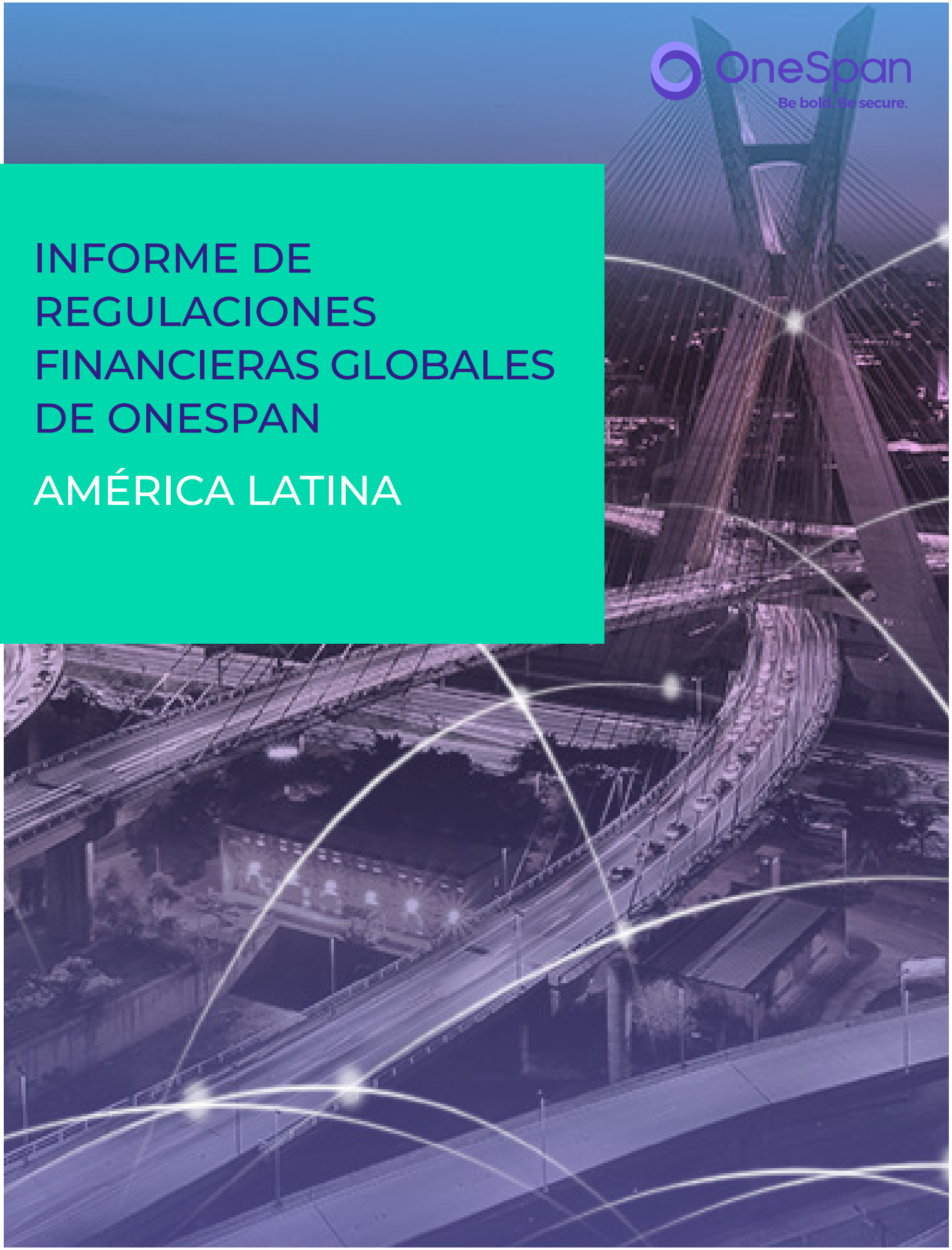


OneSpan
Be bold. Be secure.

INFORME DE REGULACIONES FINANCIERAS GLOBALES DE ONESPAN

AMÉRICA LATINA

Este es un extracto de nuestro Informe de Regulaciones Financieras Globales de OneSpan, el cual presenta regulaciones y leyes promulgadas principalmente en 2020 y que afectan al mercado latinoamericano y a sus compañías e instituciones financieras.

