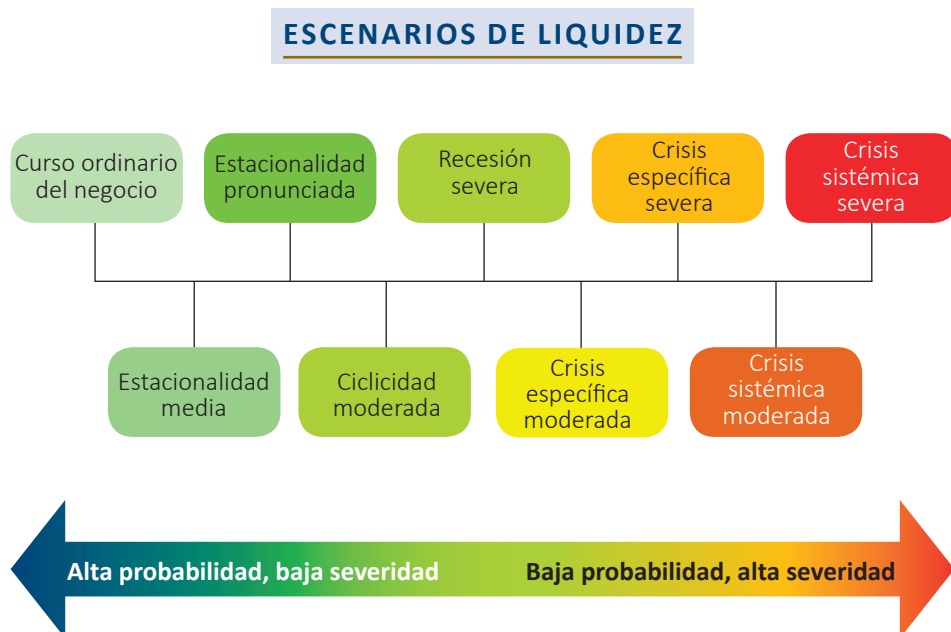
En cuanto a los horizontes de tiempo, Leonard M. Matz, sugiere que los bancos que se financian, principalmente, con depósitos minoristas y de pequeñas empresas,

deberían utilizar como mínimo horizontes mensuales; en tanto que los bancos que se financian con depósitos mayoristas o institucionales deberían utilizar una combinación de horizontes diarios, semanales, mensuales y trimestrales.

2. El riesgo de liquidez debe evaluarse en un contexto de escenarios

El riesgo de liquidez no puede medirse o gestionarse adecuadamente fuera de un contexto de escenarios. La adopción de metodologías robustas para el análisis de escenarios, bajo diferentes contextos, constituye un aspecto fundamental para una adecuada gestión del riesgo de liquidez de una entidad bancaria.

Al respecto, el autor antes citado recomienda que para la medición y gestión del riesgo de liquidez se desarrollen escenarios basados en distintas necesidades de liquidez, los cuales se presentan en el diagrama siguiente.



Fuente: Matz, Leonard M. *Liquidity Risk Management*, 2011.



Escenarios para necesidades normales y estacionales

En este tipo de escenarios se consideran los flujos de efectivo que se generan en el desarrollo ordinario de las operaciones de la entidad, así como los retiros de depósitos, desembolsos de créditos y otros flujos que presentan un comportamiento estacional.

Escenarios para necesidades cíclicas y en situaciones de crisis

En el caso de las necesidades cíclicas, las entidades deben considerar comportamientos que se producen

en el largo plazo y que generan necesidades de liquidez.

En cuanto a los escenarios en situaciones de crisis específicas, también conocidas como “crisis idiosincráticas”, se refieren a aquellas que derivan de la pérdida de confianza en una institución por parte de sus depositantes, lo que generalmente se traduce en importantes retiros de depósitos, también conocidos como “corridas”.

Finalmente, las necesidades de liquidez en situaciones de crisis sistémica derivan de alteraciones importantes

en la situación macroeconómica, los mercados o en los sistemas de pagos.

3. La confianza es un requisito crítico

Los gestores de las instituciones financieras deben comprender que el riesgo de liquidez se trata tanto de confianza como de efectivo. La confianza es un requisito crítico, ya que una falta de liquidez percibida, independientemente de si la percepción es precisa, puede convertirse en un gran problema; por el contrario, una abundancia percibida de liquidez es un requisito fundamental de gestión del riesgo de liquidez.

Referencia: *Balance Sheet Management/Liquidity Risk Management School*, organizado por la entidad *Office of The Comptroller of the Currency (OCC)*, Washington, D. C., Estados Unidos de América, julio de 2018.



Luis Francisco Vallejo García

*Contador Público y Auditor por la Universidad de San Carlos de Guatemala y Master en Contaduría Pública y Auditoría por la Universidad Galileo. Posee experiencia en supervisión de riesgos bancarios y de almacenes generales de depósito, así como en el desarrollo de herramientas de supervisión. Es Inspector del Departamento de Supervisión de Riesgos Específicos de la Superintendencia de Bancos.

