Edición Nro. 39
Año 10

Guatemala
Marzo 2021

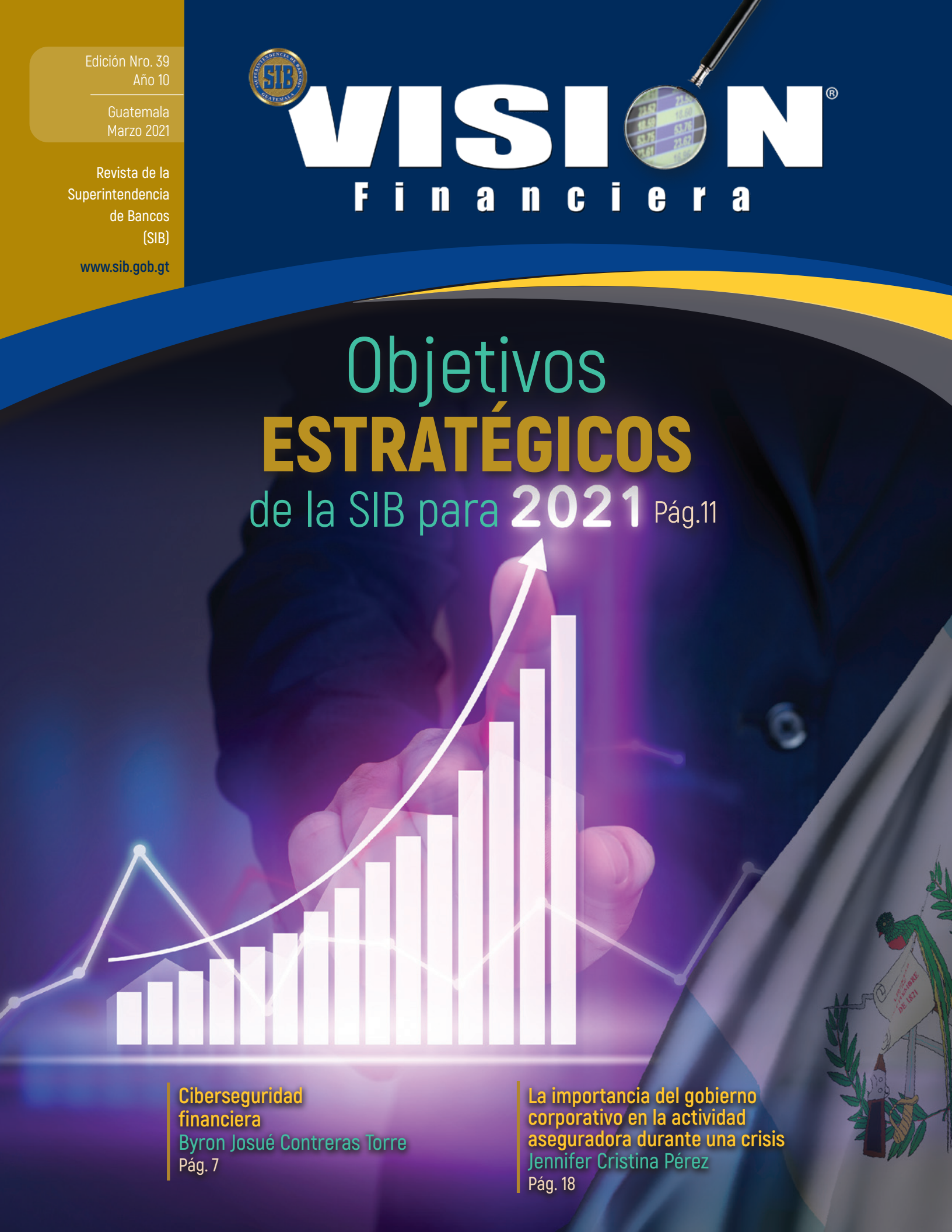
Revista de la Superintendencia de Bancos (SIB)

www.sib.gob.gt

VISION Financiera

Objetivos ESTRATÉGICOS de la SIB para 2021

Pág.11



Superintendencia de Bancos
Guatemala, C. A.

Contenido

Directorio

Director General
Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Consejo Editorial
Lic. Hugo Rafael Oroxóm Mérida
Intendente de Coordinación Técnica

Lic. Byron Vinicio Méndez Castillo
Intendente de Estudios y Normativa

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

Coordinador General
Lic. Hugo Rafael Oroxóm Mérida
Intendente de Coordinación Técnica

Director de Proyecto
Lcda. Nancy Verónica Carranza Sazo
Supervisor en funciones
Departamento de Desarrollo Institucional

Superintendencia de Bancos
Unidad de Información Pública
15 avenida 7-18, zona 13, Edificio Zepto, Nivel 3
PBX: 2429-5000 y 2204-5300
Ext. 1+2560/2561/2567
Correo electrónico: info@sib.gob.gt
www.sib.gob.gt

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

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Apreciables lectores:

En esta oportunidad, la edición 39 de la revista **Visión Financiera**, presenta como tema central la importancia de los objetivos estratégicos de la Superintendencia de Bancos para 2021, conoceremos su composición, el fundamento y el desarrollo deseado de dichos objetivos, factores esenciales para visualizar el futuro cercano de nuestra Institución.

Abordaremos el rol e importancia de la planeación estratégica, la cual es necesaria para establecer el marco de acción y los grandes temas en los cuales se enfoca la SIB, así como los planes para alcanzar los resultados deseados.

La responsabilidad de implementar la estrategia institucional descrita en el plan estratégico 2021, es un reto que no solo recae en el Comité de Dirección Estratégica, sino también en cada uno de los colaboradores de la SIB. Estos desafíos se enmarcan en temas estratégicos como la supervisión efectiva con un marco legal y regulatorio moderno, conforme a las mejores prácticas y estándares internacionales; la estabilidad, modernización e innovación del sistema financiero del país, así como la prevención de lavado de dinero u otros activos, del financiamiento del terrorismo y de la proliferación de armas de destrucción masiva.

Estos tres temas se desglosan en catorce objetivos estratégicos, cuya orientación y de acuerdo con la metodología implementada *Balanced Scorecard* (BSC) están distribuidos en las perspectivas de innovación y aprendizaje, procesos internos y usuarios. Por consiguiente, cada objetivo descansa en una serie de iniciativas estratégicas, las cuales se establecen con actividades, responsables y fechas, a fin de unificar esfuerzos y obtener los resultados previstos.

El seguimiento a la efectividad institucional es vital para conocer los avances del plan estratégico, estos se revisan con base a los indicadores establecidos para cada uno de los objetivos estratégicos y, en función de los resultados obtenidos se toman las decisiones que coadyuven a seguir en la dirección planificada. No hay que olvidar que estos objetivos estratégicos constituyen el camino que nos llevará a construir el futuro con las herramientas necesarias y apropiadas para enfrentar los cambios, que son constantes y desafiantes, motivo por el cual la Superintendencia de Bancos mantiene su compromiso de continuar trabajando para cumplir con su misión de ***"Promover la estabilidad y confianza en el sistema financiero supervisado".***

Es importante resaltar que los pilares anteriores descansan en una estrategia de transformación digital en la organización basada en la cultura, la gestión y las competencias digitales necesarias para cumplir con las funciones en la Institución. Esta estrategia se basa en la incorporación de la tecnología en sus procesos, procedimientos e información, complementada con un liderazgo y modelo de cambio que conlleve a una reorganización digital donde los procesos, personas y sistemas estén plenamente sincronizados, que implique un modelo de gestión y ejecución iterativo en busca de una mejor utilización de los recursos, mayor eficiencia y productividad.

Todo lo anterior, sin duda, hará que la Superintendencia de Bancos continúe manteniendo el liderazgo nacional e internacional en los esquemas de supervisión, regulación y gestión; implementando los nuevos desarrollos e innovaciones en un cuidadoso entorno de regulación prudencial, de manera que, los logros alcanzados sean sostenibles en el largo plazo y constituyan una sólida plataforma y contribuyan así al desarrollo de nuestro país.

Finalmente, agradezco a nuestra pluma invitada, Ing. Juan Carlos Morales Baten, Director Académico de ISACA *(Information Systems Audit and Control Association)* Capítulo Guatemala, quien desarrolla el tema sobre la importancia de la implementación de estándares y mejores prácticas en la gestión del riesgo tecnológico en instituciones financieras; así como también a los expertos colaboradores de la Superintendencia de Bancos, quienes han preparado artículos de interés y actualidad entre los cuales se encuentran el impacto de las principales medidas temporales emitidas por la autoridad monetaria derivado de la pandemia COVID-19; regulación y supervisión de reservas técnicas; importancia del gobierno corporativo en la actividad aseguradora durante una crisis; ciberseguridad financiera; y, la importancia de la gobernanza de datos.

Atentamente,

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos

Importancia de la implementación de estándares y mejores prácticas en la gestión del riesgo tecnológico en instituciones financieras

Juan Carlos Morales Baten

Director Académico en ISACA Capítulo Guatemala

Ingeniero de Sistemas y *Magister Artium* en Administración de Empresas con Especialización en Mercadeo (ESEADE) ambos títulos otorgados por la Universidad Francisco Marroquín de Guatemala. Posee más de 40 años de experiencia profesional en Tecnología de la Información (TI) colaborando con instituciones bancarias y multinacionales como *Shell Royal Dutch, Wal-Mart* y *Bayer*. Ha desempeñado posiciones a nivel internacional. Ha realizado auditorías de sistemas en los Estados Unidos de América, Brasil, Argentina, Chile, Holanda, Inglaterra y Malasia. Autor de cuatro libros y colaborador experto para la revista *Computer World* de España. Es Consultor Internacional, Auditor e Instructor acreditado por *APMG International* de COBIT 2019, CISA, CISM, CRISC y GETI.