INTRODUCCIÓN

Las instituciones financieras de todo el mundo se enfrentan al desafío de cumplir con un contexto regulatorio que cambia constantemente, a la vez que utilizan las últimas tecnologías para equilibrar el cumplimiento con las normativas, la facilidad para el consumidor, la seguridad y los gastos.

La pandemia mundial del coronavirus ha hecho que 2020 sea un año histórico y ha obligado a casi todas las organizaciones del mundo a modificar su forma de hacer negocios. Por ejemplo, los reguladores de muchas jurisdicciones han adoptado la Guía de identidad digital del Grupo de acción financiera para permitir la incorporación remota de clientes y las firmas electrónicas. Esto a su vez ha impulsado a las instituciones financieras a adquirir e implementar estas tecnologías para continuar ofreciendo servicios a sus clientes mientras siguen cumpliendo con las pautas de distanciamiento social.

Hemos explorado en todo el mundo para identificar regulaciones, leyes y políticas recientes que afectan a los bancos y a otras instituciones financieras, específicamente en las áreas de privacidad, seguridad cibernética, antilavado de capitales, requisitos de «conocer a su cliente», identidad digital, autenticación y firmas electrónicas. Este informe no pretende ser un inventario de todas las regulaciones. Se enfoca en las normativas promulgadas durante 2019 y 2020, o que entrarán en vigor en 2021 y 2022.

Esperamos que sea un recurso valioso para usted y para su organización. Como este es nuestro informe regulatorio inaugural, agradecemos sus comentarios y sugerencias. Su aportación nos permitirá mejorar este trabajo para la edición de 2021. Puede enviarnos un correo electrónico a regulaciones@onespan.com.

Atentamente,

Firmado por Michael Magrath
el 2021-06-17 19:07:03 GMT

Michael Magrath
Director of Global Regulations and Standards

OneSpan

INFORME DE REGULACIONES FINANCIERAS GLOBALES DE ONESPAN

AMÉRICA LATINA

América Latina presenta un panorama digital desafiante pero fértil para los bancos e instituciones financieras que están buscando nuevas oportunidades para expandir sus esfuerzos de inclusión financiera y que quieren atraer a nuevos clientes con servicios de banca digital. El sector regional de tecnología financiera no ha hecho más que seguir creciendo a causa de la pandemia de COVID-19, debido a una mayor demanda de servicios financieros móviles por parte de los consumidores. Las aplicaciones de pago digital, que se usan generalmente para transacciones de remesas de consumidores de Estados Unidos, son cada vez más populares en los cinco mercados de tecnología financiera más grandes de América Latina: México, Colombia, Brasil, Chile y Argentina.

De hecho, algunos expertos presentan a América Latina como el mercado más atractivo de las tecnologías financieras (conocidas también como Fintech) debido en gran parte a una inversión y financiamiento continuos en el sector. Esta declaración que presenta a América Latina como una futura estrella de la banca abierta supone un contraste con un marco regulatorio bastante rezagado en cuanto a varios servicios electrónicos. Por ejemplo, muchos países de América Latina promueven el uso de firmas de tinta húmeda manuscritas en lugar de firmas digitales, y este es el método preferido por la mayoría de las compañías. Brasil, Costa Rica y Colombia son solo algunos de los países que específicamente no permiten que los documentos firmados electrónicamente sean notarizados.

Las autoridades reguladoras no han sido rápidas a la hora de ponerse al día con el progreso de los negocios regionales de tecnología financiera mediante la implementación de marcos legales para los servicios digitales, pero esto se debe en parte a la preferencia generalizada por el dinero en efectivo entre los consumidores que viven en áreas rurales y que trabajan en el sector agrícola. La mayoría de los países centroamericanos son principalmente agrícolas y, aunque los esfuerzos de inclusión financiera han tenido un éxito moderado, los bancos y las instituciones financieras aún no han aprovechado plenamente la preferencia de los consumidores por la familiaridad con respecto a las iniciativas de transformación digital. Con un número creciente de tecnologías financieras dedicadas a modernizar el sector financiero de América Latina, los bancos y las instituciones tradicionales, por ejemplo, las uniones de crédito, están optando por asociarse con nuevas entidades o presionando a los gobiernos nacionales para mantener a los proveedores de servicios financieros en las entidades ya establecidas.

BANCO CENTRAL

El Banco Central de Brasil (BCB) es el banco central del país, el cual es responsable de la política monetaria, además de ser la autoridad financiera nacional. Uno de los principales objetivos del banco es promover políticas de inclusión financiera en Brasil.

