



VISION[®]

Financiera

RETOS DE LA SUPERVISIÓN FINANCIERA ANTE LA TRANSFORMACIÓN **DIGITAL** DEL SISTEMA FINANCIERO

Pág.12



Revista de la Superintendencia de Bancos (SIB)
Guatemala, septiembre 2022
www.sib.gob.gt

Edición

Nº.45

Año 11

Cooperación y tecnología: la receta para el futuro de las finanzas / Pág. 04
Mantenerse competitivo en la era digital, el futuro de los bancos / Pág. 08
Transformación digital y la gestión de riesgos de seguros / Pág. 19



Superintendencia de Bancos
Guatemala, C. A.

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 Cabrera de Anzueto
Director Departamento de Desarrollo Institucional

Coordinador General

Lic. Hugo Rafael Oroxóm Mérida
Intendente de Coordinación Técnica

Director de Proyecto

Lic. José Ricardo Sánchez Segura
Supervisor Departamento de Desarrollo Institucional

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.

Superintendencia de Bancos

Oficina central

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

Oficina zona 13

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

info@sib.gob.gt

www.sib.gob.gt

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



Al correo electrónico:
comunicacion@sib.gob.gt



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

Contenido

04



Cooperación y tecnología: la receta para el futuro de las finanzas

08



Mantenerse competitivo en la era digital, el futuro de los bancos

12



TEMA CENTRAL

Retos de la supervisión financiera ante la transformación digital del sistema financiero

16



Principales aspectos relacionados con el nuevo Reglamento para la Administración del Riesgo de Crédito

19



Transformación digital y la gestión de riesgos de seguros

22



Gerencia de transformación digital: seis desafíos que enfrenta y cómo superarlos

25



Entidades financieras ciberresilientes: aspectos a considerar para su desarrollo



Promoviendo la
estabilidad y confianza
en el sistema financiero
supervisado.



Presentación

Apreciables lectores:

La edición 45 de la revista Visión Financiera se complace en presentar, gracias al valioso aporte de connotados profesionales y expertos, la importancia y retos de la transformación digital en la supervisión de los sistemas financieros; su relevancia actual en la competitividad y desarrollo de los mercados financieros; las perspectivas sobre el futuro de los medios de pago; y, la gestión adecuada de los riesgos que esa transformación trae consigo con el objeto de garantizar la ciberseguridad y continuidad de las organizaciones.

El tema central **Retos de la supervisión financiera ante la transformación digital del sistema financiero**, presentado por el licenciado Moisés Oswaldo Dardón Prado, Intendente de Supervisión de la Superintendencia de Bancos de Guatemala, trata sobre los desafíos de los entes supervisores, por un lado, para aprovechar las innovaciones digitales a fin de llevar a cabo con mayor eficiencia sus funciones y, por otro, para identificar y supervisar de forma

eficaz los riesgos emergentes a que están expuestas las entidades supervisadas que puedan afectar la estabilidad y confianza de los sistemas financieros.

En cuanto al desarrollo de la temática de la presente edición, es oportuno expresar un sincero agradecimiento por la participación de nuestros invitados especiales, que nos exponen sobre **Cooperación y tecnología: la receta para el futuro de las finanzas**, segmento desarrollado por el señor Ricardo Valentini Mola, Director de Pagos y Recaudos para Centro América y el Caribe, *Citi Treasury & Trade Solutions*, que trata especialmente sobre las tendencias en el uso de los medios de pago y su importancia en los mercados financieros. Por su parte, el licenciado Eric Campos Morgan, *Country Manager* y Gerente General de BAC-Credomatic, aborda el tema **Mantenerse competitivo en la era digital, el futuro de los bancos**, que resalta la importancia de que las organizaciones superen sus niveles de competitividad y eficiencia ante la era digital, destacando la evolución y futuro de la banca,

lo que ha permitido mejorar la experiencia de los clientes y usuarios.

Asimismo, es propicio agradecer los aportes de funcionarios de la Superintendencia de Bancos, que con diferentes tópicos relacionados con la transformación digital, exponen temas como **Gerencia de transformación digital: seis desafíos que enfrenta y cómo superarlos**, que recoge los retos y desafíos asumidos en la implementación de la transformación digital por parte de las organizaciones; **Transformación digital y la gestión de riesgos de seguros**, que desarrolla reflexiones importantes sobre el impacto y retos de las innovaciones digitales en el mercado asegurador; y, **Entidades financieras ciberresilientes: aspectos a considerar para su desarrollo**, dentro del cual se destaca el desafío que representa para las organizaciones, en especial para el sistema financiero, la adecuada gestión de la ciberseguridad a fin de preservar la continuidad del negocio ante los riesgos inherentes al uso intensivo de las tecnologías de la información.

Finalmente, pero no menos importante, en el ámbito de modernización y fortalecimiento de la regulación del sistema financiero, así como de las innovaciones en las tecnologías de la información y el aprovechamiento de la mayor disponibilidad de datos, se presenta el tema **Principales aspectos relacionados con el nuevo Reglamento para la Administración del Riesgo de Crédito** a cargo del licenciado Byron Vinicio Méndez Castillo, Intendente de Estudios y Normativa de este ente supervisor, que recoge aspectos introducidos recientemente a dicha reglamentación para robustecerla, tanto en el ámbito cualitativo como en el cuantitativo.

Esperamos que la presente edición sea de utilidad para el sistema financiero, usuarios, académicos y público en general, dada la importancia de los temas expuestos, para el desarrollo y modernización del sistema financiero guatemalteco.

Atentamente,

Lic. Erick Armando Vargas Sierra
Superintendente de Bancos



COOPERACIÓN Y TECNOLOGÍA: LA RECETA PARA EL FUTURO DE LAS FINANZAS

RICARDO VALENTINI MOLA

El acceso a servicios financieros, para las personas que hoy en día no lo tienen y por lo tanto no pueden desarrollarse, es un objetivo fundamental para nuestros países. En este sentido, muchas veces se abordan teorías en dirección de las soluciones tecnológicas, pero hay un punto en el que es necesario superar la fascinación por la tecnología per se y poner el foco en el usuario. ¿Quién es? ¿Qué necesita? ¿Cómo lo ayudamos? ¿Cómo lo cuidamos?

En este punto, la irrupción de las *Fintech* suma al desarrollo, porque desafía a la industria tradicional a ofrecer soluciones simples, intuitivas, claras y seguras.



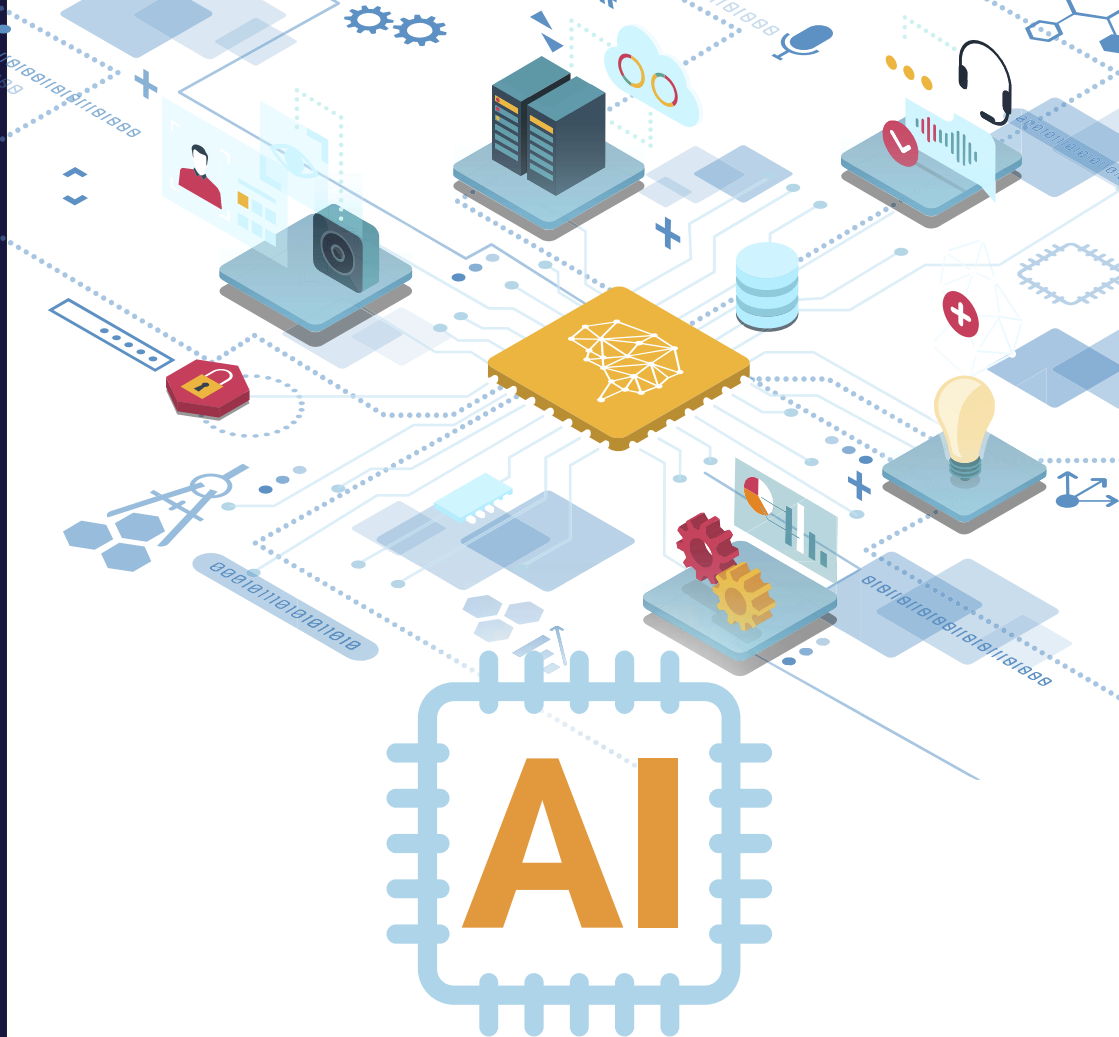
Lo importante es continuar pensando en el impacto en las personas. Y allí vuelven a abrirse las mismas preguntas sobre la importancia de la educación financiera y la responsabilidad que tenemos como industria sobre ello.