Cuando estás utilizando una aplicación en tu teléfono, la computadora portátil, una computadora de escritorio o estás frente a un mostrador realizando una gestión financiera, dependes en gran medida de la tecnología para completar tu transacción.

La tecnología facilita la entrega de los servicios financieros, pero conlleva riesgos inherentes (de su propia naturaleza). Es por ello que las organizaciones deben estar conscientes de la necesidad de gestionar dichos riesgos. Este artículo se enfoca en las instituciones financieras por su dependencia en la tecnología y el impacto que pueda tener en sus clientes, incluyéndote a ti.

Al cuestionarnos acerca de la mejor manera de gestionar el riesgo tecnológico en las instituciones financieras, debemos de pensar que no estamos solos. Existe una gran cantidad de personas y organizaciones que contribuyen a desarrollar y actualizar estándares y mejores prácticas que

pueden ayudarnos a gestionar los riesgos de la tecnología. Todo esto basado en muchos años de experiencia, conocimientos acumulados, en constante revisión, y que se mantienen vigentes.

¿Qué son buenas o mejores prácticas? Se entiende como un conjunto de acciones que han dado buenos resultados en un determinado contexto y que se espera funcionen en entornos similares. Todas las organizaciones tienen como objetivo común la creación de valor, el cual se entrega por medio de productos y servicios. Las actividades que se realizan para alcanzar este objetivo se pueden agrupar en prácticas, por eso se recomienda adaptar al ambiente único de cada organización, las buenas prácticas descritas en los marcos de referencia y los estándares internacionales.

¿Qué es riesgo? La ISO 31000 define el riesgo como el efecto de la incertidumbre en el logro de los objetivos. Gestionar riesgos conlleva lo siguiente:

- Identificar y registrar los riesgos.
- Analizar las características de los riesgos identificados.
- Evaluar el nivel de riesgo comparándolo contra los criterios previamente definidos.
- Establecer prioridades y decidir cómo tratar cada riesgo de acuerdo con el resultado de la evaluación.
- Monitorear todos los riesgos identificados, incluyendo los que han sido aceptados e informar sobre estos a quien deba tomar decisiones con base a su conocimiento.

Se debe crear una cultura de riesgos en la organización, definir los criterios que se deben utilizar para emitir un juicio acerca de la importancia de estos, definir umbrales de tolerancia y asegurarse que los mismos se gestionen.

Los marcos de referencia proveen principios y buenas prácticas; por ejemplo, COSO es de gran utilidad para la implementación de control interno y para establecer una cultura favorable para el gobierno y la gestión de riesgos, todo esto para tener una mayor certeza de que la organización logre alcanzar sus objetivos.

COBIT aporta principios y un modelo de objetivos de gobierno y gestión para la información y la tecnología. Como parte esencial de un buen gobierno organizacional, se deben crear las estructuras apropiadas y establecer procesos, cada uno con un propósito alineado al logro de los objetivos estratégicos. COBIT recomienda una visión holística en la cual se consideren todos los componentes de un sistema de gobierno y gestión: los principios, políticas, procedimientos, información, cultura, ética, comportamiento, personas, habilidades, competencias, servicios, infraestructura, aplicaciones, procesos y estructuras organizacionales.

ITIL es otro marco recomendable que contiene las buenas prácticas para la gestión de servicios.

¿Con qué nivel de riesgo se siente usted confortable? No siempre se trata de reducir el riesgo. Hay ocasiones en las que los empresarios ven oportunidades y están dispuestos a arriesgar más. Optimizar el riesgo consiste en llevarlo al nivel aceptable, y esto se logra con el gobierno y la gestión.

El modelo COSO nos dice que la organización debe especificar sus objetivos con suficiente claridad para permitir la identificación de los riesgos relacionados. Esto incluye la probabilidad de fraude. También indica la necesidad de analizarlos y evaluarlos para gestionarlos, y seleccionar y desarrollar actividades de control que contribuyan a la mitigación de los riesgos, para llevarlos a niveles aceptables para el logro de los objetivos.

El principio once del modelo COSO afirma que la organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.

¿Qué es un estándar? La Real Academia Española (RAE) define la palabra estándar como un modelo, norma, patrón o referencia. La Organización Internacional de Estándares (ISO, por sus siglas en inglés), crea documentos que proporcionan requisitos, especificaciones, pautas o características que se pueden usar de manera consistente para garantizar que los materiales, productos, procesos y servicios sean adecuados para su propósito.

Entre los principales estándares relacionados de alguna manera con las buenas prácticas o requerimientos para la gestión del riesgo tecnológico podemos mencionar los siguientes:

- ISO 31000 estándar de gestión de riesgos.
- ISO/IEC 27001 contiene los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.
- ISO 9001 estándar de calidad.
- ISO 38500 estándar para el gobierno de tecnología de la información.
- ISO 20000 estándar para la gestión de servicios.
- ISO 22301 estándar que contiene los requerimientos para establecer, implementar, mantener y mejorar un sistema de gestión de continuidad.
- ISO 22317 contiene las especificaciones técnicas para realizar un análisis de impacto en el negocio (BIA, por sus siglas en inglés).

El estándar de gestión de riesgos ISO 31000 reconoce la complejidad de estos y proporciona principios y guías. Afirma que, para ser eficaz, la gestión de riesgos requiere ser parte integral de los procesos, políticas y cultura de la organización.

La información es un activo muy valioso que debemos proteger. Sabemos que los datos se transforman en información y que, a su vez, esta se transforma en conocimiento, el cual utilizamos para tomar decisiones correctas. El principio trece del modelo COSO afirma que la organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.

La esencia de la seguridad de la información es la protección de la confidencialidad, integridad y disponibilidad de la información. Esto se logra por medio de un sistema de gestión. El órgano de gobierno, tiene como parte de sus responsabilidades, supervisar la seguridad de la información para garantizar que se alcancen los objetivos de la organización.

Una institución financiera es la que facilita servicios financieros a sus clientes o miembros. En Guatemala la Superintendencia de Bancos es la entidad que ejerce la vigilancia e inspección sobre instituciones bancarias, sociedades financieras, compañías almacenadoras, compañías de seguros, casas de cambio, entidades fuera de plaza o entidades *off shore*, casas de bolsa, tarjetas de crédito y otras instituciones.

Dada la importancia que tiene para el país la gestión del riesgo tecnológico en instituciones financieras, la Superintendencia de Bancos elevó a consideración de la Junta Monetaria el proyecto de Reglamento para la Administración del Riesgo Tecnológico, el cual fue autorizado para su publicación y vigencia a partir del 1 de septiembre de 2011. Este reglamento es conocido como JM-102-2011. En 2020 fue actualizado, incorporando el tema de seguridad cibernética con la publicación de la Resolución JM-42-2020.

En el artículo uno, se define el objetivo del reglamento de la manera siguiente: establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades *off shore* y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deberán cumplir para administrar el riesgo tecnológico. Adicionalmente, hace mención del artículo 55 de la Ley de Bancos y Grupos Financieros el cual establece que los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, del cual forma parte el riesgo tecnológico, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de gestionar los mismos.

También, es importante tener presente el Reglamento para la Administración del Riesgo Operacional publicado en 2016 con el propósito de regular los aspectos necesarios para la gestión del riesgo operacional en las entidades financieras supervisadas.

Hay muchas personas contribuyendo a que se pueda llevar a cabo la gestión eficaz del riesgo tecnológico. Ellos invierten su tiempo y conocimiento creando y actualizando reglamentos, marcos de referencia y estándares. Nos corresponde conocerlos y aplicarlos al contexto único en nuestra organización.

Ciberseguridad financiera

Byron Josué Contreras Torre

Inspector del Departamento de Supervisión de Riesgos Específicos de la SIB

Ingeniero en Sistemas por la Universidad Mariano Gálvez de Guatemala, con Maestría en Administración de Negocios por la misma Universidad; y, Maestría en Seguridad Informática y Redes de Computadoras por la Universidad Galileo de Guatemala. Cuenta con certificaciones internacionales reconocidas y avaladas por *Cisco System, Hewlett-Packard, Microsoft, Aruba Networks* y *F5 Networks*. Posee experiencia en el ámbito de ciberseguridad, *hacking* ético, seguridad de la información, servidores, virtualización, redes y telecomunicaciones en el área de banca y multinacionales.

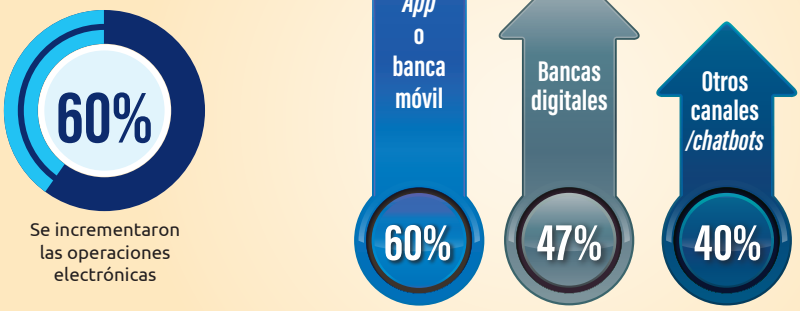
Las entidades financieras realizan inversiones en tecnología de la información para modernizar los servicios financieros que ofrecen al público y que estos sean más eficientes, dinámicos y ágiles; sin embargo, cada nueva implementación tecnológica conlleva sus riesgos, los cuales se incrementan cuando no se consideran procedimientos adecuados y buenas prácticas, dejando al descubierto brechas y vulnerabilidades que podrían ser aprovechadas por cibercriminales, de ahí la importancia de gestionar adecuadamente la ciberseguridad.