AUTORIDAD DE PROTECCIÓN DE DATOS

Para la fecha de publicación de este informe, la nueva autoridad de protección de datos de Brasil, oficialmente aprobada en agosto de 2020, no ha comenzado a llevar a cabo funciones legislativas ni regulatorias y hay varios puestos administrativos que aún no están cubiertos. Todavía no se ha anunciado el momento de inicio de operaciones de la autoridad de protección de datos.

BRAZIL

Resumen general del país

Brasil podría considerarse el centro de innovación financiera más emocionante de América Latina, y algunos expertos creen que el país está listo para emerger como un centro de innovación de servicios financieros de clase mundial. Brasil quedó categorizado como número 40 de 192 países en un informe de Índice de Preparación para la Inteligencia Artificial (IA) que fue publicado en 2019 por la compañía de investigación Oxford Insights, lo que indica que la economía de Brasil está lista para una transición hacia un futuro tecnológico. El país tiene la novena economía más grande del mundo y cuenta con casi 400 startups de tecnología financiera, porque se ha observado que los consumidores brasileños están entre los primeros a la hora de adoptar estas tecnologías en América del Sur.[1]

En enero de 2020, varias compañías francesas establecieron un centro de innovación en Brasil para apoyar a las nuevas compañías digitales y mejorar la eficiencia de las compañías digitales más grandes. Con tanto optimismo en torno a la innovación relacionada con las nuevas tecnologías y los servicios financieros, es fácil olvidar que los reguladores de servicios financieros de Brasil tienden a mantenerse muy atentos y no tienen problema para ejercer su autoridad de manera enérgica, no solo con respecto a las instituciones financieras tradicionales, sino también con respecto a las compañías de tecnología.

En junio de 2020, el Banco Central de Brasil suspendió los servicios de pago en la plataforma WhatsApp en respuesta a una protesta por parte de los bancos del país, quienes expresaron su preocupación por la competencia desleal en el mercado de sistemas de pago. El Banco Central rescindió esta suspensión solo un mes más tarde. Esto podría deberse al importante problema del uso de cuentas bancarias en Brasil: la mitad de la población del país no tiene una cuenta bancaria, "lo que corresponde a un volumen comercial de más de $170 millones (USD) por año".[2] Los brasileños valoran la conveniencia, y los bancos del país tienen un historial de servicios lentos, dificultades de acceso y lo que algunos ciudadanos llaman comisiones bancarias "abusivas".

Los reguladores de servicios financieros en Brasil tendrán mucho que hacer durante su transición al año 2021. Debido a la enfermedad de COVID-19, es evidente que los servicios financieros digitales, especialmente los que están operados por compañías que no son instituciones financieras tradicionales, seguirán aumentando en popularidad. Los reguladores tales como el Banco Central tendrán que equilibrar los intereses de los bancos del país con los de los ciudadanos que aún no hacen uso de los servicios financieros.

Otros asuntos financieros:

La **Comisión de Valores y Bolsa de Brasil (CVM)** es una agencia independiente que actúa como la autoridad de los mercados de capitales en el país. La Comisión regula todos los mercados de valores, incluidos los intermediarios financieros.

El **Consejo de Control de Actividades Financieras (COAF)** es la unidad nacional de inteligencia financiera de Brasil.

El **Ministerio de Economía**, que opera bajo la Oficina del Presidente, es la entidad principal responsable de la creación de políticas económicas y financieras del país.

Leyes y regulaciones

1. Circular número 3.978 de 2020: Políticas internas contra el lavado de dinero y el financiamiento del terrorismo para entidades supervisadas

   El 24 de enero de 2020, el Banco Central de Brasil publicó esta circular en el Diario Nacional. La circular modifica las normas con respecto a los procedimientos y políticas internos de prevención de lavado de dinero y financiamiento del terrorismo para entidades supervisadas, lo que incluye a bancos e instituciones financieras, y también reforma el marco nacional relacionado con este asunto para alinearlo con los estándares internacionales.