Supervisión consolidada de grupos financieros y riesgos asociados

Ana Luisa Sical Guerra de Fernández*
Julio Antonio Cantoral López**



Las estructuras funcionales de los grupos financieros les permiten operar bajo un esquema de economías de escala, maximizando las utilidades a través de la prestación de servicios financieros. También generan riesgos que pueden ser propios de la actividad financiera, como los provocados por la gestión de la administración, que se pueden transmitir de una entidad miembro a otra hasta llegar a afectar la liquidez, solvencia y rentabilidad del grupo en su conjunto.

Grupos financieros y riesgos asociados

Un grupo financiero es aquel que integra compañías (nacionales o extranjeras) que operan bajo control común de una controladora o empresa responsable y

cuya actividad exclusiva y predominante consiste en proporcionar principalmente servicios financieros. Estos grupos surgen como una estrategia empresarial para reducir costos y maximizar ganancias a través del uso en

común de marca corporativa, tecnología, infraestructura, directores ejecutivos, así como por la ventaja en aspectos relacionados con procesos avanzados en la administración del riesgo empresarial, competencia e innovación financiera, beneficios fiscales, consolidación de una industria en particular, entre otros.

La conformación y operación de grupos financieros trae implícito la asunción de riesgos, los cuales pueden afectar al grupo en su conjunto o a una entidad en

específico como resultado del contagio a través de operaciones intragrupo, razón por la cual estos riesgos deben ser identificados, medidos y gestionados, tanto a nivel individual como de forma consolidada. Entre los principales riesgos a los que están expuestos los grupos financieros están: de contagio, de reputación, de regulatorio, de autonomía, de país, de transferencia y de concentración, siendo el banco o bancos que forman parte del grupo financiero las entidades que, por operaciones normales de la actividad de intermediación u operaciones direccionadas por la alta administración, con el propósito de apoyar a otra empresa del grupo financiero, podrían ver afectada su liquidez, solvencia o rentabilidad, correspondiéndole al supervisor bancario verificar que, tanto la empresa controladora o responsable como las integrantes del grupo, cuenten con adecuados mitigadores de riesgo.

En ese sentido, la consolidación financiera de las entidades que conforman el grupo financiero es esencial para que los supervisores bancarios conozcan la situación financiera del grupo en su conjunto, lo que permite determinar el riesgo en forma efectiva, debido a que las cuentas contables de cada unidad por separado no dan una imagen completa de las actividades de la misma y omiten informaciones relevantes como créditos y débitos recíprocos, pudiendo existir operaciones que en conjunto son compensadas al consolidarse la información, por lo tanto, la información consolidada del grupo (balance general, estado de pérdidas y ganancias y estado de



flujos de efectivo) refleja de mejor manera su información financiera.

Principales retos para el supervisor bancario

Para una supervisión eficaz de grupos financieros, los supervisores bancarios deben contar con herramientas que les permitan evaluar la idoneidad de los administradores, directores y accionistas mayoritarios del grupo financiero, así como la gestión prudente y control de concentraciones de riesgo y transacciones y exposiciones intragrupo, su adecuación de capital incluyendo la detección de usos múltiples de capital (doble o múltiple apalancamiento y apalancamiento excesivo), para lo cual es necesario facilitar el intercambio de información y la coordinación entre los supervisores tanto locales como extranjeros. En ese orden de ideas, la supervisión de grupos financieros constituye un reto para los supervisores bancarios al considerar que sus integrantes operan bajo un control común y en jurisdicciones diferentes, lo que en alguna medida podría limitar el alcance de la acción supervisora, existiendo la contingencia de no identificar

operaciones de alto riesgo, o bien, no contar con la potestad legal para acceder a la información de ciertas entidades dependientes, para evaluar la adecuación de capital, concentraciones de riesgo y exposiciones entre empresas de un mismo grupo.

Usos múltiples de capital en grupos financieros

La emisión de doble o múltiple apalancamiento de capital resulta por la utilización simultánea del mismo capital como un colchón para el riesgo en dos o más entidades legales, incluyendo situaciones en las cuales se realiza a través de compañías *holding*, intermediarias no reguladas que tienen participaciones en dependientes o afiliadas comprometidas en actividades financieras.

El doble o múltiple apalancamiento ocurre dentro de los grupos financieros que no están totalmente consolidados y cuando una entidad mantiene capital regulatorio emitido por otra dentro del mismo grupo y al emisor se le permite que incluya el capital en su propia hoja de balance. Esta situación se mitiga cuando el grupo financiero es sujeto a requerimientos de capital en una base totalmente consolidada

y las subsidiarias también están sujetas a requerimientos de capital consolidados, por lo que el grupo deduce los beneficios de capital no regulatorio del doble apalancamiento.

Supervisión consolidada en Guatemala

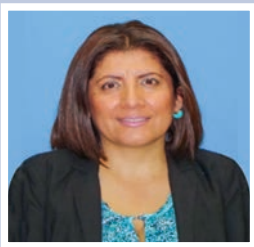
La Ley de Bancos y Grupos Financieros, Decreto Número 19-2002 del Congreso de la República, en su artículo 28 define la supervisión consolidada como: *la vigilancia e inspección que realiza la Superintendencia de Bancos sobre un grupo financiero, con el objeto de que las entidades que conformen el mismo, adecúen sus actividades y funcionamiento a las normas legales, reglamentarias y otras disposiciones que le sean aplicables, y los riesgos que asumen las empresas de dicho grupo, que puedan afectar al banco, sean evaluados y controlados sobre una base por empresa y global. Para estos efectos, la Superintendencia de Bancos tendrá acceso a la información de operaciones y*

actividades del grupo financiero, sobre una base por empresa y consolidada, resguardando la identidad de los depositantes e inversionistas conforme a lo establecido en la citada Ley.