Mayor exposición de los servicios financieros

En 2020, derivado de la pandemia del COVID-19, se incrementó exponencialmente el uso de los canales electrónicos, como consecuencia, los sectores financieros en el mundo se han visto afectados

por el incremento de ciberamenazas[1], ciberataques[2] e incidentes cibernéticos[3] como ingeniería social[4], *phishing*[5], *smishing*[6], *vishing*[7], *ransomware*[8], *botnets*[9], *clickjacking*[10], entre otros. De hecho, a nivel mundial los ciberataques reportados para los distintos sectores de comercios globales fueron: manufactura 26%, comunicación y medios 18%, servicios profesionales 14% y financieros 42%, es decir este último sector con la mayor cantidad, afectando el robo de datos, suplantación de identidad y daños a la imagen corporativa[11].

AUMENTO EN 2020 A NIVEL GLOBAL EN OPERACIONES BANCARIAS A TRAVÉS DE CANALES ELECTRÓNICOS



Fuente: *MastercardEconomicsInstitute.* Economía 2021.

En cuanto a las operaciones bancarias en el mundo a través de canales electrónicos, presentaron en 2020 un crecimiento del 60%; y, cada uno de los principales canales de servicio como las *App's* o banca móvil, bancas digitales y otros canales incluyendo *chatbots*, aumentaron 60, 47 y 40 por ciento, respectivamente. Lo anterior apunta a que, entre los principales objetivos de los ciberataques, seguirá encontrándose el sector financiero.

En ese sentido, las entidades financieras y los clientes han sido afectados por el robo de información y por pérdidas financieras, siendo el aspecto más relevante el riesgo para la estabilidad financiera, por una parte, debido a la potencial pérdida de la confianza cuando los clientes ven vulnerados sus datos personales; y, por otra, por la falta de continuidad en la prestación de servicios (interrupciones prolongadas en sistemas e infraestructura tecnológica propia y de terceros). Debido a lo anterior, es necesario comprender el contexto de la ciberseguridad y aprender a protegerse de las ciberamenazas, ciberataques e incidentes cibernéticos.

1 Es una circunstancia, situación, evento o acto con el potencial de convertirse en un ciberataque.
2 Es un evento con la intención de causar daño en uno o varios activos en el ciberespacio.
3 Es un ciberataque que vulneró en forma individual o conjunta la confidencialidad, integridad y/o disponibilidad de la información.
4 Ingeniería social, técnica para interactuar con los usuarios y manipularlos para que entreguen su información.
5 ***Phishing***, sitios web similares al original o falsos que engañan a los usuarios para obtener información personal.
6 ***Smishing***, técnica a través de mensajes de texto para que los usuarios proporcionen información.
7 ***Vishing***, técnica a través de llamadas telefónicas para que los usuarios proporcionen información.
8 ***Ransomware***, programa que cifra archivos de forma mal intencionada y que impide el acceso al computador.
9 ***Botnets***, robots informáticos que se ejecutan de forma automática para una tarea maliciosa.
10 ***Clickjacking***, código web que engaña a los usuarios para robar la información.
11 ***MastercardEconomicsInstitute***.- Economía 2021. Expansión -Economía digital.

Para las entidades financieras es imprescindible que el equipo de seguridad de la información esté debidamente capacitado y disponga de los recursos necesarios, con el objetivo de gestionar la ciberseguridad y, en consecuencia, garantizar la confidencialidad, integridad y disponibilidad de la información propia y de los clientes. No obstante, es importante que los clientes que utilizan canales electrónicos tengan conocimientos básicos sobre las amenazas de seguridad de la información a que están expuestos y de las posibles formas en que pueden ser engañados.

Ingeniería social, uno de los ciberataques más efectivos que afecta a entidades financieras y clientes

Existen ataques cibernéticos que utilizan tecnologías muy sofisticadas; sin embargo, una de las más efectivas y exitosas es la ingeniería social, que combina la habilidad de los ciberdelincuentes con la carencia de malicia y de conocimientos técnicos en el campo de la tecnología por parte de clientes. Las modalidades más comunes de ingeniería social son *phishing, smishing* y *vishing*.

Estas modalidades de fraude cibernético son muy habituales en todo el mundo y se aplican, principalmente, en las plataformas electrónicas de banca en línea o en las aplicaciones que funcionan en los dispositivos móviles. Con frecuencia, el fraude se lleva a cabo de la forma siguiente:

1. El perpetrador, mediante engaño (suplantación de identidad) obtiene información personal del cliente, por ejemplo, números de teléfono, números de cuentas bancarias y credenciales para acceso a los canales electrónicos (nombre de usuario y contraseña).
2. El perpetrador se asegura de tener una cuenta bancaria en la misma entidad en donde el cliente guarda su dinero.
3. El perpetrador accesa en alguno de los canales electrónicos de la entidad, utilizando las credenciales robadas y realiza una transferencia de la cuenta bancaria del cliente hacia su cuenta.
4. Debido a que la plataforma tecnológica de la entidad implementa un mecanismo de seguridad de doble factor, genera un *token* que es enviado al teléfono celular del cliente. El perpetrador en ese sentido, mediante mecanismos de ingeniería social (engaño), llama al cliente y le pide el número del *token* necesario para completar la transferencia.
5. El perpetrador ejecuta la transferencia de la cuenta bancaria del cliente hacia la cuenta bancaria propia; luego, con la ayuda de una segunda persona, realiza el retiro de dinero de un cajero automático con lo que el fraude queda consumado.

Importancia de la concientización de los usuarios de los servicios financieros

Sin perjuicio de los controles de seguridad que la entidad financiera tenga implementados en la plataforma tecnológica que da soporte a los canales electrónicos, el fraude financiero se concreta debido al engaño que sufren algunos clientes, mediante técnicas de ingeniería social.

Por tanto, las entidades financieras tienen un reto importante para implementar estrategias y campañas de concientización para sus clientes y usuarios internos, en materia de ciberseguridad.

Si bien la responsabilidad de la seguridad de la información es tanto de la entidad bancaria como del cliente, por constituir el eslabón de mayor debilidad, se recomienda a este último implementar las medidas siguientes:

1. Pago por métodos seguros con tarjetas de crédito y débito.
2. Evitar entregar tarjetas de crédito y débito a desconocidos.
3. Utilizar contraseñas robustas, cambiarlas con frecuencia, que sean distintas de otras cuentas utilizadas y no proporcionar contraseñas a terceras personas.
4. Utilizar, cuando están disponibles, factores de doble autenticación o *tokens*, para la autorización de operaciones.
5. Guardar en los favoritos de los navegadores los sitios web de los bancos utilizados con frecuencia y de esa manera evitar navegar en sitios web fraudulentos.
6. Validar el certificado digital cuando hacen compras en sitios web.
7. Ser muy cauteloso con mensajes de texto y llamadas telefónicas que piden datos personales.
8. No exponer datos personales en redes sociales.
9. No acceder a correos electrónicos y documentos adjuntos de procedencia desconocida.
10. Evitar conectar sus dispositivos a redes públicas (*wifi* o conexiones por cable).
11. No dejarse llevar por falsas promociones o premios, donde se requiere información confidencial.

Buenas prácticas y normativa para la gestión de la ciberseguridad

A medida que las ciberamenazas y ciberataques evolucionan y se vuelven más sofisticados, se hace necesario contar con controles, buenas prácticas y estándares internacionales en materia de ciberseguridad, con el objetivo de minimizar y gestionar dichos riesgos.

En ese contexto, la Superintendencia de Bancos de Guatemala consideró conveniente promover la incorporación al Reglamento para la Administración del Riesgo Tecnológico (Resolución JM-102-2011), de disposiciones mínimas para la gestión de la ciberseguridad, con el objetivo de que las instituciones puedan detectar, resistir, responder y recuperarse rápidamente de un ciberataque. Por tal motivo, dicho reglamento fue actualizado mediante Resolución JM-42-2020 en abril de 2020, entre otros, con aspectos basados en los estándares internacionales sobre la materia, siguientes:

1	Gestión de la ciberseguridad.
2	Designación de un Oficial de Seguridad de la Información (CISO[12]).
3	Implementación de un Centro de Operaciones de Incidentes Cibernéticos (SOC[13]).
4	Implementación de un Equipo de Respuesta de Incidentes Cibernéticos (CSIRT[14]).
5	Incorporación de aspectos de ciberseguridad en la contratación de proveedores.

Adicionalmente, en virtud de dicha modificación, las entidades deben contar con un plan de recuperación ante desastres, con el objetivo de garantizar la continuidad de las operaciones, en caso de un incidente mayor en sus sistemas de información e infraestructura tecnológica.

12 *Chief Information Security Officer.*
13 *Security Operation Center.*
14 *Computer Security Incident Response Team.*

Objetivos estratégicos de la SIB para 2021

Erick Armando Vargas Sierra

Superintendente de Bancos de Guatemala

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. Expresidente del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO).

En cualquier organización, pública o privada, la planeación estratégica se constituye en una herramienta imprescindible para la toma de decisiones, en el corto y mediano plazo, en especial cuando es necesario seleccionar los objetivos estratégicos que permitirán que la organización alcance su misión y visión. En ese sentido, la Superintendencia de Bancos (SIB) ha venido estructurando su ejercicio de planeación con el apoyo fundamental de sus más altas autoridades, quienes, de manera multianual, analizan diferentes retos internos y externos de la Institución, las tendencias que podrían afectar al sistema financiero nacional y cualquier otro componente que requiera hacer ajustes en la hoja de ruta trazada en la organización para ser referente, tanto a

nivel nacional como regional y cumplir con la implementación de las mejores prácticas y estándares internacionales aplicables al ente supervisor de Guatemala. En consecuencia y, como resultado del proceso de evaluación y ejecución del plan estratégico, en el 2021 la SIB ha realizado ajustes a sus objetivos estratégicos que permitirán alcanzar su misión, la cual es, promover la estabilidad y confianza en el sistema financiero supervisado. En el siguiente diagrama se resumen los tres temas y pilares estratégicos que guían el quehacer de la Institución.