   Aspectos destacados clave para las instituciones financieras

   - **Procedimientos de diligencia debida relacionados con los clientes y con conocer a su cliente:** El capítulo cinco de la circular describe los procedimientos de «conocer a su cliente» (Know Your Customer, «KYC», por sus siglas en inglés) con respecto a la identificación del cliente y promueve un enfoque basado en el riesgo para la debida diligencia en este aspecto. Según el artículo 13 de la circular, las entidades supervisadas "deben implementar procedimientos cuyo fin sea conocer a sus clientes, incluidos procedimientos que aseguren la debida diligencia en cuanto a su identificación, calificación y clasificación". Además, los procedimientos KYC deben tener en cuenta "el perfil de riesgo del cliente, incluida la [implementación] de medidas reforzadas para clientes en categorías de mayor riesgo".
   - **Identificación del cliente utilizando datos existentes:** Según la Sección II de las disposiciones relacionadas con el requisito KYC de la circular, las entidades supervisadas "deben utilizar procedimientos de identificación que permitan verificar y validar la identidad del cliente". Se puede identificar a las personas físicas utilizando el Registro de Contribuyentes Individuales (CPF, por sus siglas en portugués), y en cuanto a las cuentas corporativas y comerciales, estas pueden ser identificadas a través del Registro Nacional de Personas Jurídicas. Para las personas físicas y los clientes comerciales en el extranjero, la circular describe un grupo de requisitos diferentes en cuanto a la identificación de los clientes.
   - **Personas físicas en el extranjero:** "En el caso de personas físicas residentes en el extranjero que no estén obligada a registrarse en el CPF, según lo define el Servicio Federal de Ingresos de Brasil, de acuerdo con la Ley, se permite el uso de un documento de viaje junto con al menos la información sobre el país emisor y el número y tipo de documento".
   - **Clientes corporativos en el extranjero:** "Las instituciones deben obtener, al menos, el nombre de la compañía, la dirección de la sede y la identificación de la compañía o el número de registro en el país de origen correspondiente".
   - **Elegibilidad del cliente:** La Sección III describe los requisitos de identidad para que un cliente sea elegible para ciertos servicios financieros. Establece que las entidades supervisadas "deben adoptar procedimientos para determinar la elegibilidad de sus clientes mediante la recopilación, verificación y validación de información, según el perfil de riesgo del cliente y la naturaleza de la relación comercial".

2. Decreto número 10.278 de 2020: Requisitos para la digitalización de documentos públicos y privados

   El 18 de marzo de 2020, el gobierno federal emitió este decreto, el cual establece requisitos para la digitalización de documentos públicos y privados. El decreto también describe las técnicas de implementación necesarias para la digitalización de documentos.

   Aspectos destacados clave para las instituciones financieras

   - **Certificación de infraestructura de clave pública para las entidades públicas:** Según el decreto, los documentos digitalizados deben obtener una certificación digital de acuerdo con los estándares de la Infraestructura de Clave Pública Brasileña (ICP-Brasil) "para garantizar la autoría de la digitalización y la integridad del documento y sus metadatos". Escaneo de documentos digitales entre individuos: En cuanto al intercambio de documentos entre particulares, el decreto establece que "será válido cualquier medio de acreditación de la autoría, integridad y, si corresponde, la confidencialidad de los documentos escaneados, siempre que tales medios sean escogidos de común acuerdo" por los particulares. Esto también se aplica si el documento es aceptado por el destinatario previsto.
   - **Responsabilidad de la digitalización:** Con respecto a quién es el responsable de escanear los documentos para su digitalización, el proceso "puede ser llevado a cabo por el titular del documento físico o por terceros". Sin embargo, el "titular" del documento físico es "responsable ante terceros" según las disposiciones del decreto.
   - **Mantenimiento y almacenamiento de documentos escaneados:** Los documentos digitalizados se pueden almacenar según el decreto. Este establece que almacenar documentos digitalizados debe protegerlos contra la "alteración, destrucción y, cuando sea aplicable, contra el acceso y reproducción no autorizados". Además, los documentos sin valor histórico deben conservarse "hasta que hayan vencido los plazos de limitación o los derechos a los que hacen referencia".

3. Decreto número 10.332 de 2020: Estrategia de gobierno digital - 2020 al 2022

   EEl 28 de abril de 2020, el gobierno federal emitió este decreto, el cual instituye la Estrategia de Gobierno Digital de Brasil para los años 2020 a 2022. El decreto tiene como objetivo digitalizar y modernizar los servicios, unificar los canales digitales y mejorar la interoperabilidad de los sistemas en todo el sector público del país. El Comité de Gobernanza Digital, que fue establecido en virtud de un decreto anterior (Decreto número 9 759 de 2019),

desarrollará una Estrategia de Gobierno Digital con el fin de modernizar los servicios. La Estrategia de Gobierno Digital cumplirá con las disposiciones de la Estrategia Brasileña de Transformación Digital (E-Digital), la cual establece el marco para las iniciativas gubernamentales en cuanto a la modernización digital.