En concordancia con lo anterior, la referida ley, en su artículo 27, define grupo financiero como *la agrupación de dos o más personas jurídicas que realizan actividades de naturaleza financiera, de las cuales una de ellas deberá ser banco, entre las cuales existe control común por relaciones de propiedad, administración o uso de imagen corporativa, o bien sin existir estas relaciones, según acuerdo, deciden el control común.*

En conclusión, las estructuras funcionales de los grupos financieros les permiten operar bajo un esquema de economías de escala, maximizando las utilidades a través de la prestación de servicios financieros a los usuarios; sin embargo, también generan riesgos que pueden ser propios de la actividad financiera, como

los provocados por la gestión de la administración, los cuales se pueden transmitir de una entidad miembro a otra hasta llegar a afectar la liquidez, solvencia y rentabilidad de las entidades bancarias miembros de los grupos financieros, razón por la cual, la SIB juega un papel preponderante en la supervisión de grupos financieros, debiendo contar con herramientas técnicas y legales, que le permitan evaluar la adecuación de capital consolidada, detectar usos múltiples de capital, facilitar el intercambio de información entre supervisores, evaluar la idoneidad de los administradores, directores y accionistas mayoritarios del grupo financiero (empresa *holding*), así como evaluar la gestión prudente y control de concentraciones de riesgo, transacciones y exposiciones intragrupo, todo esto en cumplimiento de la misión institucional de la SIB la cual es “promover la estabilidad y confianza en el sistema financiero supervisado”.



Ana Luisa Sical Guerra de Fernández

*Licenciada en Contaduría Pública y Auditoría por la Universidad de San Carlos de Guatemala. Maestría en Administración de Empresas (MBA) por la Universidad Francisco Marroquín. Se ha desempeñado por más de 18 años en la supervisión de entidades bancarias. Es Inspectora en el Departamento A de Supervisión de Riesgos Bancarios de la Superintendencia de Bancos.



Julio Antonio Cantoral López

**Contador Público y Auditor egresado de la Universidad Francisco Marroquín. Maestría en Administración de Negocios con especialización en Dirección Estratégica otorgada por la Universidad Mesoamericana. Posee experiencia en la supervisión de instituciones financieras. Es Inspector en el Departamento de Normativa de la Superintendencia de Bancos.

La actividad fiduciaria y los principales riesgos asociados

Ana Luisa De León Enríquez*



“

La supervisión basada en riesgos, en la medida que parte del conocimiento de los riesgos del negocio, permite una supervisión que beneficia a las partes. Ratifica la confianza, base del contrato fiduciario.

Gerardo Hernández Correa
Ex-Superintendente Financiero de Colombia

”

“

El riesgo fiduciario está centrado en que el fiduciario no cumpla sus deberes, por ejemplo, no realizar los análisis precedentes, lo que puede conducir a materializar el riesgo operacional, el más grande para el negocio fiduciario.

Jorge Eduardo Peña
Profesor Programa de Formación Fiduciaria Internacional, Colombia
Ex-Superintendente Financiero de Colombia

”

La actividad fiduciaria

El negocio fiduciario constituye una herramienta versátil, que permite la conducción de un sinnúmero de propósitos no limitados al aseguramiento de bienes para cubrir obligaciones o a la planeación patrimonial; significa hoy en día una nueva forma de llevar a cabo obras públicas o privadas, administración de bienes y de capitales; y, de la personalización de

toda una estructura que funciona para fines muy distintos a los que el fiduciario usualmente conoce como parte de su negocio. Todo esto pone en jaque al supervisor financiero y, de esa cuenta, ha surgido en la mayoría de países latinoamericanos, la necesidad de buscar una mejor regulación, que permita ir más allá de las normas tradicionales que describen al fideicomiso en los códigos civiles o de comercio, en la búsqueda de una mejor comprensión y administración del llamado riesgo fiduciario.

Hay varios desafíos en el tema de actualización regulatoria de la actividad fiduciaria, los principales son: que no sea limitativa al desarrollo del negocio como tal, que permita que este se expanda en un ambiente controlado y, que de ninguna manera se aborde de forma casuística, ya que siendo el contrato de fideicomiso tan flexible, es posible que se dificulte la homogeneización de aspectos comunes entre cada tipo de fideicomiso. Los fideicomisos pueden ser tan variados que es posible notar, sin mayor dificultad, una gran diferencia entre el que genéricamente se trate de inversión y de administración, por ejemplo, en donde los riesgos en cada uno son muy distintos; sin embargo, es posible identificar procesos similares que comprenden la estructuración, gestión y liquidación del mismo, que representa el ciclo de vida de cualquier negocio fiduciario, siendo posible a través de este evaluar las herramientas de su ejecución.