Si bien hay segmentos e instancias en las que competimos, entendemos que esa relación puede ser complementaria cuando hay objetivos alineados. Así, nosotros le damos el nombre de “fintegración”, eliminando la idea de un juego de suma cero. En la relación entre ambas industrias tenemos espacios de colaboración; también somos proveedores; en ocasiones, clientes y también, competidores. Esto es bueno porque nos desafía y nos lleva a ofrecer mejores soluciones.

Nosotros desde Citi ponemos a disposición soluciones para el beneficio de los clientes, con un gran foco en los aspectos de seguridad de la información y del acceso a los datos. Abrimos nuestras API (Interfaz de Programación de Aplicaciones) para el beneficio de nuestros clientes, con un control seguro de acceso a los datos. En total, Citi ofrece 54 API que cubren un amplio espectro de operaciones: consulta de saldo, transferencias de fondos, pagos, entre otros. Sirve en los 160 países en los que operamos y podemos hacer transferencias entre países por API en lugar de hacerlo por SWIFT (*Society for Worldwide Interbank Financial Telecommunication*). Estos servicios permiten a las tesorerías de nuestros clientes avanzar en la automatización de sus procesos.



Por otra parte, tenemos un ejemplo reciente: las soluciones digitales del banco permitieron a los clientes superar desafíos financieros planteados por la pandemia de COVID-19. Por ejemplo, la analítica de datos que permite automatizar las aprobaciones y la tramitación de las solicitudes de los clientes para aumentar sus líneas de crédito a través de la aplicación móvil y la banca digital.



Además, usamos herramientas de Inteligencia Artificial (IA) para ayudar a nuestros clientes a controlar sus pagos, completar la documentación administrativa, anticipar flujos, conciliación de las cuentas por cobrar y para impulsar la toma de decisiones en aspectos como precios, facturación, pasivos y depósitos, entre otros. La IA se considera cada vez más una ventaja competitiva en las finanzas, ya que los bancos buscan analizar datos estructurados y no estructurados, convirtiendo los datos brutos en inteligencia procesable para mejorar los ingresos, reducir las pérdidas y los costes.

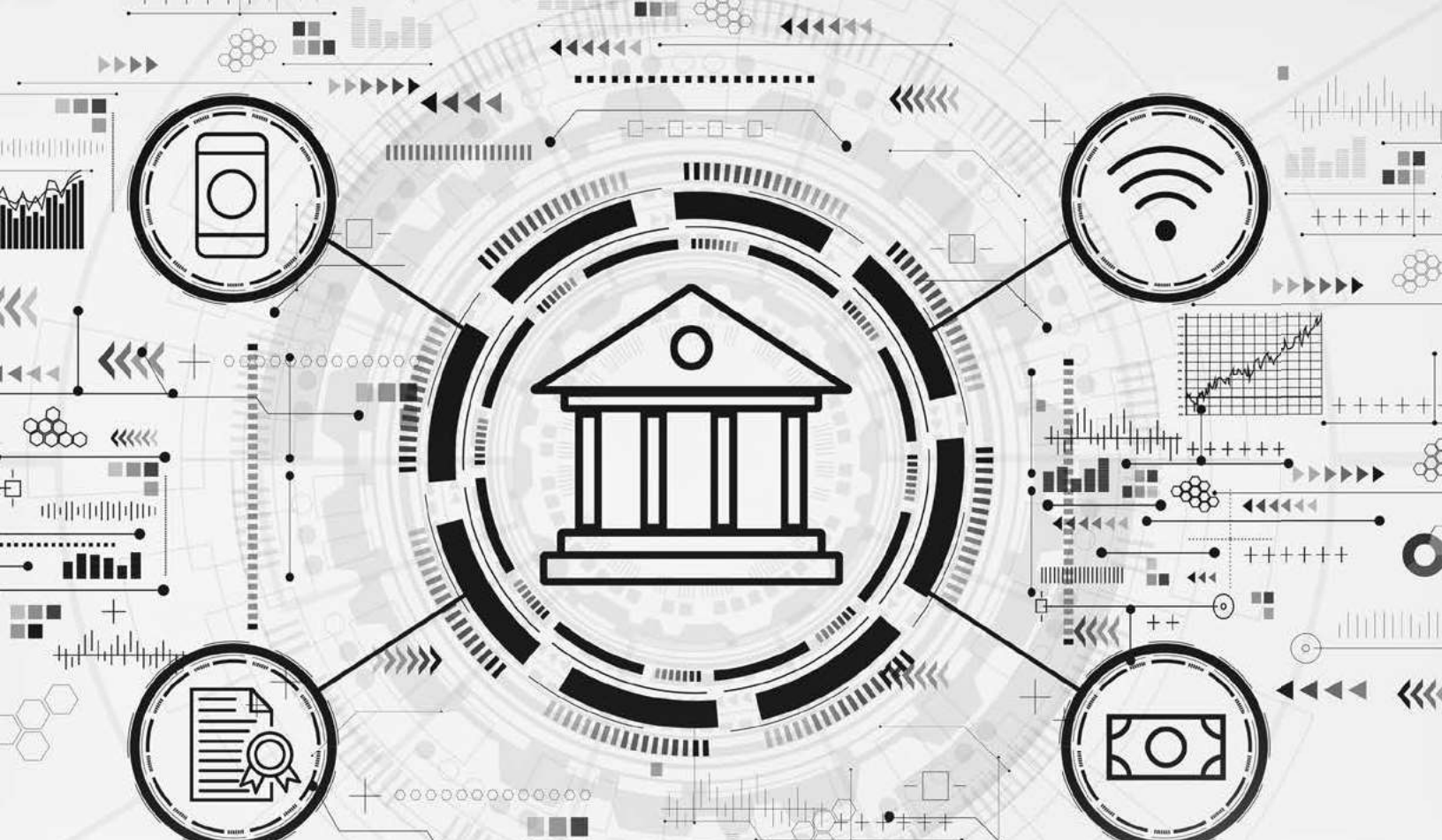
Estas aplicaciones ayudan a las instituciones financieras a aumentar el compromiso de los clientes al proporcionar información de datos sobre su comportamiento y sus hábitos, para ofrecer recomendaciones contextuales y personalizadas.



RICARDO VALENTINI MOLA

Director de Pagos y Recaudos para Centro América y el Caribe, *Citi Treasury & Trade Solutions*

Posee más de 25 años de experiencia en banca y tecnología. Ingresó a Citi Brasil en 1999 y ha ocupado diferentes posiciones como Gerente de Canales Electrónicos, Servicio al Cliente e Implementaciones. Ha trabajado como líder en productos para instituciones financieras como Santander y JP Morgan y DocuSign. En 2017, regresó a Citi para asumir como responsable del negocio de Pagos y Recaudos para Brasil, hasta ser designado en su actual cargo.



MANTENERSE COMPETITIVO EN LA ERA DIGITAL, EL FUTURO DE LOS BANCOS

ERIC CAMPOS MORGAN

La banca tiene una larga historia de adaptación y cambio desde su origen moderno en la Venecia del siglo XV, especialmente bajo los Médici, quienes dejaron grandes legados de su impacto en nuestro mundo moderno, por ejemplo la partida contable de doble entrada. Desde entonces, el concepto de banca se ha expandido de financiar las aventuras mercantes con África y el Lejano Oriente a convertirse en un indicador del nivel de desarrollo de una sociedad; a más profundidad e inclusión financiera, más desarrollo de un país o, dicho de otra manera, no hay países desarrollados sin instituciones financieras sólidas y mercados financieros profundos.

Actualmente, estos procesos de innovación financiera no se han detenido, al contrario, se han visto acelerados y potenciados por el desarrollo de las Tecnologías de Información y Comunicaciones (TIC), en un contexto acelerado de globalización universal, que abarca todos los países del planeta. Así pues, vemos como el salto de las TIC ha permitido acortar las distancias de desarrollo entre las naciones, saltando la necesidad de la cobertura telefónica analógica y pasar directamente a la celular, al acceso a internet y la conectividad permanente. Guatemala es un claro referente de ese éxito, que alcanza a más de un celular por guatemalteco, que supera ya los once millones de personas.