Fuente: SIB

El primer tema estratégico, es la supervisión efectiva con un marco legal y regulatorio moderno, conforme a las mejores prácticas y estándares internacionales, el cual busca promover que las entidades sujetas a su vigilancia e inspección implementen adecuadas prácticas de gobierno corporativo y de gestión de riesgos, a través de la aplicación de un enfoque de supervisión basado en riesgos de naturaleza prospectiva, al mismo tiempo que se moderniza el sistema financiero y su regulación, aspectos que se constituyen en los elementos de mayor énfasis en el 2021 y que han requerido realizar ajustes a los objetivos estratégicos de corto y mediano plazo.

En efecto, el Comité de Dirección Estratégica de la Superintendencia de Bancos, que tiene por objeto diseñar y dar seguimiento a la implementación de la estrategia institucional, alinear la gestión operativa y el diseño de proyectos integrales e institucionales de carácter estratégico a fin de definir una hoja de ruta completa para su realización, decidió incorporar el aspecto prospectivo en la supervisión y regulación financiera que implica, en primer lugar, centrar a la organización en datos para la toma de decisiones y, en segundo, incorporar las herramientas, modelos e indicadores que permitan a la SIB anticiparse a los eventos que pueden afectar el ciclo financiero y, por ende, a las instituciones financieras; así como utilizar la información y datos para desarrollar normativa basada en estándares internacionales y mejores prácticas que contenga elementos de medición de riesgos de naturaleza prospectiva, en particular el esquema de provisiones y las pruebas de resistencia, lo que coadyuvará a la generación de una cultura de riesgos.

Fuente: SIB

Desde una perspectiva metodológica la SIB desarrollará un marco integral que permita llevar a cabo un análisis de sensibilidad y de pruebas de resistencia utilizando modelos propios, considerando a su vez los elementos proporcionados por las entidades y sus respectivas evaluaciones para evaluar la liquidez y solvencia ante diversos escenarios en un determinado horizonte de tiempo. Asimismo, se desarrollarán esquemas de alerta temprana con carácter individual y sistémico, y se incorporarán elementos regulatorios que permitan evaluar la viabilidad de una institución, como los planes de recuperación y resolución, siendo estos una herramienta esencial en las evaluaciones y monitoreo de la Superintendencia de Bancos. Lo anterior, con el firme convencimiento de que anticiparse a los riesgos es siempre menos costoso que abordarlos cuando estos se materializan, lo cual, como la historia a nivel mundial lo ha confirmado una y otra vez, en ciertas circunstancias es demasiado tarde.

En este pilar también se continuará fortaleciendo la supervisión consolidada y transfronteriza emprendiendo acciones para mejorar el marco de supervisión aplicable a las entidades supervisadas en lo individual y desde el punto de vista consolidado y transfronterizo, en línea con las mejores prácticas y con el fortalecimiento de las disposiciones legales y normativas para el efecto. Por su parte, la supervisión macroprudencial continuará brindando herramientas para identificar y cuantificar el impacto de choques externos y domésticos en la estabilidad financiera y en la situación individual de cada entidad del sistema financiero; así como herramientas que permitan identificar exposiciones comunes, concentraciones de riesgos, vínculos e interconexiones que pueden ser fuentes de contagio y poner en riesgo el funcionamiento del sistema financiero.

Otro elemento primordial, es el fortalecimiento de la red de seguridad financiera que permita robustecer el marco institucional, los procedimientos y mecanismos que contribuyen a la estabilidad del sistema financiero, particularmente, en materia de riesgo sistémico en la resolución de entidades financieras, que conlleva necesariamente la adopción de los estándares internacionales en esta materia. En el componente normativo, en adición a los esquemas prospectivos señalados anteriormente, se continuará fortaleciendo las normas y analizando la necesidad de incorporar nueva normativa derivado de las innovaciones en el sector financiero, que permita, por un lado, el desarrollo e innovación de los canales digitales y, por otro, un crecimiento ordenado sin poner en riesgo la estabilidad financiera, así como la normativa para hacer frente a los riesgos cibernéticos.

El segundo pilar, que se refiere a la estabilidad, modernización e innovación del sistema financiero incorpora la implementación de una estrategia de gobierno de datos, definido como el conjunto de procesos, funciones, políticas, normas y mediciones que garantizan el uso eficaz y eficiente de la información con el fin de generar información oportuna y de calidad para uso interno y de terceros, aspectos clave para el diseño y la calibración de los modelos prospectivos comentados anteriormente y aplicados al ejercicio de las funciones de supervisión y

regulación. De esa cuenta las decisiones se basarán en información y datos en su nivel más alto de madurez. La implementación del gobierno de datos es un proceso crítico donde se reconoce ampliamente que los datos son un activo institucional muy valioso que se debe gestionar dentro de un marco de referencia basado en estándares internacionales. Contar con un gobierno de datos, es crucial y estratégico para la Superintendencia de Bancos, que permitirá hacer uso de las principales tendencias e innovaciones tecnológicas como: computación en la nube, inteligencia artificial, técnicas de *machine learning,* entre otras. En consecuencia, se espera que la SIB, sea un órgano supervisor referente, tanto en Centroamérica como en Latinoamérica al estar entre los primeros que aplican un gobierno de datos en el ejercicio de sus funciones, en especial al implementar las estrategias de gobierno de datos, complementada con la de gestión de datos y la de alineación de datos.

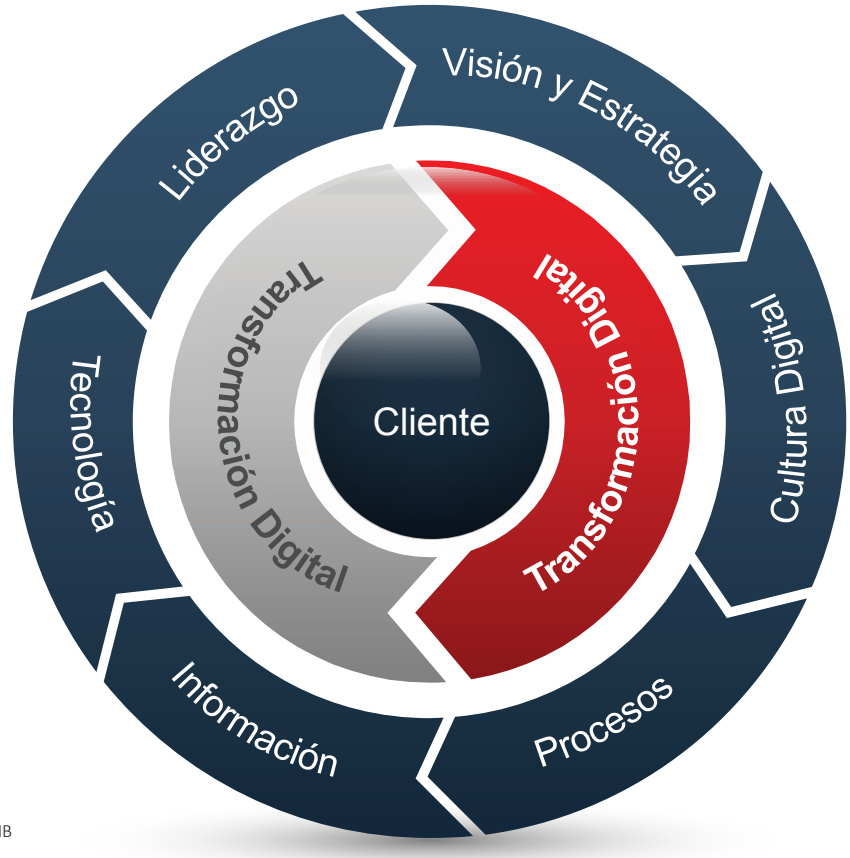
Aunado a lo anterior y, en línea con las mejores prácticas internacionales, en la Superintendencia de Bancos de Guatemala, se creó la figura del Oficial de Seguridad de la Información (CISO, por sus siglas en inglés), como parte de la respuesta estratégica que los entes supervisores y reguladores deben implementar para hacer frente a los ataques cibernéticos, un riesgo cada vez más relevante a nivel mundial. En ese orden de ideas, se ha iniciado una capacitación y concientización con el sistema bancario nacional. El Oficial de Seguridad de la Información estará encargado, entre otros aspectos, de definir la estrategia global de seguridad de la información de la Institución, coordinar su materialización en todos los ámbitos de esta, identificar el nivel de riesgo existente y promover una cultura de resiliencia en esta materia.

El tercer pilar busca prevenir el lavado de dinero u otros activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva, además de impulsar un cambio legal, se incorporó la generación de información estratégica y de inteligencia, lo cual en conjunto con una supervisión basada en riesgo de las Personas Obligadas y una gestión y análisis operativo de la información, todo lo anterior basado en las mejores prácticas, permitan combatir este flagelo en el país y cumplir con los estándares internacionales en este tema.

Es importante resaltar que los pilares anteriores descansan en una estrategia de transformación digital en la organización basada en la cultura, la gestión y las competencias digitales necesarias para cumplir con las funciones en la Institución. Dicha estrategia se apoya en la incorporación de la tecnología en los procesos, procedimientos e información de la SIB, complementada con un liderazgo y un modelo de cambio que conlleve una reorganización digital donde los procesos, personas y sistemas estén plenamente sincronizados, que implique un modelo de gestión y ejecución iterativo en busca de una mejor utilización de los recursos y mayor eficiencia y productividad.

Todo lo anterior, sin duda, hará que la Superintendencia de Bancos continúe manteniendo el liderazgo nacional e internacional en los esquemas de supervisión, regulación y gestión; implementando los nuevos desarrollos e innovaciones en un cuidadoso entorno de regulación prudencial, de manera que los logros alcanzados sean sostenibles en el largo plazo y constituyan una sólida plataforma y contribuyan así al desarrollo de la economía guatemalteca.