El negocio fiduciario puede ser utilizado para diferentes propósitos, algunos de tal envergadura



que suponen la financiación de proyectos del sector público para cubrir necesidades primordiales. La experiencia en algunos países de Latinoamérica ha sido exitosa al poder concluir proyectos importantes de infraestructura.

Todo lo anterior lleva implícito un elemento por parte de los fiduciarios: **la profesionalidad** en el **régimen de responsabilidad** que le fuera conferido. Esta responsabilidad se

fija como un objetivo regulatorio para mantener a los fiduciarios no únicamente en el interés de negocio, priorizando las ganancias sobre los posibles riesgos asumidos, sino con la suficiente claridad de que el establecimiento de un régimen de identificación, evaluación y control de los riesgos, facilitan el cumplimiento de esta obligación profesional asumida y, sin duda, confieren al sector, al mercado y a los clientes la confianza necesaria.

¿Cómo mitigar los riesgos asociados al negocio fiduciario?



Los negocios desarrollados a través del fideicomiso presentan desafíos importantes para la mitigación de diversos tipos de riesgo; a pesar de esto, algunas acciones importantes pueden ser las siguientes:

- Conocer a la persona natural detrás del negocio, incluso cascada arriba, esto es entender el negocio del cliente comparado

con pares, no únicamente a través de estados financieros. Clasificar el perfil del cliente en alto, medio y bajo, por ejemplo, para optimizar los recursos y ser asertivo en las visitas a realizar antilavado de dinero y antifinanciamiento del terrorismo.

- Conservar registros que permitan conocer y establecer la trazabilidad de operaciones antilavado de dinero y antifinanciamiento del terrorismo.
- Análisis previo de garantías.

Todas las acciones que las instituciones emprendan deben establecerse en un marco efectivo para la administración de riesgos, previa ponderación del riesgo inherente a la actividad fiduciaria.



Respecto a los riesgos asociados

El Comité de Supervisión Bancaria de Basilea define el riesgo operacional a través de macroeventos que pueden resultar en pérdidas para las entidades, uno de estos son las fallas en los procesos. Como fue ya mencionado, existen procesos similares en la actividad fiduciaria que permiten la administración de los riesgos asumidos, por ejemplo:

- En el proceso de estructuración es importante la identificación de los riesgos del negocio. En Colombia, se emite una lista de riesgos por tipo de fiducia (administración, inversión, garantía, etcétera), esto permite conocer la manera de mitigar los distintos factores que pueden concurrir en cada tipo y las obligaciones que generan para el fiduciario, ya que ambas pueden ser muy diferentes según el negocio subyacente.

- En el proceso de ejecución es importante conocer el riesgo de cumplimiento, esto derivado de las obligaciones que ya se conocen del proceso de estructuración.
- En el proceso de liquidación es importante conocer los procedimientos que deberá seguir el fiduciario para la rendición de cuentas, para lo cual es relevante haber establecido una adecuada administración de la información, reportes, trazabilidad de las operaciones y, en general, las acciones que garanticen que el fiduciario extinga su responsabilidad sin generar contingencias.

Sabemos que el resultado de cualquier falla en estos procesos comunes al fideicomiso da como consecuencia la exposición a pérdidas, lo que significaría un evento de riesgo operacional. El riesgo legal surge entonces, cuando la falla en el proceso pueda afectar a alguna de las partes interesadas, que pueda provocar desacuerdo entre las partes y, por lo tanto, que motive al litigio. Si bien es cierto que dentro del patrimonio autónomo pueden preverse los recursos necesarios para su defensa, también es cierto que estos recursos no están disponibles cuando se trata del incumplimiento de obligaciones asumidas y de la responsabilidad objetiva del fiduciario o negligencia en el desempeño de estas.

Referencia: XXVI Congreso Latinoamericano de Fideicomiso (COLAFI)



Ana Luisa De León Enríquez

*Licenciada en Ciencias Jurídicas, Abogada y Notaria por la Universidad de San Carlos de Guatemala; LLM en Derecho de Empresas por la Pontificia Universidad Católica de Chile. Docente del Centro de Estudios y Desarrollo Especializado (CEDE) de la Superintendencia de Bancos. Especialista en evaluación de derivados y estructuras de emisión de deuda bursátil y extrabursátil. Es Inspectora de Riesgo Legal adscrita al Departamento de Supervisión de Riesgos Específicos de la Superintendencia de Bancos.

Ciberseguridad en el sector financiero

Daniel Augusto Monzón Pérez*



La Unión Internacional de Telecomunicaciones (UIT) en su recomendación X.1205 (04/08), define la ciberseguridad como: “el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno¹. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones,

los sistemas de comunicaciones, las comunicaciones multimedia y la totalidad de la información transmitida o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades

de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio²; y, la confidencialidad”.

La ciberseguridad es hoy en día, uno de los retos más importantes a los que se enfrentan los sectores de un país (gobiernos, entidades financieras,

1 Ciber-entorno: incluye a usuarios, redes, dispositivos, software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes. Fuente: Recomendación UIT-T X.1205. Recuperado de: <https://www.itu.int/rec/T-REC-X.1205-200804-I/es>

2 No repudio: se refiere a conocer exactamente quienes son los actores que participan en una transacción o una comunicación y no puedan negarlo en ningún momento. Fuente: Comisión Interamericana de Telecomunicaciones. (2005). “Boletín electrónico/ Número 15). Recuperado de: http://www.oas.org/en/citel/infocitel/2005/septiembre/seguridad_e.asp



infraestructuras críticas, sector privado y ciudadanos), ya que se trata de un aspecto de crucial importancia en un entorno interconectado y dependiente de la tecnología.