FEB 2022

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

GUATEMALA

Metric	Value	Comparison
TOTAL POPULATION	18.42 MILLION	URBANISATION 52.7%
CELLULAR MOBILE CONNECTIONS	20.26 MILLION	vs. POPULATION 110.0%
INTERNET USERS	11.97 MILLION	vs. POPULATION 65.0%
ACTIVE SOCIAL MEDIA USERS	9.55 MILLION	vs. POPULATION 51.9%

SOURCES: INTERNETACTIVELY, CELULARSIGNALS, GOVERNMENT'S DOCS, CENSA, INTELSAT, VEE, DATA FOR PEOPLE, CHINA, AFRICA, AND INNOVATION, COMPANY ADDRESSING RESOURCES AND PARTNERS' REPORTS, CEDIA, SCHLASS, KESPO, ANAGRAMAS, ADVISOR, LOCAL MEDIA, AND A VERY HOT LIST OF UNUSUAL PERSONS. **CONFIDABILITY:** SOURCE AND BASE CHANGES

we are social

KEPIOUS

1 <https://hbr.org/2015/12/what-is-disruptive-innovation>

La banca se enfrenta a un nuevo contexto de competencia de sus capacidades para agregar valor y ser relevantes en el diario vivir de sus públicos de interés, un contexto que abre nuevos flancos competitivos y, al mismo tiempo, nuevas oportunidades para ampliar los beneficios de la inclusión financiera. Por un lado, está el advenimiento de compañías fuera del mundo financiero, principalmente comerciales, como *Amazon* o *Apple*, que extienden sus servicios a los medios de pago y a las facilidades financieras, invadiendo el espacio típico reservado al sector financiero. Por ello, se pueden ver cada vez más soluciones comerciales compatibles con *Apple Pay* o *OneClik* de *Amazon*, así como nuevos jugadores como *PayPal*, fundado por el ahora famoso y reconocido *Elon Musk*.

La competencia que enfrenta la banca en un mundo hiperconectado por las TIC no excluye a Guatemala, donde hay más de 30 empresas *Fintech* agrupadas bajo la Asociación *Fintech* Guatemala². Emprendimientos que buscan emular muchas de las iniciativas realizadas no solo en los Estados Unidos de América y Europa, sino también en Latinoamérica, que registra un número sin precedentes en ideas asociadas a servicios financieros con aplicaciones tecnológicas o *Fintech*.



La posibilidad de conectar con los clientes en nuevas experiencias adicionales a la tradicional visita e interacción en una agencia bancaria, abre nuevas oportunidades de inclusión financiera, desde la extensión de los servicios bancarios en los corresponsales o agentes bancarios de barrio y pueblo hasta las facilidades cada vez más amplias de los servicios vía internet o celular. Estas han expandido la base de cobertura con costos accesibles, como las transferencias ACH (*Automated Clearing House network*), versus otros servicios de mayor costo, como la emisión de cheques. El canje y uso de cheques ha decrecido en favor de un crecimiento casi exponencial en el uso de transferencias ACH en tiempo real.

Asimismo, las posibilidades de acceso ágil a los servicios financieros se pueden ver beneficiados con procesos simplificados y digitales de generación de productos bancarios.

Muestra de ello ha sido el crecimiento en los bancos de Guatemala generando más opciones para la creación de cuentas bancarias desde el internet y, especialmente, desde el móvil. Hoy contamos con tecnología digital que nos permite utilizar mecanismos seguros de biometría en el celular para autenticación del cliente y así crear cuentas bancarias en tiempo real.

Estos logros de mayor oferta y competencia digital en originación de cuentas bancarias se han hecho gracias a los cambios regulatorios como el Formulario Electrónico de Información del Cliente (FEIC), impulsados desde la Superintendencia de Bancos en los últimos tiempos. Esta tendencia podría acelerarse aún más en ahorros transaccionales y tiempo para el cliente, en la medida que logremos avanzar como sistema financiero en regulación simplificada que permita acelerar gestiones, de forma segura y documentada digitalmente, la inclusión ágil de clientes al sistema, derribando barreras y paradigmas que empujan a la población a sistemas paralelos de acceso a alternativas financieras más caras, informales y muchas veces fuera de la ley. Lograr el desarrollo incorporando la informalidad en un desarrollo inclusivo digital.

El sistema financiero tiene la oportunidad gracias a las TIC, de contar con unos actores bancarios robustos y competitivos, así como una adecuada



2 <https://www.guatemalafintech.com/>

y moderna regulación, de reducir las barreras de ingreso de varios tipos de servicios, desde fiscales para la pequeña empresa, documentales y legales en muchos casos, para su ágil y sencilla incorporación al sistema bancario y por ende a la modernidad. Se ha mejorado en inclusión, pero según *Global Findex* del Banco Mundial³ al 2017 teníamos una penetración del 44% en cuentas bancarias, menor del 20%; en tarjetas de crédito, o débito, adicionalmente una tasa de crédito al producto interno bruto (PIB) menor del 40%, con una concentración del crédito al sector empresarial mayor y donde todavía el crecimiento del crédito al sector pyme o empresarial menor crece a tasas de un solo dígito.

Los riesgos asociados a la ciberseguridad es otro reto fundamental en este nuevo contexto competitivo digital. Estos se han trasladado de las cajas, ya sea por asaltos o desfalcos, en las agencias bancarias a los celulares de los clientes y los sistemas operativos de los bancos. Tenemos amenazas que empiezan con el ataque al cliente bancario con ingeniería social, sobre todo a los grupos de mayor riesgo, específicamente adultos mayores o personas de baja escolaridad, que son sujetos de fácil engaño por medio de diversos mecanismos en redes sociales para revelar credenciales seguras y, con ello, causar un daño económico a las personas y a las empresas, así como a la reputación del sistema. Estas amenazas se extienden directamente a los bancos, ya sea para introducirse a sus sistemas operativos o para el robo de data sensible, o bien, para lograr chantajes electrónicos, como el publicitado caso de la red de *Hackeo Conti* en el país vecino de Costa Rica.

³ <https://www.worldbank.org/en/publication/globalfindex/Data>



Los bancos y la regulación, tenemos al mismo tiempo la oportunidad de adaptarnos a estos nuevos requerimientos de seguridad con regulaciones ágiles y modernas; de igual forma, obtener tecnologías y metodologías de última generación para asegurarnos la debida protección de los activos de nuestros clientes, empezando por su data. Tenemos que aprovechar los modelos de defensa de múltiples capas, que nos den cobertura y mitiguen los riesgos asociados a las TIC, que incluyan los conocidos sistemas de encriptación, dobles factores de autenticación, *firewalls*, etc., todo esto sumado al monitoreo externo con empresas especializadas en lo que se conoce como el *white hacking* y, más importante, contar con el gobierno corporativo de la gestión integral de riesgos de ciberseguridad para cubrir desde el conocimiento interno a todo nivel, hasta talento y controles cruzados.

No menos importante en este nuevo contexto competitivo digital es la responsabilidad ampliada de los bancos con la sociedad y la gestión de riesgos ambientales y sociales contenidos en los principios Ambientales, Sociales y de Gobernanza (ASG), que deben incorporarse en la estrategia y gobierno corporativo de las organizaciones. En nuestro caso la ambición de ser un banco neto positivo nos ha llevado a un reenfoque de nuestras acciones y estrategias para reimaginar productos de triple valor positivo, económico, ambiental y social, que nos permita ofrecer mejores servicios digitales amigables con el planeta y de amplio alcance que facilite la inclusión financiera digital.

Guatemala tiene muchos retos, pero también muchas fortalezas, entre ellas y de importancia capital, un sistema financiero competitivo, sólido y en busca constante de mejora para el servicio del país en la nueva realidad digital del siglo XXI.

MODELO DE TRES LÍNEAS DE DEFENSA



LIC. ERIC CAMPOS MORGAN
Country Manager y Gerente General BAC Credomatic Guatemala

Master in Business Administration (MBA) por el Instituto Centroamericano de Administración de Empresas (INCAE) y Economista. Ingresó a BAC en 2000 ocupando desde entonces varias posiciones tales como *Chief Innovation Officer*, *Chief Banking Operation Officer* y desde 2017 lidera la operación de Guatemala.

RETOS DE LA SUPERVISIÓN FINANCIERA ANTE LA DIGITAL TRANSFORMACIÓN DEL SISTEMA FINANCIERO



MOISÉS OSWALDO DARDÓN PRADO

En virtud de la evolución de las tecnologías de información, las entidades financieras han incorporado innovaciones digitales en sus productos y servicios y en los procesos internos de operación, entre otros, con el objetivo de mejorar la experiencia de sus clientes, así como mantener o superar sus niveles de competitividad y eficiencia ante la llegada de nuevos competidores. Los órganos supervisores, no son ajenos a dicha evolución, por un lado, para aprovechar las innovaciones tecnológicas e incorporarlas en sus procesos de supervisión y, por otro, para identificar nuevos riesgos que puedan afectar la estabilidad y confianza de los sistemas financieros, como consecuencia de la transformación digital.



Importancia de la supervisión financiera

Dada la relevancia que tiene para la actividad económica en general, a lo largo de su historia contemporánea, el desarrollo de los sistemas financieros ha sido acompañado de regímenes de regulación y supervisión estatal, normalmente configurados a partir de la adopción de estándares y buenas prácticas a nivel global, con el objetivo de contribuir a la solidez y estabilidad de dichos sistemas.

En ese contexto, la supervisión financiera se materializa en la vigilancia e inspección que delegan los Estados en órganos de carácter técnico especializados, que procuran el buen funcionamiento de los sistemas financieros.

En el caso de Guatemala, la supervisión financiera se encuentra instituida en la Constitución Política de la República y desarrollada en la Ley de Supervisión Financiera, la cual contempla, entre otros aspectos, que esta corresponde a la Superintendencia de Bancos, órgano de Banca Central que actúa bajo la dirección general de la Junta Monetaria. Además de las funciones propias de supervisión, el ente supervisor participa en el proceso de regulación de las entidades supervisadas, en vista que, de conformidad con la ley, le corresponde proponer a la Junta Monetaria los reglamentos, disposiciones y demás normativa que esta deba dictar en materia de su competencia.