LOS PILARES CLAVE DE LA TRANSFORMACIÓN DIGITAL



Fuente: SIB

Regulación y supervisión de reservas técnicas

Genrry Amado Tzoc Chen

Inspector del Departamento de Supervisión de Riesgos de Seguros y Otros de la SIB

Contador Público y Auditor con Maestría en Administración Financiera, ambas por la Universidad Mariano Gálvez de Guatemala; y, Licenciado en Ciencias Jurídicas y Sociales, Abogado y Notario por la Universidad Da Vinci de Guatemala, con experiencia en operaciones financieras en los sectores público y privado. Tiene más de 20 años al servicio de la Superintendencia de Bancos, con conocimientos en ejecución presupuestaria, relaciones laborales, operaciones bancarias y de seguros, mercados financieros, lavado de dinero y operaciones de banca central.

Regulación y supervisión

El artículo 2 del Decreto número 18-2002 Ley de Supervisión Financiera, del Congreso de la República de Guatemala, define la función de supervisión que realiza la Superintendencia de Bancos, a las entidades sujetas a su vigilancia e inspección, entre otras, a las entidades de seguros, indicando que en ningún caso dicha función implica la asunción de responsabilidades por esta o por sus autoridades, funcionarios o personal, por la gestión que las mismas realicen, ni garantiza el buen fin de dicha gestión, pues la misma es siempre por cuenta y riesgo de la propia entidad.

Empresas de seguros

El artículo 875 del Decreto número 2-70, Código de Comercio de Guatemala, define que se le considera asegurador: a la sociedad mercantil autorizada legalmente para operar seguros, que asume los riesgos especificados en el contrato de seguro. Asimismo, el artículo establece que la prima es

la retribución o precio del seguro, el siniestro es la ocurrencia del riesgo asegurado; y, el riesgo es la eventualidad de todo caso fortuito que pueda provocar la pérdida prevista en la póliza.

Reservas técnicas

Por su parte, el artículo 2 del Reglamento para la constitución, valuación e inversión de las reservas técnicas de aseguradoras y de reaseguradoras, anexo a la resolución de Junta Monetaria JM-3-2011, establece que estas constituyen las provisiones que reflejan el valor cierto o estimado de las obligaciones contraídas por las aseguradoras o reaseguradoras derivado de los contratos suscritos.

De conformidad con el Decreto número 25-2010 del Congreso de la República de Guatemala, Ley de la Actividad Aseguradora y el reglamento referido en el párrafo anterior, las entidades aseguradoras tienen la obligación de calcular y contabilizar las reservas o provisiones técnicas siguientes:

- Reservas para seguros de vida (matemáticas)
- Reservas para seguros de daños (de riesgo en curso)
- Reservas para riesgos catastróficos
- Reservas para obligaciones pendientes de pago
- Reservas para primas anticipadas
- Otras reservas de previsión extraordinarias y contingentes

Dichas reservas, deben estar invertidas en todo momento, en la moneda correspondiente y en los activos que la misma normativa establece.

En concordancia con la normativa indicada, dada la naturaleza de sus operaciones, dentro de los principios de seguros emitidos por la Asociación Internacional de Supervisores de Seguros (IAIS, por sus siglas en inglés), se establece que las aseguradoras deben identificar y cuantificar sus obligaciones existentes con el fin de garantizar que las reservas técnicas sean suficientes para cubrir todos los reclamos por siniestros.

También se establece que las aseguradoras deben administrar sus inversiones de forma sana y prudente, para evitar problemas de liquidez y solvencia en el corto plazo.

IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

A lo largo de la historia, se ha visto una evolución en la regulación para la constitución de las reservas técnicas, la cual va desde el cálculo de la Reserva de Prima No Devengada (RPND), que asume una distribución uniforme de los siniestros, seguida del cálculo de la Reserva de Insuficiencia de Prima (RIP), que complementaba a la RPND con un enfoque totalmente contable; y luego aparece el cálculo mediante "casos especiales y modelos propios" de las aseguradoras, debido a que el regulador reconoce que existen líneas de negocio a las que no aplica un enfoque de RPND puro, llegando finalmente, a los cálculos considerados en regulaciones más modernas a través de las denominadas *Best Estimate*, las cuales se orientan a la generación de flujos de ingresos y salidas de mayor estimación[1].

1 Taller actuarial Regulación y Supervisión de Reservas – *Insurance and Actuarial Engineering - Prime Re Solutions* – noviembre 2020.

Derivado de la importancia que las reservas técnicas tienen para la actividad aseguradora y como parte de la gestión, corresponde a las compañías de seguros adoptar nuevas metodologías para una adecuada estimación de dichas reservas, y de la misma forma, la regulación debe considerar nuevos modelos de estándares internacionales, así como sanas y modernas prácticas contables en materia de estimación y supervisión.

En ese sentido, dentro de la clasificación de los métodos para una adecuada estimación se puenden citar los siguientes:

1. **Métodos deterministas**, que establecen la estimación de reservas, a través de medidas de tendencia central.
2. **Métodos estadísticos**, que determinan la volatilidad y el error de predicción.
3. **Métodos estocásticos**, que estipulan una distribución predictiva a través de los márgenes de riesgo[2].

Para el caso de los métodos deterministas, se pueden mencionar los siguientes:

1. ***Chain Ladder***: asume que el patrón de liquidaciones (pagos o reservas) es estable en el tiempo, excepto por los posibles efectos aleatorios.
2. **Siniestralidad esperada**: es utilizado cuando no se cuenta con datos e información histórica para la realización del análisis.
3. ***Bornhuetter-ferguson***: consiste en una combinación de los métodos *chain ladder* y siniestralidad esperada[3].

En lo que respecta a los métodos estocásticos se puede mencionar el *Bootstrapping*, que consiste en un método utilizado para aproximar la distribución en el muestreo de un dato estadístico[4].

Finalmente, las estrategias de supervisión y regulación, así como las de gestión que realizan los propios aseguradores, deben considerar la implementación de modelos y metodologías de estimación de reservas técnicas, de acuerdo con las mejores prácticas que requieren una adecuada evaluación y medición de estas, a efecto de que las entidades aseguradoras las adapten a sus necesidades para presentar su información financiera apegada al nivel de riesgo que están asumiendo.

2, 3 y 4 Taller actuarial Regulación y Supervisión de Reservas – *Insurance and Actuarial Engineering - Prime Re Solutions* – noviembre 2020.

La importancia del gobierno corporativo en la actividad aseguradora durante una crisis

Jennifer Cristina Pérez Garrido

Inspector del Departamento de Normativa de la SIB

Licenciada en Ciencias Jurídicas y Sociales, Abogada y Notaria por la Universidad Rafael Landívar, con Maestría en Derechos Humanos de dicha casa de estudios, *Legum Magister* en Finanzas por la Universidad Francisco Marroquín y Máster en Seguros y Gerencia de Riesgos por la Universidad Pontificia de Salamanca. Posee experiencia en los ámbitos bancario, seguros, constitucional e inclusión financiera.

El concepto gobierno corporativo surgió internacionalmente en los años noventa derivado de las experiencias de las quiebras financieras provocadas por la toma de decisiones y asunción de riesgos por parte de los directivos de las empresas en exceso de sus facultades y atribuciones, con lo cual se demostró la necesidad de que estas cuenten con reglas claras para la toma de decisiones, una estructura y límites para la relación entre los accionistas, el consejo de administración, los gerentes y otros grupos de interés *(stakeholders),* así como la implementación de mecanismos, políticas y procedimientos dirigidos a la creación de valor, generación de confianza y al crecimiento de la entidad.

De tal cuenta, en el ámbito financiero, diversos reguladores internacionales han emitido normas para la administración de riesgos y el gobierno corporativo; y, por su parte, los entes emisores de estándares internacionales han publicado diversos instrumentos en dichas materias. En tal sentido, el gobierno corporativo se ha desarrollado y cobrado relevancia, recogiendo diversos elementos que confluyen en la gestión de las entidades, con la

finalidad de disminuir la probabilidad de que por decisiones inadecuadas de los directivos, las entidades puedan caer en crisis económicas como las ocurridas en el pasado; asimismo, provee un ambiente ordenado con límites de responsabilidades, constituyéndose en la piedra angular para la administración de riesgos que requiere además un sistema de control interno efectivo.

Las instituciones financieras juegan un papel muy importante en el desarrollo y la estabilidad económica de un país, por lo que, sus accionistas, miembros del consejo de administración y gerentes, deben contar con normas y políticas que regulen sus relaciones; así como adaptarse a las mejores prácticas de gobierno corporativo para la consecución de sus fines, la buena marcha de sus operaciones y una adecuada prestación de sus productos y servicios al público en un marco de estabilidad financiera.

La actividad aseguradora por su parte es esencial en el ciclo económico por proveer de liquidez y otros mecanismos de apoyo como respuesta a los siniestros ocurridos; no obstante, su función puede verse afectada por factores externos no previsibles, impactando en los límites de responsabilidad en cuanto a los contratos de seguros colocados, entre otros aspectos. De tal cuenta, las decisiones que adopten sus órganos de autoridad podrían repercutir directamente en sus riesgos, sobre todo el de suscripción.

La Junta Monetaria, mediante la resolución JM-3-2018, emitió el Reglamento de Gobierno Corporativo para Aseguradoras y Reaseguradoras, con fundamento en los artículos 28 y 29 de la Ley de la Actividad Aseguradora, y considerando el principio 7 de Gobierno Corporativo de los Principios Básicos de Seguros emitidos por la Asociación Internacional de Supervisores de

Seguros (IAIS, por sus siglas en inglés), el cual requiere que las aseguradoras establezcan e implementen un marco de gobierno corporativo que brinde una administración y supervisión de la actividad de la aseguradora, estable y prudente, que reconozca y proteja de manera adecuada los intereses de los asegurados. Asimismo, dicho reglamento regula los aspectos mínimos que deben observar las aseguradoras con relación a la adaptación de las mejores prácticas de gobierno corporativo, como un fundamento esencial de los procesos integrales de administración de riesgos, así como de un efectivo sistema de control interno.