Las tecnologías de información se han vuelto indispensables en las entidades financieras, grandes y pequeñas, para asegurar el desarrollo, optimización y efectividad de los procesos del negocio. Por ello, es importante considerar los riesgos derivados del uso de las nuevas tecnologías, los cuales pueden ser provocados por descuidos o errores, irregularidades, falta de concientización de la importancia de la ciberseguridad y ataques malintencionados, tanto internos como externos. Todos los anteriores podrían causar daños económicos y comprometer la integridad, disponibilidad y confiabilidad de la

información, así como también la reputación y continuidad del negocio.

Actualmente, los ataques son cada vez más complejos y sofisticados, toda vez que el cibercrimen³ utiliza todo tipo de medios a su alcance, se aprovecha de las debilidades tecnológicas y no tecnológicas; y, es más difícil de detectar.

De acuerdo con el Informe Global de Riesgos 2018⁴, publicado por el Foro Económico Mundial, los riesgos en cuanto a ciberseguridad están creciendo, tanto en términos de su prevalencia como de su potencial disruptivo, por lo cual los ataques en

contra de entidades financieras casi se han duplicado en cinco años y, los incidentes que antes se consideraban algo fuera de lo común, se están volviendo cada vez más comunes.

El impacto financiero de toda violación contra la ciberseguridad va en aumento; uno de los costos más elevados en 2017 se relaciona a ataques con *ransomware*⁵, que representaron el 64% de todos los *e-mails* maliciosos. Entre los ejemplos más notables de ataques cibernéticos, se incluye el denominado *WannaCry*⁶ que afectó a 300,000 computadoras

3 Cibercrimen: es toda aquella actividad que involucra el uso de tecnologías de información y comunicaciones, con la finalidad de cometer actos ilegales en contra de personas, instituciones o Estados. Fuente: OF 000600 CB/2520 |60|6355 Ministerio de la Defensa.

4 *World Economic Forum*. (2018). Informe Global de Riesgos 2018.

5 *Ransomware*: es una clase de *software* malicioso (*malware*) que se propaga utilizando diferentes técnicas para instalarse en los ordenadores de las víctimas, sin su conocimiento ni autorización; y, por bloquear el acceso a los sistemas infectados o a la información almacenada en ellos, siendo necesario el pago de un rescate para recuperar el acceso normal. Fuente: Glosario de términos de Ciberseguridad INCIBE.

en 150 países; y, el *NotPetya*⁷, que causó pérdidas trimestrales de USD 300 millones a varias empresas afectadas. Tal es el grado de impacto de los riesgos cibernéticos, que el mencionado informe clasifica a los ataques cibernéticos y al fraude o robo de datos en la tercera y cuarta posición, respectivamente; en cuanto a los cinco riesgos globales en términos de probabilidad, únicamente por debajo de los eventos meteorológicos extremos y los desastres naturales.

El riesgo cibernético se ha convertido en una amenaza para la estabilidad financiera global. Según el Fondo Monetario Internacional, las potenciales pérdidas anuales se estiman en 9% de los ingresos netos de los bancos a nivel mundial (USD 100 millones); y, en un escenario severo, la frecuencia de los ciberataques sería de 2.5 a 3.5 (USD 250-350 mil millones) y con mayor contagio, equivalentes a la mitad de los ingresos netos de los bancos, poniendo en riesgo al sector financiero⁸.



¿Cómo gestionar la ciberseguridad?

Hoy en día existen distintas normas internacionales en materia de ciberseguridad, dentro de las cuales se encuentran las siguientes: Tecnologías de la información – Técnicas de seguridad – Directrices para la ciberseguridad (ISO/IEC 27032:2012); Guía de ciber resiliencia⁹ para infraestructuras del sector financiero (CPMI-IOSCO¹⁰); Elementos fundamentales de ciberseguridad para el sector financiero (G7); Marco para mejorar la infraestructura crítica de ciberseguridad (NIST¹¹); y Normas de seguridad cibernética y

prácticas de supervisión (FSB¹²); entre otras. Dichas normas se enfocan en identificar, proteger, detectar, responder y recuperarse ante los riesgos cibernéticos.

En junio de 2018, Guatemala presentó la Estrategia Nacional de Seguridad Cibernética, que contiene los objetivos y acciones que se implementarán en el marco de los mecanismos de colaboración, cooperación y coordinación del Sistema Nacional de Seguridad; y, que permitirá dar cumplimiento a la Resolución de la Organización de Estados Americanos AG/RES. 2006 (XXXIV-0/04), en la cual se insta a los Estados a fortalecer una red regional de cooperación, coordinación y comunicación, a través de la implementación de un

6 *WannaCry*: los ataques *ransomware* de la variedad *WannaCry* (en inglés *WannaCry ransomware attack* o *Wanna Cry Doble Pulsar Attack*), son ataques informáticos que usan el criptogusano conocido como *WannaCry* (también denominado *WannaCrypt*, *WanaCrypt0r 2.0*, *Wanna Decryptor*), dirigidos al sistema operativo *Windows* de *Microsoft*. Fuente: *Ransomware*. Recuperado de: <https://es.unionpedia.org/i/Ransomware>.