Transformación digital del sector financiero

De acuerdo con expertos especializados, la transformación digital se refiere a la capacidad de las organizaciones, sus líderes y empleados para adaptarse a la rapidez de los cambios provocados por la evolución de las tecnologías digitales¹.

Cada vez más las personas se relacionan a través de los medios digitales; de hecho, para las nuevas generaciones esta interacción constituye algo inherente a su vida y demandan soluciones ágiles y accesibles para facilitar sus quehaceres, incluyendo, pero no circunscrito a sus actividades de comercio y servicios financieros. De manera casi espontánea, este proceso de interacción con la tecnología fue acelerado durante la actual crisis sanitaria provocada por COVID-19, la cual demandó la prestación de servicios diligentes ante los cierres parciales o totales decretados por diversos países.

La industria financiera, además de aumentar el uso de las tecnologías de información, para responder a esa demanda creciente, ha tenido que reforzar sus estrategias de transformación digital, replanteando sus procesos operativos internos y modelos de negocio, a fin de mantenerse a la vanguardia y evitar ser desplazada por nuevos actores del mercado como las *Fintech*, *Insurtech*, *Big Tech*, etc., industrias crecientes que tienen la ventaja de estar diseñadas sobre tecnologías de la información.

¹ *The Technology Fallacy: How People are The Real Key to Digital Transformation*. Jerry Kane. Abril 2019.

Servicios financieros con mayor transformación digital

De acuerdo con el avance en el sector financiero global, particularmente la banca, estudios empíricos sobre la materia reflejan dos dimensiones de la transformación digital: los servicios financieros objeto de transformación y las tecnologías más utilizadas². Destaca entonces, entre los servicios financieros, los siguientes:

Pagos, compensación, liquidación

Créditos, depósitos
y captaciones de capital

Gestión patrimonial

Banca de inversión

Comunicación

Las tecnologías financieras predominantes incluyen *cloud computing*, Inteligencia Artificial (IA), aprendizaje automático, *big data*, interfaces de programación de aplicaciones (API, por sus siglas en inglés), *chatbots* y tecnología de contabilidad distribuida (DLT, por sus siglas en inglés), inmersos en los procesos de la banca y productos financieros.



² *Stay Competitive in the Digital Age: The Future of Banks*. Estelle Xue Liu. Fondo Monetario Internacional, Departamento Europeo. Febrero 2021.



Retos de la supervisión ante la transformación digital de los supervisados

Los desafíos de la innovación tecnológica se extienden a los órganos supervisores desde dos perspectivas: una al fortalecimiento de los marcos de supervisión para abordar los potenciales riesgos emergentes asociados a la transformación digital del sector financiero; y, la otra, a la incorporación de dicha innovación en los procesos y herramientas de supervisión, puesto que la experiencia internacional demuestra que hacen más eficiente la evaluación y monitoreo de los riesgos que asumen las entidades supervisadas (*Suptech*), además de facilitar a dichas entidades el cumplimiento regulatorio (*Regtech*).

Riesgos emergentes asociados a la transformación digital

La transformación digital del sector financiero aumenta la exposición de las entidades y usuarios, principalmente, a los riesgos operacionales y tecnológicos, ya que conlleva el incremento de fraudes electrónicos y de amenazas cibernéticas que exponen la integridad, disponibilidad y confidencialidad de los activos en el ciberespacio, así como la continuidad de la prestación de los servicios financieros; por tal motivo, dicha transformación demanda el fortalecimiento de la regulación y supervisión, especialmente, en materia de ciberseguridad.

Cabe destacar que, en el ámbito local, en 2020 y 2021, a propuesta de la Superintendencia de Bancos se incorporaron modificaciones al Reglamento para la Administración del Riesgo Tecnológico, orientadas a que las entidades supervisadas establecieran una estructura organizacional específica para la gestión de la ciberseguridad, implementando funciones y dependencias especializadas alineadas a las mejores prácticas internacionales, como el Oficial de Seguridad de la Información (CISO, por sus siglas en inglés), el Equipo de Respuesta ante Incidentes Cibernéticos (CSIRT, por sus siglas en inglés) y el Centro de Operaciones de Seguridad Cibernética (SOC, por sus siglas en inglés), con el objetivo de realizar un monitoreo continuo de los riesgos cibernéticos, contener y mitigar el impacto de estos, así como promover los procesos de recuperación y resiliencia ante los eventos e incidentes cibernéticos.

Innovaciones tecnológicas en los procesos de supervisión

La evolución de las tecnologías de información ha originado a nivel internacional, las tendencias denominadas: *Suptech*³, en referencia al uso de tecnologías innovadoras por parte de los entes supervisores para apoyar la supervisión, y *Regtech*⁴, relativo en general a la automatización de las funciones regulatorias y de cumplimiento.

Según la experiencia a nivel global, recopilada por el Instituto de Estabilidad Financiera (FSI, por sus siglas en inglés) del Banco de Pagos Internacionales (BIS, por sus siglas en inglés), las tecnologías *Suptech*, que se encuentran en diferente grado de desarrollo, abarcan principalmente los procesos de recopilación de datos y análisis de estos, sobresaliendo entre las áreas de avance hasta el momento⁵, las siguientes:

Obtención de la información directamente de los sistemas de las entidades supervisadas.

Validación y consolidación de datos.

Recopilación de información de usuarios y la atención a estos.

Análítica descriptiva y predictiva de datos.

Asimismo, si bien existen diferentes generaciones de dichas tecnologías, hay cierto consenso entre los expertos que analizan el tema, en cuanto a que el desafío de los supervisores se encuentra en la adopción de las referentes a *big data* e inteligencia artificial, las cuales hacen posible la gestión de datos en variedades y magnitudes que no pueden procesarse en aplicaciones comunes.

³ *The suptech generations*. Stefan Hohl, Jermy Prenio, Simone di Castri, Arend Kulenkampff. Instituto de Estabilidad Financiera, Banco de Pagos Internacionales, en colaboración con BFA's RegTech for Regulators Accelerator (R2A). 2019.

⁴ *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions - Market developments and financial stability implications*. Financial Stability Board (FSB). 2020.

⁵ *Innovative technology in financial supervision (suptech) - The experience of early users*. Dirk Broeders and Jermy Prenio. Instituto de Estabilidad Financiera, Banco de Pagos Internacionales. Julio 2018.

TECNOLOGÍAS QUE PUEDEN APLICARSE PARA UNA ARQUITECTURA DE **BIG DATA**

Tecnología	Proceso que cubre
Application programming interface (API)	Recopilación de datos
Robotic process automation (RPA)	Validación
Data lake	Gestión de datos no estructurados
Cloud computing	Procesamiento y almacenamiento
Distributed ledger technology (DLT)	Validación a través de diferentes ubicaciones
Tableros dinámicos (dashboards)	Visualización e interacción
Machine learning (ML), Natural language processing (NLP) Visual analytics	Análisis de datos

Fuente: *The suptech generations*. Instituto de Estabilidad Financiera, Banco de Pagos Internacionales, en colaboración con BFA's RegTech for Regulators Accelerator (R2A). 2019.

Las tecnologías descritas brindan velocidad a los datos, en cuanto al tiempo en que se generan, recopilan y convierten en informes y acciones; facilitan la validación consistente en la aplicación de criterios de calidad y aceptación de dichos datos; y, permiten el manejo de variedad de estos tanto estructurados como no estructurados (web, correos electrónicos, imágenes, redes sociales, entre otros).

Por su parte, la tendencia *Regtech*, que también se fundamenta en algunas de las tecnologías innovadoras descritas, es motivada por la complejidad y volumen de las regulaciones, así como por la necesidad de minimizar las consecuencias del incumplimiento.

En esta perspectiva de la innovación, es importante mencionar que, la Superintendencia de Bancos ha iniciado la ruta de transformación digital de sus procesos, implementando entre soluciones innovadoras, tres *chatbots* basados en inteligencia artificial, para atender a usuarios externos que consultan la página web, atender y dar soporte a Personas Obligadas ante la Intendencia de Verificación Especial (IVE), y brindar información de supervisión a

usuarios internos, respectivamente; una arquitectura de modelos de datos y *dashboards* para el análisis financiero y de riesgos; una infraestructura de *big data* para el análisis de patrones y tendencias de lavado de dinero, así como la incorporación de *machine learning* para optimizar el análisis de transacciones sospechosas; un sistema integrado para la gestión de las actividades del proceso de supervisión en ambiente automatizado; una plataforma para la comunicación virtual con los supervisados y Personas Obligadas, que incorpora el uso de documentos, notificaciones y firma electrónicos; un centro virtual de estudios y capacitación (*e-learning*); y, la consulta en línea del historial crediticio de los deudores. Asimismo, para asegurar que este proceso sea exitoso, el ente supervisor contempla en su plan estratégico proyectos en curso para implementar una gobernanza de datos apegada a estándares internacionales; desarrollar un marco de gestión de la ciberseguridad y ciberresiliencia institucional; y, promover la legislación y regulación de los modelos de negocio basados en tecnología.

No obstante, esto solo es el principio, puesto que la transformación digital será un proceso dinámico de incorporación permanente de nuevas tecnologías al proceso de supervisión financiera, con el objetivo de coadyubar a la estabilidad y confianza del sistema financiero supervisado.