Desde la perspectiva supervisora, el gobierno corporativo es un fundamento preponderante que contribuye a la buena marcha de las entidades financieras supervisadas, cuya evaluación constituye un elemento clave de la supervisión basada en riesgos. Por lo tanto, un gobierno corporativo deficiente puede propiciar la materialización de diversos riesgos y que las consecuencias sean mayores a las previstas, de hecho, una mala gobernanza es en muchos aspectos un riesgo adicional en sí mismo.

A través de la historia, la humanidad ha atravesado diversas crisis que han puesto a prueba sus capacidades de protección y reconstrucción a nivel social y económico. La reciente crisis derivada del virus SARS-CoV-2 (COVID-19) llevó a los líderes de los países y de organizaciones empresariales (entre estas, entidades financieras) a adoptar diversas acciones y establecer medidas de forma inmediata para procurar la continuidad de las múltiples actividades sociales y económicas, no obstante, las circunstancias adversas provocadas por la pandemia.

En lo que respecta a la actividad aseguradora, la crisis trajo consigo una disrupción en cuanto a la prestación de sus productos y servicios, así como la atención a los asegurados y al público llevando a las aseguradoras a operar en circunstancias anormales y extremas, requiriendo de sus órganos de autoridad la toma de decisiones y acciones urgentes e inmediatas para la optimización de sus recursos y otras medidas para la continuidad de sus operaciones y la adecuada atención de sus clientes.

Adicionalmente, el estrés operativo que esta situación conllevó en el cambio del concepto del trabajo, que mudó de ser presencial a distancia, debilitó algunos procesos y controles internos, requiriendo una nueva cultura organizacional y obligando a priorizar y a reconfigurar sustancialmente los negocios a la luz de la crisis. Para los consejos de administración, supuso un cambio en los patrones normales de reuniones e interacciones con la alta gerencia, presentando interrupciones y una comunicación deficiente de la información, así como la implementación de mecanismos confiables que permitieran acreditar de forma fidedigna las reuniones y las decisiones adoptadas.

Para las aseguradoras, el riesgo de suscripción constituye el riesgo fundamental en su administración de riesgos por ser el específico a su giro de negocio. En virtud del COVID-19, algunas aseguradoras ampliaron sus coberturas de vida y salud a sus asegurados con diagnóstico positivo a dicho virus, no obstante que esta condición no se encontrase incluida en sus contratos, para lo cual tuvieron que considerar sus políticas de suscripción y realizar las adecuaciones o ajustes necesarios para la adopción de tal decisión. Asimismo, las entidades implementaron nuevos modelos comerciales y de organización, dentro de los que resalta la atención de reclamos de forma remota mediante la implementación de otros mecanismos como la comunicación por medios electrónicos.

Para el órgano supervisor, el COVID-19 trajo consigo desafíos similares a los de las entidades supervisadas, ante los cuales se encuentran la adopción de diversas medidas para la continuidad de sus labores de supervisión, migrando de la supervisión presencial a la remota y a la implementación de mecanismos para la atención oportuna y recepción de la información en tiempo real; asimismo, el fortalecimiento de la comunicación eficaz con sus supervisados.

Ante la crisis, resalta el papel y la relevancia del Plan de Continuidad de Operaciones adecuado a la entidad y, derivado de las lecciones aprendidas por la crisis del COVID-19, actualmente, resulta necesaria su revisión y actualización mediante la incorporación de otros posibles riesgos y sucesos, así como hechos externos no previsibles que pudieran afectar a la organización a futuro. Es de enfatizar la necesidad de establecer las facultades y responsabilidades en un escenario de crisis.

Actualmente, es de considerar los retos que enfrenta el gobierno corporativo en cuanto a la transición de la crisis a la nueva normalidad, para lo cual será necesario el fortalecimiento del liderazgo de las personas que ostentan posiciones de decisión; asimismo, a nivel organizacional se deberá realizar el análisis de escenarios derivados de las crisis, analizar y proponer los posibles ajustes de las políticas, procedimientos y sistemas para la administración integral de sus riesgos conforme a la naturaleza, complejidad y volumen de sus operaciones, observando en todo caso la normativa aplicable.

Es de concluir que el gobierno corporativo es necesario en tiempos normales y más en momentos de crisis como la reciente provocada por el COVID-19, que no se puede considerar concluida y cuanto menos sus efectos, algunos que aún son desconocidos. Su importancia estriba en la implementación de prácticas sanas y eficientes, que deberán atender a las necesidades de los clientes y de la entidad, que tengan como finalidad la gestión efectiva de sus actividades que conlleven al fortalecimiento de los niveles de confianza en el mercado, la protección y trato equitativo de los intereses de los accionistas, asegurados y clientes en general, así como a la estabilidad del mercado asegurador.

La importancia de la gobernanza de datos

Wendy López García

Profesional miembro de la Comisión de Gobernanza de Datos (GOSIB)

Licenciada en Administración de Negocios e Informática por la Universidad Francisco Marroquín (UFM), con Maestría en Contaduría Pública y Auditoría Internacional por la Universidad Galileo, Certificaciones internacionales como Auditora de Sistemas CISA y COBIT *Foundations,* posee experiencia en la implementación y realización de auditorías de Tecnología de la Información.

Italo Esaú Chicas Mejía

Inspector del Área de Innovación y Desarrollo de la SIB, miembro de la Comisión de Gobernanza de Datos (GOSIB)

Contador Público y Auditor, egresado de la Universidad de San Carlos de Guatemala, con Maestría en Administración de Sistemas de Información y Bases de Datos por la Universidad Galileo. Con especialización en Auditoría de Sistemas de Información con Certificación CISA, emitida por *Information Systems Audit and Control Association* (ISACA, por sus siglas en inglés); Certificación en Ciberseguridad y Riesgo Operacional, NEMESIS, España. Actualmente, entre sus funciones está la coordinación de las actividades del *SIB InnovatioN HUB* de la Superintendencia de Bancos.

El gobierno de datos se define como el ejercicio de autoridad y control (planificación, seguimiento y ejecución) sobre la gestión de los datos como un activo[1], es decir un recurso controlado con el cual se espera soportar beneficios económicos futuros, mediante el ofrecimiento de nuevos servicios, incrementar la lealtad de los clientes,

1 DAMA DMBOOK, Guía del Conocimiento para la Gestión de Datos.

entre otros, por lo que el gobierno de datos inicia a partir de una iniciativa estratégica en la que se reconoce que los datos son un activo corporativo muy valioso que debe gestionarse dentro de un marco de referencia y evaluado bajo un modelo de madurez.

En ese sentido, cuando se determina que los datos son activos valiosos para una institución se empieza a enfrentar el desafío de analizar y almacenar de forma segura grandes volúmenes de datos con calidad, que permitan generar información, conocimiento y sabiduría para sustentar adecuadamente la analítica, decisiones inteligentes de negocio y, por ende, incrementar la productividad y los beneficios económicos; sin embargo, se deberá reconocer que la calidad de datos es un problema crítico que crea esa imperante necesidad de implementar y gestionar el gobierno de datos .

El gobierno de datos facilitará a la organización contar con capacidad para gestionar el conocimiento que se obtiene sobre su información y responder a preguntas como: ¿Qué sabemos sobre nuestra información?, ¿De dónde provienen esos datos?, ¿Están estos alineados con nuestras políticas? Por lo que es fundamental hablar de gestión de datos que a juicio de Gartner Inc. la empresa consultora y de investigación de las tecnologías de la información, indica: "*Las solicitudes de datos aumentan constantemente dentro de las organizaciones, que van desde solicitar un acceso más fácil y flexible a los datos, pasando por una mayor gobernanza de datos, hasta la esperanza de poder cuantificar el valor de los datos y venderlos*". Estas diferentes expectativas de los datos, en un panorama cada vez más complejo y distribuido, está cambiando la atención de las organizaciones sobre la manera en que gestionan los mismos.

Por otra parte, debemos referirnos a la gobernanza de datos, como un marco de referencia que consiste en organizar procesos, estándares, políticas, estructura organizacional y las tecnologías necesarias para gestionar y garantizar disponibilidad, usabilidad, integridad, coherencia, auditabilidad y la seguridad de los datos de manera efectiva. Dado que, el programa de gobierno de datos consiste en las interrelaciones de estrategia, estándares, políticas y comunicación con respecto a los datos, el mismo tiene una acción conjunta con su gestión, es decir que no podemos hablar de gobierno de datos sin considerar la gestión de estos.

En tal sentido, el gobierno de datos proporciona el marco de referencia para la gestión de datos, alineado con las prioridades de la organización y las partes interesadas, permitiendo a los distintos niveles ser parte activa y colaborar para gestionar los datos, identificar brechas y proponer acciones que impulsen la mejora continua para la consecución del objetivo de mantener la calidad de los datos.

Asimismo, el gobierno de datos no solo tiene como objetivo asegurar y supervisar la efectividad de la gestión de datos, sino también la creación de valor de ellos y la satisfacción de las necesidades de la organización, ya que estos en sí mismos son meramente el combustible a consumir para alcanzar el fin deseado, la mejora de la productividad y mantener el programa de calidad, entre otros. El uso de datos requiere que las actividades se ejecuten con disciplina por lo que para ello muchas organizaciones crean una estrategia de gestión de datos.

Es fundamental para la gestión de los datos asegurar que estos sean de alta calidad, para garantizar la satisfacción de los requerimientos y el cumplimiento de los objetivos de la empresa, en consecuencia, debemos trabajar en forma conjunta con los usuarios y dueños de esos datos para definir sus necesidades, incluyendo características que a su criterio producirán datos de alta calidad, ya que si no podemos confiar en estos entonces el esfuerzo para recopilar, almacenar, proteger es en vano.