7 *NotPetya*: es una variante del virus *Petya*, el cual es un *malware* de tipo *ransomware* reportado por la empresa *Heise Security*. Fuente: Recuperado de: [https://es.wikipedia.org/wiki/Petya_\(malware\)](https://es.wikipedia.org/wiki/Petya_(malware)).

8 Fuente: problemas de ciberseguridad ponen en riesgo 100 mil millones de dólares advierte el FMI. Recuperado de: <https://www.merca20.com/problemas-de-ciberseguridad-ponen-en-riesgo-100-mil-millones-de-dolares-advierte-el-fmi/>

9 Resiliencia: Capacidad de un material, mecanismo o sistema para recuperar su estado inicial, cuando ha cesado la perturbación a la que había estado sometido. Fuente: Real Academia Española.

10 CPMI-IOSCO: *The Committee on Payments and Market Infrastructures and The Board of The International Organization of Securities Commissions*.

11 NIST: *National Institute of Standard and Technology*.

12 FSB: *Financial Stability Board*.

CSIRT¹³ Nacional, el cual, en conjunto con el Comité Nacional de Seguridad Cibernética, permitirá cuando sea necesario, la creación del subcomité de Bancos, Aseguradoras, Financieras, etc., quien coordinará que sus actuaciones sean abordadas de forma conjunta, con el fin de elevar los niveles de seguridad cibernética en todo el país.

Para que la ciberseguridad aborde de manera efectiva los constantes desafíos de brindar una protección adecuada para los activos de la información, es fundamental contar con una estrategia de ciberseguridad. Esta estrategia debe documentar la dirección y metas para el programa de ciberseguridad, según lo determine la alta dirección. Posteriormente, debe establecerse la base para implementar un gobierno efectivo de ciberseguridad, siendo el primer paso que la alta dirección determine los resultados que desea del programa de ciberseguridad. A menudo, esos resultados se establecen en términos de gestión de riesgo y los niveles de riesgo aceptables. Esto se puede lograr mediante una serie de reuniones facilitadas con la alta dirección y los líderes de la unidad de negocios.

13 Equipo de respuesta a incidentes de seguridad informática, por sus siglas en inglés (CSIRT): Es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular. Fuente: Organización de los Estados Americanos. (2016). "Buenas prácticas para establecer un CSIRT nacional".

Para alcanzar los objetivos de la estrategia, es necesario identificar controles, estándares y procesos existentes, relacionados a la ciberseguridad, así como los activos críticos que se desean proteger. Adicionalmente, se considera necesario llevar a cabo las actividades siguientes:

- ✓ Contratación de ciberseguros.
- ✓ Evaluación de vulnerabilidades.
- ✓ Descubrimiento electrónico (*E-Discovery*).
- ✓ Auditorías de ciberseguridad.
- ✓ Ciberejercicios y entrenamiento.

Un ataque bien planificado puede bastar para devastar a cualquier organización. Por eso, en ciberseguridad es crucial mantener activas técnicas, procedimientos y políticas con visión de futuro, así como avanzar en ellas. En la era digital nada es estático y mucho menos puede serlo la defensa de una compañía frente a los potenciales ciberataques. El atacante siempre juega con ventaja, así que es necesario estar lo mejor preparados posibles, y la mejor forma es practicar. Como explica *Malcolm*

Gladwell en su libro titulado *Fuera de Serie: "la práctica no es lo que uno hace cuando es bueno. Es lo que uno hace para volverse bueno"*¹⁴.

14 Rubén García Ramiro. (2018). Ciberejercicios y entrenamiento: la importancia de "practicar" la seguridad. Recuperado de: <https://aunclidelastic.blogthinkbig.com/ciberejercicios-de-seguridad-clave-para-adelantarse-a-las-crisis/>



Daniel Augusto Monzón Pérez

*Ingeniero en Sistemas de Información y Ciencias de la Computación; Magister Artium en Informática con énfasis en Banca Electrónica y Comunicaciones, ambos títulos otorgados por la Universidad Mariano Gálvez de Guatemala; con postgrado en Auditoría de Sistemas por la Universidad Virtual de Bolivia. Posee certificaciones CISA, CSXF, CRTX, Perito Forense Digital, *Ethical Hacker*, *Cobit 5 Foundation*, *SCRUM Master*, *SCRUM Fundamentals*, *ITIL Practitioner*, *Quality Management*, *Project Management*, *Software Project Management* e *Investigative Financial Forensic Auditing*. Es Inspector del Departamento de Supervisión de Riesgos Específicos de la Superintendencia de Bancos.