LIC. MOISÉS OSWALDO DARDÓN PRADO
Intendente de Supervisión 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 de Guatemala. Cuenta con especializaciones internacionales en temas relacionados con Supervisión Basada en Riesgos, Supervisión Consolidada, Supervisión Transfronteriza, Estabilidad Financiera y Gestión de Riesgos Financieros. Ha desarrollado su carrera profesional en la Superintendencia de Bancos desde 1996, ocupando los cargos de Inspector Bancario, Supervisor, Asistente de la Intendencia de Supervisión y Director del Departamento de Supervisión de Riesgos Bancarios "A". Autor del libro *Historia del Sistema Financiero Guatemalteco (1821-2021)*.



PRINCIPALES ASPECTOS RELACIONADOS CON EL **NUEVO REGLAMENTO** PARA LA ADMINISTRACIÓN DEL RIESGO DE CRÉDITO

BYRON VINICIO MÉNDEZ CASTILLO

La Ley de Bancos y Grupos Financieros establece que, los bancos y las empresas del grupo financiero que otorguen financiamiento tienen la obligación de valorar sus activos, operaciones contingentes y otros instrumentos financieros que impliquen exposiciones a riesgos, de conformidad con la normativa que emita la Junta Monetaria, a propuesta de la Superintendencia de Bancos (SIB); así como que esa normativa debe contener el régimen de clasificación de activos y de reservas o provisiones, tomando en cuenta la capacidad de pago y cumplimiento del deudor.

En ese orden de ideas, la Junta Monetaria ha emitido la reglamentación específica relacionada con el riesgo de crédito; sin embargo, derivado de la evolución en la regulación en dicha materia a nivel internacional, de la emisión de nuevos estándares internacionales para mitigar y gestionar el referido riesgo y del desarrollo de las prácticas de gestión en el sistema financiero guatemalteco, se realizó una revisión integral de esa reglamentación, con el propósito de desarrollar una norma que permita avanzar a nuevos enfoques conforme lo requieren las mejores prácticas, lo que implicó que dicho cuerpo colegiado por medio de la resolución JM-47-2022 aprobara la emisión de un nuevo Reglamento para la Administración del Riesgo de Crédito que contempla, entre otros, los aspectos siguientes:

1 Incorporación de disposiciones para la administración del riesgo de crédito.

El nuevo reglamento incorpora temas concretos orientados a la administración del riesgo de crédito, como la obligación de establecer políticas, procedimientos y sistemas; responsabilidades y segregación de funciones para el Consejo de Administración, el Comité de Gestión de Riesgos y la Unidad de Administración de Riesgos; incorporación de pruebas de tensión; y, la elaboración del manual de administración del riesgo de crédito, todo ello congruente con la práctica internacional y los Principios Básicos para una Supervisión Bancaria Eficaz del Comité de Basilea (Principio 17 -Riesgo de Crédito-), permitiendo a su vez homologar esta normativa con la ya existente a nivel local asociada a la administración de otros riesgos.

2

Incorporación de disposiciones sobre financiamiento de proyectos nuevos.

Este tipo de financiamiento se define como el crédito empresarial o productivo, cuya fuente de pago está constituida por los ingresos que deriven de la realización, puesta en marcha o explotación de un proyecto.

En ese contexto, un proyecto se considera nuevo desde que inicia hasta que acumula información financiera suficiente que le permita a la institución bancaria efectuar una clasificación del activo crediticio con base en el criterio de capacidad de pago, conforme la normativa aplicable, o a partir del momento en que el deudor esté contractualmente obligado a efectuar pagos de capital.

En tal sentido, el financiamiento a proyectos nuevos requiere de un análisis de riesgo de crédito diferenciado de los créditos concedidos a empresas que cuentan con una trayectoria, en virtud que los mismos carecen de información financiera histórica.

3

Mejora en la agrupación de activos crediticios para su segmentación en función de su riesgo específico.

La segmentación de los activos crediticios permite identificar grupos homogéneos que reúnen características similares de concesión, destino y finalidad. Los bancos deben disponer de un proceso de calificación del riesgo de crédito para lo cual previamente necesitan agrupar las exposiciones crediticias con base en características de riesgo comunes, de tal manera que puedan valorar razonablemente las variaciones del riesgo de crédito y, por lo tanto, su impacto en la estimación de la pérdida esperada.

En virtud de lo expuesto, la nueva segmentación considera créditos empresariales; productivos (otorgados a personas individuales para actividades con fines lucrativos); hipotecarios de vivienda y cédulas hipotecarias; y, de consumo. A su vez, estos segmentos se dividen en subsegmentos para contar con mayor precisión en la estimación de sus probabilidades de incumplimiento.

4

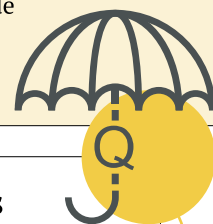
Incorporación de reservas o provisiones específicas conforme el cálculo de pérdidas esperadas por riesgo de crédito.

La pérdida esperada es el monto estimado de las pérdidas por riesgo de crédito que podrían producirse a consecuencia del incumplimiento de un deudor en un período determinado.

El Comité de Supervisión Bancaria de Basilea, principal órgano normativo mundial de regulación prudencial bancaria, a partir de la emisión del documento *Convergencia Internacional de Medidas y Normas de Capital*, conocido como *Basilea II* y emitido en junio de 2004, aprobó directrices para cuantificar el riesgo de crédito que los bancos asumen desde una perspectiva de requerimiento de capital, permitiendo a los bancos elegir entre dos amplias metodologías para calcular sus requerimientos de capital por riesgo de crédito. Una de ellas, la metodología basada en calificaciones internas que introduce el concepto de pérdidas esperadas, cuyo cómputo se fundamenta en la experiencia estadística y modelos matemáticos.

El nuevo reglamento contempla, que las instituciones deberán calcular las pérdidas esperadas mediante la multiplicación de los componentes siguientes: Probabilidad de Incumplimiento (PI), Pérdida Dado el Incumplimiento (PDI) y Exposición al Momento del Incumplimiento (EMI); además, establece los parámetros de esos componentes con el propósito de que los bancos constituyan provisiones específicas con base en dicho cálculo.

Lo indicado es congruente con lo establecido en las Normas Internacionales de Información Financiera (NIIF), específicamente la NIIF 9, la cual establece que, para el reconocimiento del deterioro de valor de un crédito, ya no es necesario que previamente ocurra un suceso relacionado con el crédito; en su lugar, una entidad contabilizará siempre las pérdidas esperadas, con el objeto de reconocer el deterioro de valor durante el tiempo de vida del activo crediticio.



5

Incorporación de reservas o provisiones dinámicas.

Las reservas o provisiones dinámicas buscan ser un soporte contracíclico ante eventos desfavorables en condiciones atípicas de las economías. Dichas reservas se constituyen sobre los activos crediticios de riesgo normal, en momentos de crecimiento del crédito, con el objetivo de contar con una reserva que permita mitigar el efecto de eventos adversos en la actividad económica y, por ende, en la solvencia y liquidez de los deudores de los bancos, en un período de tensión financiera.



6

Incorporación del requerimiento de información financiera auditada con base en la Norma Internacional de Auditoría 700 (NIA 700).

Este requerimiento está orientado para los solicitantes o deudores que tengan un endeudamiento total agregado a nivel del sistema mayor a Q20 millones o USD2.6 millones. El propósito es que los bancos cuenten con información de mejor calidad para su evaluación y seguimiento.



7

Alineación de activos crediticios a la categoría de mayor riesgo con base en la información del Sistema de Información de Riesgos Crediticios.

De acuerdo con la nueva reglamentación, este proceso forma parte de la valuación de activos crediticios y consiste en aplicar la categoría de mayor riesgo a los créditos del deudor en función del segmento que corresponda, para efecto del cálculo de las reservas o provisiones específicas, utilizando la información disponible en el Sistema de Información de Riesgos Crediticios.

Lo anterior, tiene como propósito realizar una valuación más precisa, al considerar el comportamiento de pago de un deudor en el sistema financiero en su conjunto y no solamente en la institución que lo está evaluando.



8

Características diferenciadas entre reestructuraciones y refinanciaciones.

La nueva regulación incorpora características específicas para las reestructuraciones y refinanciaciones, a efecto de darles tratamiento diferenciado en función de la esencia de la operación, buscando reflejar adecuadamente las modificaciones a los términos y condiciones del contrato de crédito que resultan tanto de dificultades en la capacidad de pago del deudor como de las que devienen de actualizaciones de las operaciones normales en los negocios y que no están asociadas a dichas dificultades.

Esto tiene como propósito que los bancos puedan hacer un mejor seguimiento de los créditos y, por consiguiente, constituir provisiones acordes al nivel de riesgo asumido.

9

Modificación en la periodicidad de las valuaciones por mora.

La vigente reglamentación establece una periodicidad trimestral para la valuación por mora de los activos crediticios por parte de las instituciones; sin embargo, la nueva normativa dispone que dicha periodicidad sea mensual, sustentado en el hecho de que los avances tecnológicos permiten a las instituciones realizar las valuaciones de sus activos crediticios con mayor frecuencia y registrar de manera oportuna las provisiones respectivas. Dicha modificación es consistente con lo que al respecto establece el Criterio 4 contenido en el Principio 18, *Activos dudosos, provisiones y reservas*, de los Principios Básicos para una Supervisión Bancaria Eficaz del Comité de Supervisión Bancaria de Basilea.

Finalmente, es importante resaltar que el nuevo Reglamento para la Administración del Riesgo de Crédito, cuya vigencia será a partir del 1 de enero de 2023, permitirá fortalecer la gestión del principal riesgo de los bancos, a efecto de contar con un sistema bancario más resiliente.