Lo expuesto anteriormente hace necesaria la creación de una estrategia que marque el inicio y curso de acción, que permita obtener ventaja competitiva a partir de los datos y así cumplir con los objetivos estratégicos. La elaboración de la estrategia deberá responder ciertas interrogantes como:

¿Qué datos necesita la organización?, ¿Cómo se obtienen los datos?, ¿Cómo se gestionarán y asegurará su fiabilidad en el tiempo?, ¿Cómo se utilizarán?; entre otras, sin perjuicio, de que la estrategia de datos requerirá también de un plan para mantener y mejorar la calidad, la integridad, el acceso y la seguridad de los datos, mientras se mitigan los riesgos conocidos e implícitos.

El *DAMA-DMBOK*, Guía del Conocimiento para la Gestión de Datos, define las áreas de conocimiento y expone que dicha gestión implica un conjunto de funciones interdependientes, cada una con sus propias metas, actividades y responsabilidades, por lo que tener un marco de referencia ayuda para entender la gestión de datos de manera exhaustiva y ver las relaciones entre sus componentes ordenadamente en formato tabular, lo que permite la caracterización o asignación lógica de una serie de procesos.

Asimismo, el *DAMA-DMBOK* expone los marcos de referencia siguientes:

> El Modelo de Alineación Estratégica (Henderson y Venkatraman, 1999), abstrae los motivadores fundamentales para cualquier enfoque de la gestión de datos. En su centro está la relación entre datos e información.

> El Modelo de Información de Ámsterdam (AIM, por sus siglas en inglés), muestra las relaciones de alto nivel que influyen en cómo una organización gestiona los datos.

Cuando se elige un marco de referencia de gobierno de datos para su implementación se debe considerar que existe una gama de marcos de referencia, los cuales han sido elaborados por proveedores independientes y organizaciones sin ánimo de lucro que pueden servir de fuente de consulta y que podemos utilizar para fortalecer el proceso de implementación del modelo seleccionado.

Fuente: DAMA, diseño propio de autores.

Adicional a la elección de un marco de referencia, si una de nuestras prioridades es acelerar el trabajo para la implementación de un programa de calidad de datos, es necesario que se establezcan formalmente las prioridades, entre las que se deberá hacer una comunicación clara que convoque y facilite la participación de toda la organización, así como la identificación y capacitación desde el inicio de quienes deberían participar en decisiones y actividades relacionadas con la calidad, desarrollo y mantenimiento de estándares, políticas de calidad y cumplimiento de modelos de datos, en adición a que deben implementarse prácticas de seguridad.

La implementación de un gobierno de datos eficaz tiene como objetivo una operatividad eficiente al resolver problemas de integración de datos complejos; sin embargo, lograrlo no es una tarea fácil ya que conlleva superar retos como la calidad de datos, identificación de los activos de datos, obtención de un consenso sobre la política de custodia de los datos desde la corresponsabilidad, identificación de dueños o custodios de la información y sus usuarios en toda la organización.

Finalmente, en el desarrollo de la ruta crítica hacia un gobierno de datos implementado, que no solo tiene como objetivo asegurar y supervisar la efectividad de la gestión de datos, sino también, asegurar la satisfacción de los requerimientos del negocio y que los datos en sí mismos son los medios para agregar valor a la organización.

Impacto de las principales medidas temporales emitidas por la autoridad monetaria derivado de la pandemia COVID-19

Carlos Humberto Oliva Murcia

Supervisor del Departamento de Normativa de la SIB

Contador Público y Auditor, egresado de la Universidad de San Carlos de Guatemala, con Maestría en Finanzas por la Universidad Rafael Landívar. Cuenta con participaciones a nivel nacional e internacional en temas relacionados con supervisión, contabilidad bancaria y normas internacionales de información financiera. Ingresó a la Superintendencia de Bancos hace 30 años, habiendo desempeñado cargos de Inspector y Supervisor de Área. Actualmente, es el representante de la Superintendencia de Bancos ante el Comité de Normas Contables y Financieras del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO).

Luis Francisco Vallejo García

Inspector del Departamento de Supervisión de Riesgos Específicos de la SIB

Contador Público y Auditor por la Universidad de San Carlos de Guatemala y Máster en Contaduría Pública y Auditoría por la Universidad Galileo. Posee experiencia de más de 18 años en supervisión de riesgos bancarios y de almacenes generales de depósito; asimismo, ha contribuido en el desarrollo de herramientas de supervisión.

La rápida propagación del COVID-19 a nivel mundial conllevó a que las autoridades de diversos países, incluyendo a Guatemala, implementaran medidas sanitarias para su contención, así como disposiciones de carácter temporal en materia financiera, monetaria y fiscal orientadas a mitigar el impacto económico de dicha pandemia; asimismo, en el ámbito de la supervisión bancaria, los entes reguladores y varios organismos internacionales se pronunciaron sobre las acciones de respuesta ante el COVID-19.

Al respecto, el Fondo Monetario Internacional y el Banco Mundial manifestaron de manera conjunta que, dado el papel fundamental del sector bancario para mitigar el *shock* macroeconómico y financiero sin precedentes causado por la pandemia, se hacía necesario adoptar acciones regulatorias y de supervisión oportunas, dirigidas y bien diseñadas, aplicando la flexibilidad que cada marco regulatorio y contable permitiera; así como, fomentar una reestructuración razonable de los préstamos, para que

la crisis sanitaria no se convirtiera en un mediano plazo en una crisis financiera.

Por su parte, el Comité de Supervisión Bancaria de Basilea expresó su respaldo a las medidas regulatorias y de supervisión adoptadas en distintas jurisdicciones para mitigar el impacto de la referida pandemia en la estabilidad financiera, tendientes a impulsar el otorgamiento de préstamos bancarios a la economía real y facilitar la absorción de pérdidas de manera ordenada por parte de los bancos, reconociendo la posibilidad de que se adoptaran medidas adicionales en caso de ser necesario.

Medidas temporales emitidas durante el 2020

En este contexto, a continuación se describen las principales medidas regulatorias temporales emitidas por la Junta Monetaria y los resultados generales de su aplicación.

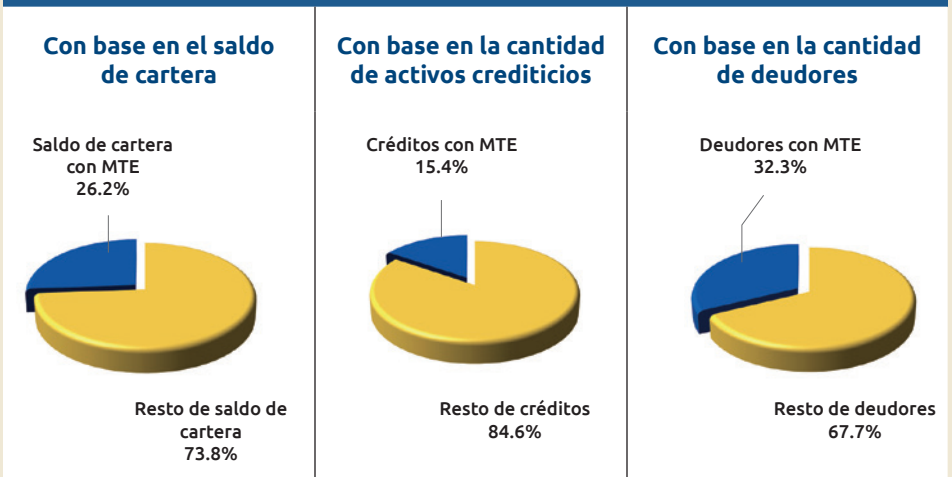
a) Medidas temporales especiales relacionadas con activos crediticios

Estas medidas (en adelante MTE) fueron emitidas por medio de Resolución JM-32-2020 de Junta Monetaria, la cual estuvo vigente hasta el 31 de diciembre de 2020. Las mismas, fueron aplicables a las instituciones supervisadas que otorgan financiamiento[1] (en adelante las entidades) y se enfocaron en los aspectos siguientes:

- Revisión de términos y condiciones en materia de tasas de interés y plazos, de los activos crediticios que al 29 de febrero de 2020 no presentaran mora mayor a un mes, pudiendo mantenerse en "Categoría A".
- Concesión de esperas o diferimientos de pago, dejando en suspenso el cómputo de la mora.
- Facultar para realizar modificaciones a solicitud simple de los deudores o por iniciativa de las propias entidades.
- Traslado contable de los créditos vigentes a vencidos a los 180 días calendario de atraso en el pago de por lo menos una de las cuotas de capital, intereses, comisiones u otros recargos, en vez de los 90 días que originalmente establece la normativa contable.
- Posibilidad de que las instituciones utilicen las reservas genéricas en calidad de reservas específicas.
- Facultar a las instituciones para la utilización del saldo de reservas para eventualidades que tuvieran como parte de su patrimonio, a efecto de hacerle frente al deterioro de los activos crediticios.

Al respecto, de conformidad con la información reportada por las entidades al 31 de diciembre de 2020, el 26.2% del saldo agregado de la cartera de créditos, que comprende el 15.4% de los activos crediticios y el 32.3% de los deudores, había sido beneficiado con la aplicación de una o más de las MTE descritas, según se aprecia a continuación.

INSTITUCIONES SUPERVISADAS QUE OTORGAN FINANCIAMIENTO
PROPORCIÓN DE CARTERA CREDITICIA BENEFICIADA CON MTE AL 31.12.2020



Saldo de cartera con MTE:	Q57,566.6 millones	Cantidad de créditos con MTE:	1,153,959	Cantidad de deudores con MTE:	585,003

Fuente: información enviada a la Superintendencia de Bancos por las entidades supervisadas que otorgan financiamiento.

La principal medida aplicada fue la concesión de esperas o diferimientos de pago, estipulada en el inciso b) del numeral 1 de la mencionada resolución, ya que el 97.5% de los activos crediticios con MTE se acogieron a dicho beneficio.