La incidencia de la nube en los planes de continuidad de tecnología

Luis César Vielman Monroy*



En Resolución JM-102-2011 de la Junta Monetaria, del 17 de agosto de 2011, se establece el Reglamento para la Administración del Riesgo Tecnológico, en donde se estipula que las entidades del sistema financiero supervisado deberán contar con un plan de continuidad de operaciones de Tecnología de la Información (TI) o Plan de Recuperación ante Desastres (DRP, por

sus siglas en inglés), para recuperar los procesos críticos de las principales líneas de negocio soportados por TI, así como la información asociada en caso de una interrupción. Asimismo, deberán contar con un Centro de Cómputo Alterno (CCA), con las características físicas y lógicas necesarias para dar continuidad a las operaciones y procesos críticos de negocios, el cual debe estar ubicado lo

suficientemente alejado del Centro de Cómputo Principal (CCP), para evitar que ambos estén expuestos al mismo nivel de riesgo ante la ocurrencia de un mismo desastre, por ejemplo, falla de la energía eléctrica, corte en las comunicaciones, terremoto y todo evento que interrumpa las operaciones principales de dichas entidades.



Fuente: propia del autor, con información <https://www.valoradata.com/blog/importancia-de-la-contingencia-bcp-y-drp/>

Actualmente, varias entidades del sistema financiero supervisado, están evaluando implementar o ya tienen implementados servicios en la nube, que no es más que un conjunto de tecnologías que permiten disponer de servicios de computación, por ejemplo: procesador, memoria, disco duro, entre otros, a través de una red, que usualmente es Internet; debido a las ventajas y beneficios que ofrece, dentro de los cuales se podrían mencionar la flexibilidad para aumentar o disminuir la demanda de los recursos de cómputo, adaptándose a los requerimientos de cada organización en el momento necesario;

agilidad en la implementación de servicios tecnológicos; reducción de actividades de mantenimiento del *hardware* y sus costos asociados.

Los tipos de implementación de servicios en la nube pueden ser: **nube privada**, que consiste en que los servicios tecnológicos son colocados en centros de cómputo propiedad de la misma organización; **nube pública**, cuando los servicios son utilizados en centros de cómputo de algún proveedor de la nube; y, **nube híbrida**, donde algunos servicios son utilizados en centros de cómputo propios y otros en centros de cómputo de un proveedor de la nube.

Tradicionalmente la computación en la nube ofrece tres modelos de servicios. 1) La infraestructura como servicio IaaS (*Infrastructure as a Service*); 2) Plataforma como servicio PaaS (*Platform as a Service*); y, 3) *Software* como servicio SaaS (*Software as a Service*). Sin embargo, con el crecimiento de su implementación se han desarrollado nuevos servicios y opciones, por ejemplo las copias de respaldo como servicio BaaS (*Backup as a Service*), o la recuperación ante desastres como servicios DaaS (*Disaster Recovery as a Service*). Con este último modelo de servicio se propone que el CCA se traslade a la nube y utilizar o activar dichos servicios en caso algún evento inhabilite los servicios en el CCP. También, se ha diseñado un modelo en la nube que consiste en trasladar de forma parcial o total los servicios del CCP a servicios en la nube y así minimizar el riesgo que los servicios de cómputo se vean afectados al presentarse algún evento negativo en los centros de datos de las organizaciones.

Recientemente se han diseñado nuevos modelos de computación en la nube, como los múltiples, en los que se utilizan diferentes tipos de servicios o diferentes proveedores. Estos modelos pueden brindar ventajas como aumentar la disponibilidad de los servicios y distribuir los riesgos, sin embargo, se convierten en infraestructuras más complejas de implementar y de gestionar.

Es importante indicar que también han evolucionado los estándares internacionales y buenas prácticas en seguridad de la información, así como de tecnología, los cuales han sido adoptados por varios proveedores de servicios en la nube, lo que ha



aumentado la confianza de los usuarios para la adopción de servicios en esta tecnología.

La implementación de un DRP con servicios en la nube puede tener múltiples beneficios, entre los que destacan el hecho de contribuir a reducir el tiempo de recuperación objetivo RTO (*Recovery Time Objective*), así como el punto de recuperación objetivo RPO (*Recovery Point Objective*). Si algún evento afecta las instalaciones de una organización, los servicios y la información en la nube no se verían

afectados, por encontrarse fuera de las instalaciones, permitiendo que el tiempo para activar los servicios tecnológicos en otra ubicación física, se reduzca considerablemente. También impacta positivamente en el aprovechamiento de los beneficios relacionados con la tecnología de la nube, como la flexibilidad, versatilidad, agilidad, entre otros.

Cuando se cuenta con servicios en la nube en los Planes de Recuperación ante Desastres, se debe considerar y asegurar lo siguiente:

- a) Acceder a los servicios en la nube en cualquier momento.
- b) Conectividad a los servicios de la nube desde las ubicaciones donde se necesite operar durante una contingencia, para lo cual es necesario disponer de enlaces a Internet adecuados y redundantes en cada ubicación.
- c) Adecuada selección de proveedores en la nube que tengan implementados controles de seguridad y de gestión.
- d) Establecer desde un inicio la disponibilidad de los servicios en los acuerdos de nivel de servicio con el proveedor de la nube.
- e) Mantener actualizado el DRP para identificar y contemplar los servicios que se encuentren en la nube.

Asimismo, cada organización debe analizar los riesgos asociados a trasladar sus servicios e información a la nube; entre los que podemos mencionar los riesgos tecnológicos, legales y la ubicación donde residan sus servicios y datos.