LIC. BYRON VINICIO MÉNDEZ CASTILLO

Intendente de Estudios y Normativa de la SIB



Contador Público y Auditor egresado de la Universidad de San Carlos de Guatemala, con Maestría en Administración Financiera por la Universidad Mariano Gálvez de Guatemala. Cuenta con especialización a nivel nacional e internacional en temas relacionados con gestión y supervisión de riesgos financieros, supervisión consolidada y transfronteriza, red de seguridad bancaria y estabilidad financiera. Ha desarrollado su carrera profesional en la Superintendencia de Bancos desde 1995, ocupando los cargos de Director del Departamento A de Supervisión de Riesgos Bancarios, Subdirector del Departamento de Análisis Macropudencial y Estándares de Supervisión, Asistente del Despacho Central, Supervisor de Área e Inspector en los departamentos de supervisión de riesgos bancarios. Ha representado a Guatemala en comités técnicos del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras (CCSBSO) y en grupos de trabajo de la Asociación de Supervisores Bancarios de las Américas (ASBA); además, ha participado en comisiones interinstitucionales conformadas para proponer reformas a la Ley de Bancos y Grupos Financieros y a la Ley Orgánica del Banco de Guatemala.



Transformación digital y la **gestión de riesgos** de **seguros**

MAYRA KARINA CHOJOLÁN PRILLWITZ

A medida que las sociedades avanzan e interactúan en sistemas digitales, es fácil recordar aquellas frases en las que se afirma que todo está en movimiento, todo cambia de una forma constante. El escenario, los modelos de negocio y los clientes cambian; e, indudablemente la tecnología impulsa la transformación digital y conlleva nuevas formas de relacionarse.

Esta realidad es atribuible también al sector financiero, al que ha llegado la transformación digital para reducir los procesos, convertirlos en *software*

y generar datos. Estos contribuyen a conocer los clientes y sus preferencias, crear productos en función de sus gustos, descubrir nuevas oportunidades, predecir tendencias, entre tantos beneficios que ha provocado la explosión de datos y dispositivos conectados; sin embargo, se requiere concientizar sobre la importancia del análisis de los datos y su protección para que redunde en rentabilidad y confianza de las entidades financieras.

En el negocio del seguro existen principios fundamentales que rigen intrínsecamente su funcionamiento. Uno de ellos es la buena fe, el cual se refiere a que el asegurador y el asegurado actúan con la mejor intención, sin ánimo de perjudicar a la contraparte o hacer cometer o permitir actos malintencionados o voluntarios que lleguen a causar daño. En este sentido, es importante considerar que la transformación digital abre la puerta a multitud de datos de los clientes, pero los principios fundamentales que rigen el seguro siguen vigentes, incluyendo la buena fe en el uso de la información de los asegurados.

El negocio del seguro sigue siendo la transferencia de riesgos; sin embargo, la forma en que se lleva a cabo aborda un panorama de riesgo cambiante en el que los modelos antiguos ya no funcionan.

El desafío de la innovación en la era digital no se trata de una renovación sutil de los negocios existentes, sino de una reconstrucción total. Para crear innovaciones digitales con impacto empresarial se requiere que, la mentalidad, la cultura, las formas de trabajar y los roles también cambien. Se necesita una visión transformadora y se requiere un compromiso a mayor escala; la transformación digital en las aseguradoras le permite combinar diferentes funciones, pero necesita que el gobierno corporativo se involucre y revise cómo interactúan el negocio y la Tecnología de la Información (TI). Sería muy difícil hacer transformación digital con el mismo tipo de liderazgo de TI que desarrolló el sistema heredado.

La gestión de riesgos de seguros y el gobierno corporativo tienen como objetivo que las aseguradoras cuenten con sistemas efectivos de gestión de riesgos, que incluyan estrategias, objetivos, principios y asignación de responsabilidades, políticas con una definición y categorización de los riesgos, además de los límites aceptables, definición de apetito al riesgo, herramientas y procesos adecuados que incluyan el desarrollo de planes de contingencia, así como las respectivas revisiones.

Los principios internacionales de solvencia indican que el régimen de supervisión debe establecer los requerimientos para la gestión de riesgos empresariales con propósitos de solvencia y requiere que las aseguradoras consideren todos los riesgos relevantes y materiales.

Dentro de estos riesgos está considerado el tecnológico, por lo que, a nivel internacional, los supervisores han realizado trabajos formativos para conocer las experiencias en diferentes países por medio de casos de estudio y descripción de las prácticas que se realizan, relacionadas con este riesgo para el sector asegurador¹.

La base del negocio de seguros es la confianza del asegurado...

Las aseguradoras enfrentan el riesgo tecnológico desde fuentes internas y externas, incluyendo terceros; en adición al evidente y necesario volumen de información de sus asegurados, que reúnen, procesan y almacenan; y, entre los que se puede identificar información personal y sensible, en un negocio que se basa en la

confianza y la buena fe.

De esta cuenta, las debilidades relativas a la seguridad se relacionan con una falta de visión general del panorama de TI, por ejemplo la falta de un inventario de *hardware* y *software* con licencia; y, controles inadecuados, que comprende usuarios con mayores privilegios que los garantizados por el sistema y la falta de reconocimiento cuando una cuenta ya no necesita ciertos privilegios del sistema.

Como se ha indicado, las aseguradoras recopilan y almacenan información personal de sus asegurados y, en algunos casos, información de terceros, como nombres, fechas de nacimiento, números de seguro social, direcciones de correo electrónico, números de identificación médica, y datos de empleo, como los ingresos. Esto, convierte a las aseguradoras

en un blanco apetecible como herramientas para la extorsión, el fraude y el robo de identidad.

En el caso de pólizas comerciales, por ejemplo, un ciberseguro, las aseguradoras pueden poseer información sobre los controles de seguridad de la red del titular de la póliza y otra información de resiliencia cibernética que podría ser valiosa para los piratas informáticos y otros delincuentes cibernéticos.

La base del negocio de seguros es la confianza del asegurado en que la información recopilada por las aseguradoras estará protegida y que las reclamaciones se pagarán de manera oportuna cuando corresponda. Si una aseguradora sufre una violación de datos y expone a sus asegurados a la pérdida de datos confidenciales, esa confianza puede ser quebrantada.





De igual manera, si una aseguradora sufriera un incidente de seguridad en sus sistemas, que le impida realizar pagos de reclamos a tiempo o interrumpe de otro modo sus operaciones, esa confianza también puede ser vulnerada.

Cuando se rompe la base fundamental del negocio, se abre la puerta al riesgo reputacional que podría extenderse en su conjunto y afectar negativamente la confianza de los asegurados, inversores, agencias de calificación y socios comerciales.

La gestión de riesgos de seguros, deberá incluir la evaluación del riesgo tecnológico, así como la debida observancia de los mitigadores y controles internos relacionados, en virtud que la información que almacenan los convierte en objetivos importantes de los ciberdelincuentes que buscan información que luego pueden utilizar para obtener ganancias mediante actividades delictivas. Además, porque las aseguradoras contribuyen significativamente al sector financiero mundial y las interrupciones de los sistemas de las aseguradoras debido a percances de ciberseguridad pueden tener implicaciones de largo alcance y afectar la confianza pública en estas entidades.

Debido a la creciente frecuencia y gravedad de incidentes de ciberseguridad en todas las entidades comerciales, es de suma importancia que las aseguradoras se preparen para la resiliencia cibernética, sin importar su tamaño, especialidad, domicilio o alcance geográfico. Las aseguradoras deben contar con una visión completa de la importancia de la seguridad cibernética y la gestión de riesgos para comprender la exposición al riesgo tecnológico.

En lo atinente a la supervisión, aun cuando no existen principios específicos que se refieran al riesgo tecnológico y la resiliencia cibernética, se espera que las aseguradoras puedan demostrar la efectividad de los sistemas y controles en el marco de su gobierno corporativo.

La gestión del riesgo operacional establece que el sistema de gestión de riesgos debe tener en cuenta todos los riesgos materiales relevantes y razonablemente previsibles, incluidos los riesgos actuales y emergentes, también describe los componentes típicos de un sistema de control interno eficaz, en el que se incluyen las funcionalidades críticas de TI.

Adicionalmente, al celebrar o revisar un acuerdo de subcontratación, el Consejo y la alta gerencia deben considerar cómo el perfil de riesgo y la continuidad del negocio de la aseguradora se verán afectados por la subcontratación. Esto puede aplicarse al gobierno corporativo, la gestión de riesgos y los controles internos del proveedor de servicios con respecto al riesgo tecnológico.

Finalmente, en el marco de la supervisión se requiere la implementación de un plan de continuidad de operaciones, incluyendo las operaciones de TI, que asegure la operatividad normal del negocio ante la ocurrencia de eventos adversos que puedan crear una interrupción o inestabilidad en sus operaciones.

La transformación digital ha puesto en evidencia los volúmenes de información confidencial, personal y comercial, que las aseguradoras recopilan, almacenan y administran; por lo que, el riesgo tecnológico representa un desafío creciente para el sector de seguros, mismo que están obligados a atender para mantener la confianza sobre la que se fundamenta el negocio del seguro.



LCDA. MAYRA KARINA CHOJOLÁN PRILLWITZ

Supervisor del Departamento de Supervisión de Seguros y Otros de la SIB

Contador Público y Auditor, egresada de la Universidad Francisco Marroquín, con Maestría en Contaduría Pública y Auditoría Internacional por la Universidad Galileo. Posee más de 20 años de experiencia en supervisar las operaciones de compañías de seguros; gestión de riesgos y gobierno corporativo para aseguradoras; y, requisitos mínimos de capital y solvencia para aseguradoras.