De acuerdo con la agrupación y la actividad económica de destino de los activos crediticios, la proporción del saldo de cartera con MTE en cada segmento fue la siguiente:

1 Incluye bancos, sociedades financieras, entidades fuera de plaza, empresas especializadas en emisión y/o administración de tarjetas de crédito y otras entidades que otorgan financiamiento.

INSTITUCIONES SUPERVISADAS QUE OTORGAN FINANCIAMIENTO
PROPORCIÓN DE CARTERA CREDITICIA BENEFICIADA CON MTE AL 31.12.2020
POR AGRUPACIÓN Y ACTIVIDAD ECONÓMICA DE DESTINO

AGRUPACIÓN	%*
Hipotecario para vivienda	43.4%
Empresariales menores	35.4%
Empresariales mayores	24.4%
Consumo	24.2%
Microcrédito	14.3%

ACTIVIDAD ECONÓMICA DE DESTINO	%*
Transporte y almacenamiento	46.6%
Construcción	38.3%
Establecimientos financieros, bienes inmuebles y servicios prestados a las empresas	30.4%
Servicios comunales, sociales y personales	28.0%
Consumo, transferencias y otros destinos	27.7%
Agricultura, ganadería, silvicultura, caza y pesca	24.5%
Comercio	24.1%
Industrias manufactureras	19.6%
Explotación de minas y canteras	14.0%
Electricidad, gas y agua	10.4%

* Porcentaje que representa la proporción del saldo de cartera beneficiado con MTE en cada segmento.

Fuente: información enviada a la Superintendencia de Bancos por las entidades supervisadas que otorgan financiamiento.

b) Cambio en el método de reconocimiento de ingresos

Una medida trascendental fue la modificación temporal del método para el reconocimiento de ingresos, la cual se reguló por medio de Resolución JM-37-2020, permitiendo a los bancos y sociedades financieras reconocer en los resultados del ejercicio 2020 los ingresos provenientes de intereses y otros productos devengados, aunque no necesariamente estuvieran percibidos. También se reguló que el registro contable de los referidos ingresos debía suspenderse cuando ocurriera un atraso de 180 días calendario, debiendo reconocerse como gasto los intereses y otros productos devengados que no se hubieran percibido durante dicho período.

De conformidad con información contable enviada a la Superintendencia de Bancos, varias entidades bancarias hicieron uso de esta medida temporal, estimándose que derivado de su aplicación, el importe registrado en los resultados al cierre del ejercicio mencionado por parte del sistema bancario en su conjunto equivale aproximadamente al 3.0% del resultado neto del ejercicio 2020.

Como se indica más adelante, en 2021 las entidades que aplicaron esta medida temporal deberán observar las disposiciones para el retorno al régimen contable de lo percibido, contenidas en la Resolución JM-149-2020 de Junta Monetaria.

c) Flexibilización en el cómputo del encaje bancario

Por medio de Resolución JM-55-2020 la Junta Monetaria emitió esta disposición de carácter temporal, considerando que se hacía necesario que el sistema bancario contara con reservas adicionales de recursos, a fin de atender la demanda de los mismos recursos que los hogares y empresas requirieran para hacer frente a la emergencia sanitaria.

La flexibilización estuvo vigente de mayo a octubre de 2020 y consistió en permitir a los bancos que, como parte de su encaje computable, incluyeran determinadas inversiones en títulos valores, hasta por un valor equivalente al 5.3% de su encaje requerido; asimismo, se incrementó el límite para computar los fondos en efectivo que las citadas entidades mantuvieran en sus cajas, de 25% a 50% del encaje requerido.

Al respecto, según la información reportada a la Superintendencia de Bancos, el promedio mensual de las inversiones incluidas por el sistema bancario en su conjunto como parte del encaje computable fue de 5.3% en moneda nacional y 5.2% en moneda extranjera; mientras que, para los saldos de caja, en promedio, lo incluido como parte del encaje computable no excedió el límite original de 25%.

Disposiciones transitorias para la finalización de las medidas temporales

El 9 de diciembre de 2020, la Junta Monetaria mediante resolución

JM-149-2020 promulgó las disposiciones transitorias por la finalización de las medidas temporales especiales emitidas para atender la coyuntura derivada de la pandemia COVID-19 de la forma siguiente:

a) Retorno al régimen contable de lo percibido

Esta medida transitoria aplica a los intereses y otros productos devengados no percibidos que, al 31 de diciembre de 2020, derivado de la medida temporal descrita en el inciso b) del apartado anterior, se encontraran registrados como ingresos en cuentas de resultados. Para el efecto, los ingresos cuya recuperación no se haga efectiva deberán reconocerse como gasto en el período 2021, conforme la gradualidad siguiente:

FECHA LÍMITE DE REGISTRO EN GASTO	INTERESES DEVENGADOS NO PERCIBIDOS AL 31.12.2020
31 de marzo de 2021	De 120 a 179 días de atraso en el pago
30 de junio de 2021	De 60 a 119 días de atraso en el pago
30 de septiembre de 2021	De 1 a 59 días de atraso en el pago

Cabe comentar que, a partir del 1 de enero de 2021 cobró vigencia nuevamente la normativa contable en toda su extensión, por lo que los intereses y otros ingresos generados a partir de la fecha indicada se deberán registrar bajo el método de lo percibido.

b) Reclasificación contable al inicio del ejercicio 2021 de los intereses y otros productos devengados no percibidos registrados como ingresos al 31 de diciembre de 2020

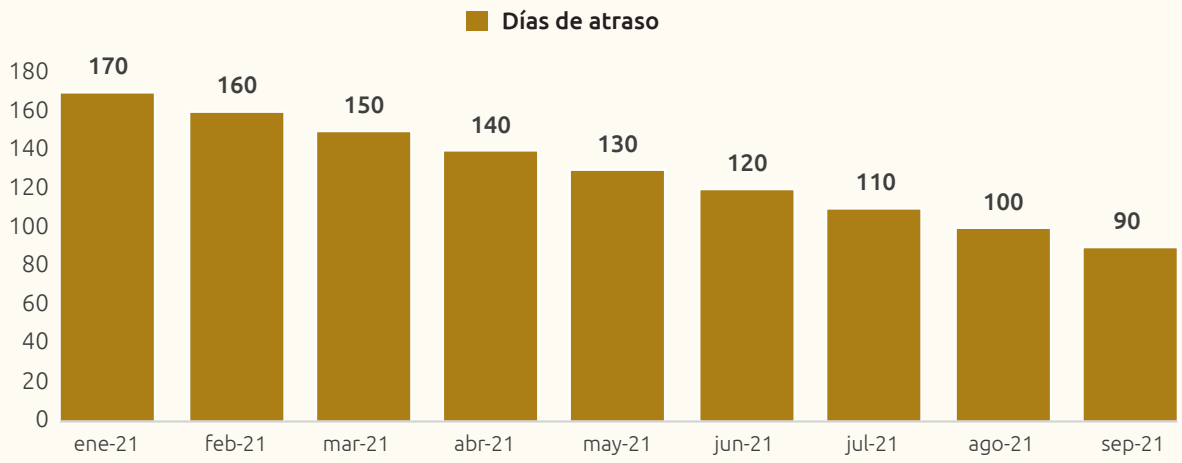
Esta disposición ordenó que en la partida de apertura del ejercicio 2021, se reclasificara el importe de los intereses y otros productos devengados no percibidos a que se hace referencia en la literal a), desde cuentas de capital (Ganancias del Ejercicio) hacia el rubro de otras cuentas acreedoras; lo anterior, con el objetivo de neutralizar el efecto favorable de dichos intereses y otros productos en el patrimonio computable de las entidades bancarias. El importe referido se regularizará conforme se produzca su recuperación, o bien, se efectúe su reconocimiento como gasto, según la gradualidad indicada en la literal a).

c) Traslado de créditos de vigentes a vencidos

Tal como se indicó, en la Resolución JM-32-2020 se permitió temporalmente a las entidades para que realizaran el traslado contable de los créditos vigentes a vencidos a los 180 días de atraso en el pago de por lo menos una de las cuotas de capital, intereses, comisiones u otros recargos, en vez de los 90 días estipulados originalmente por la normativa contable.

Esta disposición finalizó el 31 de diciembre de 2020, por lo que en el período contable 2021 cobra vigencia la disposición original; no obstante, para mitigar un impacto abrupto en enero de 2021, la Junta Monetaria estipuló en Resolución JM-149-2020 que el traslado contable de créditos de vigentes a vencidos se realice con la gradualidad que se ilustra a continuación.

GRADUALIDAD PARA EL TRASLADO DE CRÉDITOS VIGENTES A VENCIDOS



Fuente: elaboración propia de los autores, con base en lo estipulado en Resolución JM-149-2020.

IMPORTANCIA DE LA INICIATIVA DE LEY PARA LA PREVENCIÓN Y REPRESIÓN DEL LAVADO DE DINERO U OTROS ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO (LD/FT)

Principales beneficios de la iniciativa de ley

Manifiesta el compromiso del país a nivel internacional en la lucha contra el lavado de dinero u otros activos y del financiamiento del terrorismo.

Transforma y fortalece el Sistema Nacional contra LD/FT, adoptando un régimen preventivo con un enfoque basado en riesgos y debidamente diferenciado del régimen represivo.

Actualiza el marco legal apegado a los estándares y tratados internacionales de la materia.

Contribuye con el fortalecimiento de los esfuerzos globales y nacionales al combate del lavado de dinero u otros activos y del financiamiento del terrorismo.

INICIATIVA DE LEY 5820 IMPULSADA POR EL ORGANISMO EJECUTIVO.

PREVENIR Y COMBATIR EL LAVADO DE DINERO ES UN ESFUERZO DE PAÍS.

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

Superintendencia de Bancos
Guatemala, C. A.