Para finalizar, es importante recomendar a las organizaciones que utilicen servicios en la nube para su DRP, la adopción interna de buenas prácticas y estándares en seguridad de la información, así como en tecnología, para gestionar adecuadamente su información sin importar dónde se encuentre alojada.



Luis César Vielman Monroy

*Ingeniero en Sistemas de Información y Ciencias de la Computación; Magister Artium en Informática con énfasis en Banca Electrónica y Comunicaciones (Magna Cum Laude), ambas por la Universidad Mariano Gálvez de Guatemala. Posee Certificación ITILv3 Foundation en Gestión de Servicios Tecnológicos, Ingeniero en Sistemas Certificado Microsoft, ha implementado sistemas de gestión certificados en las normas ISO/IEC 20000-1:2011 e ISO/IEC 27001:2013, planes de recuperación ante desastres, entre otros. Es Supervisor del Área de Gestión de Servicios Tecnológicos en el Departamento de Tecnología de la Información de la Superintendencia de Bancos.

¿CÓMO FUNCIONA EL PROCESO DE PREVENCIÓN Y COMBATE DEL LAVADO DE DINERO U OTROS ACTIVOS?

Prevenir y combatir el lavado de dinero y el financiamiento del terrorismo es un esfuerzo de país.



*Artículos 18 de la Ley Contra el Lavado de Dinero u Otros Activos y 5 de su reglamento.

Las **Personas Obligadas** deben conocer a su cliente y el origen de sus recursos para evitar operaciones con dinero y bienes de procedencia ilícita.*

Las **Personas Obligadas** reportan a la Superintendencia de Bancos a través de la Intendencia de Verificación Especial (IVE), las operaciones que no tienen un fundamento económico o legal evidente.

El trabajo de la **IVE**, se activa por los reportes de las **Personas Obligadas** o a requerimiento de autoridad competente.

La IVE, dentro del ámbito estrictamente administrativo, analiza las transacciones reportadas y de encontrar indicios del delito de lavado de dinero, presenta la denuncia ante el Ministerio Público.

El **Ministerio Público** realiza la investigación penal y ejerce la **Acción de Extinción de Dominio**.

El **Organismo Judicial** emite sentencia, al concluir el proceso de investigación.

Personas Obligadas

- Banco de Guatemala
- Bancos del sistema
- Sociedades financieras
- Casas de cambio
- Personas individuales o jurídicas que se dediquen al corretaje o a la intermediación en la negociación de valores
- Emisores y operadores de tarjetas de crédito
- Entidades fuera de plaza off shore
- Empresas que se dedican a las transferencias sistemáticas o sustanciales de fondos y/o movilización de capitales
- Compañías de seguros y fianzas
- Empresas que se dedican a realizar operaciones sistemáticas o sustanciales de canje de cheques
- Instituto de Fomento de Hipotecas Aseguradas
- Entidades que se dedican a factoraje
- Entidades que se dedican al arrendamiento financiero
- Almacenes generales de depósito
- Otras que la legislación someta específicamente a la vigilancia e inspección de la SIB
- Las cooperativas que realicen operaciones de ahorro y crédito, independientemente de su denominación
- Las entidades autorizadas por el Ministerio de Gobernación para realizar loterías, rifas y similares, independientemente de la denominación que utilicen
- Personas jurídicas sin fines de lucro, sin importar su denominación, que reciban, administren o ejecuten fondos del Estado y/o reciban o envíen fondos del o hacia el extranjero
- Intermediarios de seguros a los que se refieren las literales b) y c) del artículo 80 del Decreto Número 25-2010, del Congreso de la República, Ley de la Actividad Aseguradora (agente de seguros independiente y corredores de seguros)

Personas individuales o jurídicas que realicen las actividades siguientes:

- De promoción inmobiliaria o compraventa de inmuebles
- De compraventa de vehículos automotores, terrestres, marítimos o aéreos
- Relacionadas con el comercio de joyas, piedras y metales preciosos
- Relacionadas con el comercio de objetos de arte y antigüedades
- Servicios de blindaje de bienes de cualquier tipo y/o arrendamiento de vehículos automotores blindados

Contadores Públicos y Auditores que presten servicios relacionados con cualquiera de las actividades siguientes:

- Administración de dinero, valores, cuentas bancarias, inversiones u otros activos
- Actividades de contaduría y auditoría en general

Personas individuales o jurídicas que se dediquen a prestar servicios por instrucciones y/o a favor de sus clientes o terceros relacionados con cualquiera de las actividades siguientes (servicios societarios):

- Actuación, por sí mismo o a través de terceros, como titular de acciones nominativas, socio, asociado o fundador de personas jurídicas
- Actuación por sí mismo o a través de terceros, como director, miembro del consejo de administración o junta directiva, administrador, apoderado o representante legal de personas jurídicas
- Provisión de dirección física para que figure como domicilio fiscal o sede de personas jurídicas

www.sib.gov.gt



SIB Guatemala



@sib_guatemala



SuperBancosGuatemala



sib_guatemala



Superintendencia de Bancos (SIB)



Superintendencia de Bancos
Guatemala, C. A.