GERENCIA DE TRANSFORMACIÓN DIGITAL: SEIS DESAFÍOS QUE ENFRENTA Y CÓMO SUPERARLOS

GUSTAVO GABRIEL GODOY OSORIO

Actualmente, la humanidad está afrontando cambios significativos en su comportamiento, motivados en general por COVID-19, los efectos del cambio climático, los conflictos geopolíticos a nivel global y la creciente dependencia de la tecnología, entre otros.

Por ese dinamismo, las personas están demandando soluciones digitales ágiles, por lo cual las empresas, especialmente las del sector financiero, deben adaptarse al entorno teniendo claro cómo funciona su modelo de negocio y establecer en

qué medida dependen del uso de las tecnologías digitales, a fin de establecer en sus planes estratégicos una visión integral para implementar dichas tecnologías. Independientemente del grado de innovación en que se encuentre una organización, la alta gerencia debe tener presente que, al competir en un mercado económico para generar utilidades, la inclusión de las tecnologías de la era de la información es vital en su negocio en marcha.

Tecnologías de la era de la información.

Conjunto amplio de tecnologías independientes que, consideradas colectivamente, constituyen una red de información, la cual se compone de su infraestructura básica: computadoras, enlaces de comunicaciones y nodos de conmutación y del contenido de información que almacena y transporta dicha infraestructura. Banco Interamericano de Desarrollo (BID).

Relevancia de las tecnologías digitales

De acuerdo con el Banco Mundial, es importante aprovechar las tecnologías digitales que se han implementado en el mercado, así como las que se vayan desarrollando, a fin de coadyuvar a los rendimientos productivos de las organizaciones para garantizar el desarrollo digital constante de los países.

Dicho organismo, destaca que “las tecnologías digitales están a la vanguardia del desarrollo y brindan a los países una oportunidad única para acelerar el crecimiento económico y conectar a los ciudadanos con los servicios y el empleo”¹; así también, facilitan a las empresas y sector financiero contar con mayor rapidez y agilidad en las operaciones, siendo necesario prestar especial atención a la ciberseguridad dados los riesgos de ciberataques asociados a la tecnología que puedan derivar en pérdidas significativas o comprometer su negocio en marcha y por ende la reputación de las organizaciones.

Las tecnologías digitales contribuyen a la transformación y si estas se gestionan adecuadamente, facilitan el comercio; desarrollan agilidad en la prestación de servicios; ofrecen nuevas oportunidades de empleo; y, permiten contar con profesionales altamente calificados.

Gerencia de transformación digital

Para la gestión de la transformación digital, las organizaciones deben contar con profesionales con habilidades y diversas especialidades, puesto que esta función es un eslabón importante para alcanzar sus objetivos estratégicos.

Al respecto, la escuela de educación digital en Europa *Talent Garden* destaca que el papel del gerente de transformación digital es que sea “un gestor de transformación digital que adquiera una visión global de la empresa en su conjunto y de todos sus elementos y funciones (partes interesadas, dirección, empleados, clientes). Debe conocer el estado actual de la digitalización, así como las eventuales resistencias a las que se pueda enfrentar, considerando todo el ecosistema de la empresa”².

Desafíos para enfrentarse a una era digital

Los desafíos para la gerencia de transformación digital son retadores, los cuales es importante que sean enfrentados y superados de manera eficiente. A continuación, los seis desafíos más significativos:



Fuente: Sap Concur, publicación noticias destacadas el 30 de abril de 2021.

1 Banco Mundial (2022), Panorama general. Disponible en: <<https://www.bancomundial.org/es/topic/digitaldevelopment/overview>>

2 Talent Garden (2021), El papel del Gerente de Transformación digital. Disponible en: <<https://talentgarden.org/es/digital-transformation/the-role-of-the-digital-transformation-manager/>>

¿Cómo superar los desafíos que enfrenta la gerencia de transformación digital?

Una hoja de ruta, que permita estimar la generación de beneficios económicos a largo plazo, es fundamental para abordar los desafíos de la transformación digital, siendo ideal que esta cuente con los ejes siguientes:

1 Modularidad

Implementación de sistemas de información y gestión.

2 Escalabilidad

Adaptación a las condiciones del mercado sin que el producto o servicio pierda calidad.

3 Interoperabilidad

Integración e interconexión de información.

4 Enfoque de los programas (Best of breed):

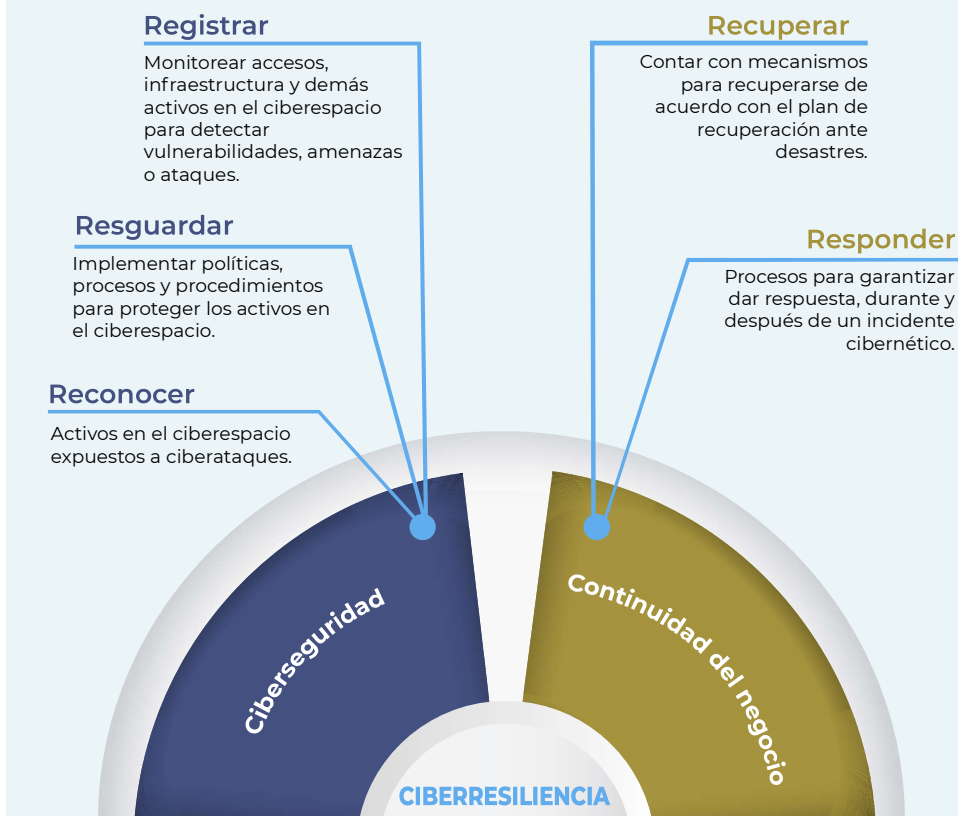
Flexibilización en las plataformas para incorporar funcionalidades y servicios desarrollados por terceros.

Además, para afrontar los riesgos operacionales y tecnológicos asociados a la transformación digital, las entidades financieras deben tener un plan de continuidad del negocio para: 1) identificar los eventos atribuibles a su modelo de negocio; 2) asignar roles y responsabilidades; 3) capacitar al personal clave; 4) efectuar pruebas que se consideren pertinentes; y, 5) conocer el plan de continuidad del negocio³.

Lo anterior debe estar alineado al plan de recuperación ante desastres para recuperar servicios tecnológicos críticos que se identifiquen en las principales líneas de negocio, activos en el ciberespacio e información relacionada a una interrupción⁴.



Es trascendental considerar, adicionalmente, la ciberresiliencia de las entidades financieras, la cual se logra implementando políticas y procedimientos, combinando la ciberseguridad con el proceso de continuidad del negocio.



Fuente: Comisión de Fortalecimiento de la Ciberseguridad Institucional de la Superintendencia de Bancos.



LIC. GUSTAVO GABRIEL GODOY OSORIO

Inspector del Departamento de Supervisión de Riesgos Específicos de la SIB

Contador Público y Auditor con Maestría en Contabilidad y Auditoría con Enfoque en Riesgos Internacionales por la Universidad Mariano Gálvez de Guatemala y Maestría en Gerencia de Sistemas de Información por la Universidad Rafael Landívar. Cuenta con las Certificaciones Internacionales en Economía Digital, ISO 27001 Foundations, Educación en Cambio Climático y Scrum Foundations. Ha desarrollado su carrera por más de diez años en la banca. Participa activamente en el Programa de Educación Financiera de la Superintendencia de Bancos. Es docente de pregrado y posgrado en las universidades Mariano Gálvez y Rafael Landívar.

³ Resolución de la Junta Monetaria JM-4-2016, Reglamento para la Administración del Riesgo Operacional.

⁴ Resolución de la Junta Monetaria JM-104-2021, Reglamento para la Administración del Riesgo Tecnológico.

The background is a dark blue gradient with various white and yellow icons. On the left, there's a large padlock icon. Above it, a Wi-Fi symbol. To the right, a globe with a classical building facade (columns and pediment) superimposed on it. Surrounding the globe are several circular icons: a downward arrow, a magnifying glass with a 'Q', a bar chart with an upward arrow, a document with a 'Q', a double-headed arrow, and a bar chart with a percentage sign. The main title is in large, bold, sans-serif font, with 'CIBERRESILIENTES:' in yellow and the rest in white and blue.

Entidades financieras **CIBERRESILIENTES:** ASPECTOS A CONSIDERAR PARA SU DESARROLLO

**PERCY FERNANDO MC NUTT MARIN
Y HUGO GERARDO CERVANTES GRAJEDA**

En la edición 43 de esta revista, enfocada al Plan Estratégico de la Superintendencia de Bancos 2022-2024, se mencionó que la Superintendencia de Bancos, en cumplimiento de su misión: *Promover la estabilidad y confianza en el sistema financiero supervisado* estableció, entre sus objetivos estratégicos, el promover la ciberresiliencia del ecosistema financiero, con el objeto de propiciar el desarrollo de capacidades digitales de protección, detección, respuesta y recuperación, ante una interrupción o incidente de ciberseguridad en el ecosistema financiero, impulsando la cooperación entre las partes, y en concordancia con las buenas prácticas y estándares de la industria dentro de un marco normativo adecuado. Adicionalmente, se indicó que, derivado de la aprobación por parte de la honorable Junta Monetaria, a través de la aprobación de las modificaciones al Reglamento para la Administración del Riesgo Tecnológico, según Resolución JM-104-2021, se propician en buena medida, el desarrollo de habilidades de ciberresiliencia en las instituciones sujetas al cumplimiento de este reglamento.

Este marco normativo encamina y direcciona a las entidades financieras hacia la ciberresiliencia, con requerimientos mínimos regulatorios; sin embargo, es un hecho que la adecuada gestión de tecnologías y estrategias de ciberseguridad de las entidades financieras es planificada y realizada por las propias entidades.

En esta oportunidad abordaremos aspectos importantes relacionados con la estrategia y controles que una organización o entidad financiera debe considerar en el proceso hacia la obtención de la ciberresiliencia.

Inicialmente, se debe establecer que una estrategia de ciberresiliencia está basada en varias actividades operativas que ya funcionan en las entidades financieras supervisadas, entre las que se pueden mencionar: continuidad de negocio, planes de recuperación de desastres, procesos y procedimientos de respuesta a incidentes cibernéticos, así como otros proyectos y soluciones tecnológicas de ciberseguridad. El reto es conjugar todas estas actividades operativas de manera tal, que se obtenga la colaboración entre las partes involucradas, planes de acción cumpliendo los plazos establecidos y la realización de ejercicios periódicos de respuesta a incidentes de ciberseguridad, para prevenir, detectar, responder y recuperarse de incidentes cibernéticos de alto impacto. Para lograrlo, resulta imperativo el involucramiento y apoyo de la alta dirección de las instituciones.

A continuación, algunas prácticas que se consideran esenciales para la obtención de la ciberresiliencia:



Protección de la identidad digital: la búsqueda de la ciberresiliencia no es función únicamente de los grupos de trabajo dedicados a la gestión de la tecnología de la información o de la ciberseguridad, es necesario

involucrar tanto a los usuarios internos como externos de la entidad, haciendo conciencia sobre el uso adecuado, la protección y resguardo de la identidad digital, fortaleciendo los controles de acceso y, entre otras buenas prácticas, el uso responsable de un segundo o tercer factor de autenticación que coadyuve en esta función y que permita distinguir al usuario con acceso autorizado y no autorizado; es importante, proteger nuestra identidad, de la misma forma como protegemos una escritura de propiedad o nuestro documento personal de identificación.



Protección al correo electrónico: el servicio de correo electrónico, se vuelve un punto de infección más común entre los atacantes, utilizando correos tipo

*phishing*¹ que cada vez son más sofisticados, realistas y con novedosas formas para engañar y motivar a su lector a que ejecute un *link* que rompa las capas de seguridad implementadas, por ello es importante que ante la menor duda de la legitimidad del mensaje y solicitud de alguna acción por esta vía, se confirme el remitente y se reporte el mensaje por el canal de comunicación que la entidad tenga destinado para este efecto.

¹ *Phishing:* técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza. <https://csrc.nist.gov/glossary/term/phishing>



Programas de concientización: en complemento a la protección contra ataques a través del correo electrónico u otro medio tecnológico, es de vital importancia el

establecimiento de un programa de concientización y un plan de comunicación adecuado, dirigido a los usuarios, a efecto de sensibilizarlos sobre la importancia de los ataques o incidentes cibernéticos, a fin de conseguir una cultura de ciberresiliencia en la entidad, consecuentemente a esta concientización se deben realizar ejercicios controlados de simulación de ataques tipo *phishing*, evaluando de forma periódica el comportamiento y la reacción de los usuarios identificando oportunidades de mejora y dando un seguimiento oportuno de las mismas.



Adecuada gestión de la infraestructura tecnológica: esta permitirá a la entidad

reaccionar de una manera oportuna y eficiente ante un ataque cibernético de impacto, que afecte la disponibilidad de los servicios tecnológicos. La adopción de buenas prácticas y marcos de referencia relacionados, aporta guías y da valor a dicha gestión.



Identificar capacidades: ante un evento el cual requiera recuperar información, la entidad debe prepararse reconociendo sus capacidades, esto

incluye recursos que necesita para iniciar el proceso de recuperación de dicha información, planes de respuesta a incidentes que describan y dimensionen los componentes tecnológicos, almacenamiento, recurso humano y autorizaciones necesarias para restablecerse rápidamente.



Plan de respuesta a incidentes:

en momentos de crisis, la improvisación es otro elemento que hace compleja la situación, por ello es importante

tener un plan de respuesta que permita a la entidad seguir las acciones consensuadas, que ayuden a recuperar o restablecer la disponibilidad, integridad y confidencialidad de la información y servicios en un menor tiempo. Un adecuado plan de respuesta a incidentes debe describir las actividades a realizar durante la preparación, detección y análisis de la situación, contención, erradicación, recuperación y, sobre todo, actividades posincidente.



Adecuados contratos con los proveedores de servicios: la dependencia de terceros, entidades externas y proveedores es común para

el funcionamiento de los servicios tecnológicos y, en ocasiones, para el resguardo y procesamiento de la información de las entidades. Tener un estricto control de esta dependencia es importante, tanto como incluir este aspecto dentro de la gestión de riesgos que realiza la entidad. En caso se requiera escalar un inconveniente a un proveedor o tercera parte, es importante conocer los acuerdos de servicio acordados y su vigencia; revalidarlos continuamente, con la finalidad que sean lo más adecuados a la realidad de la entidad y que cumplan los tiempos convenidos internamente para recuperar rápidamente la normalidad.



Identificar oportunidades de mejora: la ciberseguridad demanda fortalecer las capacidades de forma dinámica ya que los ataques y amenazas también lo son y evolucionan día con día. El ciclo de mejora debe reflejarse en la adecuada gestión de las herramientas de ciberseguridad, en fortalecer el conocimiento

a través de la concientización, adecuar y mejorar continuamente los planes de respuesta, promover la comunicación interna entre las áreas involucradas, identificar y mejorar las condiciones de los servicios contratados con terceras partes, así como una oportuna y clara comunicación a los altos mandos y autoridades de las entidades, a través de indicadores que reafirmen el involucramiento, apoyo y patrocinio necesario, orientando a la entidad de forma integral al desarrollo de las capacidades digitales de resiliencia digital o ciberresiliencia.

Referencias:

- ▶ NIST Cybersecurity Framework
- ▶ Revista Visión Financiera Nro. 43
- ▶ KnowB4



ING. PERCY FERNANDO MC NUTT MARIN

Profesional del Departamento Administrativo, Análisis Estratégico y Tecnología de la SIB

Ingeniero en Sistemas de Información y Ciencias de la Computación, egresado de la Universidad Mariano Gálvez de Guatemala. Es Magister Artium en Administración de Negocios, por la misma Universidad. Posee acreditaciones CISSP (*Certified Information Systems Security Professional*); fundamentos de COBIT 2019 (*Control Objectives for Information and Related Technology*); e, ITIL v4 (*Information Technology Infrastructure Library*); cuenta con más de 20 años de experiencia en la administración de servicios tecnológicos



LIC. HUGO GERARDO CERVANTES GRAJEDA

Profesional de Ciberseguridad y Seguridad de la Información de la SIB

Licenciado en Telecomunicaciones egresado de la Universidad Francisco Marroquín, con Maestría en Reingeniería y Tecnologías de Aseguramiento, así como Maestría en Informática Forense, ambos títulos otorgados por la Universidad Galileo. Cuenta con las certificaciones de Auditor Líder ISO 27001:2013 e ITIL. Posee experiencia en diseño y gestión de servicios tecnológicos e infraestructura, implementación de sistema de gestión basado en las normas ISO27001 e ISO20000, gestión de soluciones y servicios de ciberseguridad en el sector bancario e implementación de proyectos relacionados. Actualmente, es integrante de la oficina del Oficial de Ciberresiliencia Institucional en apoyo del desarrollo de las actividades estratégicas de ciberresiliencia orientadas al sector bancario y al fortalecimiento de capacidades internas.



NUEVO

Reglamento para la Administración del Riesgo de Crédito

Resolución JM-47-2022



Superintendencia de Bancos
Guatemala, C. A.

Con vigencia a partir del 1 de enero de 2023

RARC

EL NUEVO REGLAMENTO CONSIDERA,
PRINCIPALMENTE, LOS CAMBIOS SIGUIENTES:



LA NUEVA REGULACIÓN PERMITIRÁ FORTALECER LA GESTIÓN DEL PRINCIPAL RIESGO DE LOS BANCOS, A EFECTO DE CONTAR CON UN SISTEMA BANCARIO MÁS RESILIENTE