4. Circular número 4.015 de 2020

   Normas para la banca abierta: El 4 de mayo de 2020, el Banco Central de Brasil aprobó esta nueva circular, la cual regula el alcance de los datos y servicios dentro del sistema abierto del país. La circular enumera los productos y servicios elegibles, así como de la Resolución Conjunta número 1, la cual incluye: depósitos a la vista prepagos, cuentas de ahorro y pago, cuentas de pago pospago, operaciones de crédito, préstamos y financiación inmobiliaria.

5. Resolución Conjunta número 1 de 2020

   Regulación para la banca abierta: Esta resolución conjunta fue aprobada por el Banco Central de Brasil (CBC) y el Consejo Monetario Nacional el 4 de mayo de 2020. La resolución establece regulaciones de implementación para la banca abierta en el país y permite el intercambio de datos personales entre instituciones financieras, así como la integración de los sistemas API de las instituciones financieras existentes.

   La iniciativa de banca abierta del CBC tiene como objetivo fomentar la innovación, promover la competitividad y aumentar la eficiencia y la transparencia en el sistema de pagos nacional.

   Aspectos destacados clave para las instituciones financieras

   - **Consentimiento del consumidor:** Las instituciones financieras y otras entidades que recopilan datos personales ahora pueden compartir datos de registro para fines relacionados con el consentimiento del consumidor. Sin embargo, hay ciertos tipos de datos de registro que están exentos de esta regla, los cuales incluyen: datos personales confidenciales, puntajes o calificaciones crediticias y credenciales de autenticación, así como otros usos de información para autenticar la identidad del cliente.
   - **Requisitos para compartir datos personales:** El capítulo cuatro de la resolución describe los requisitos necesarios para compartir datos de transacciones y de incorporación al registrar clientes para sistemas API de banca abierta. Las solicitudes están divididas en tres etapas: consentimiento, autenticación y confirmación. Las tres etapas deben llevarse a cabo "exclusivamente a través de canales electrónicos", y tanto la identificación del cliente como su consentimiento deben ser obtenidos antes de que se puedan compartir los datos personales, de acuerdo con la Sección 1.

     El consentimiento del consumidor solo puede obtenerse a través de ciertos medios y, según lo dispuesto en la Sección II, está prohibido que las instituciones financieras y otras entidades obtengan el consentimiento de un consumidor de las siguientes maneras: a través de un acuerdo estándar de cliente, de un formulario con el campo de acuerdo completado por adelantado, o basándose únicamente en la presunción sin ningún intento de establecer la "voluntad" del cliente.
   - **Autenticación del cliente:** La Sección III de las regulaciones establece que la autenticación del cliente se puede realizar "solo una vez por cada consentimiento válido"; pero en el caso de la autenticación de una institución receptora de datos o un proveedor de servicios de inicio de pago, la autenticación del cliente debe realizarse "una vez por cada llamada de interfaz". La regulación requiere un enfoque basado en el riesgo para los procedimientos y controles relacionados con la autenticación de clientes.

     La última etapa de la autenticación de clientes es la confirmación del intercambio de datos por parte del cliente. Según la Sección IV, se requiere que la confirmación del cliente "ocurra simultáneamente con los procedimientos de autenticación" descritos en las secciones anteriores.

6. Instrucción de CVM 626

   El 1 de junio de 2020 entraron oficialmente en vigor las reglas emitidas por la Comisión de Valores y Bolsa de Brasil (CVM) el 15 de mayo de 2020 y relacionadas con un entorno de pruebas (sandbox) regulatorio cuyo objetivo es mejorar los productos y servicios en el mercado. En resumen, esta Instrucción tiene como objetivo apoyar la innovación con respecto a las criptomonedas en un nuevo entorno de pruebas regulatorio, clarificando la seguridad jurídica en torno a las autorizaciones de pruebas en el mercado de valores. El propósito del sandbox en sí, tal y como se establece en la Instrucción, es promover la innovación en el mercado de capitales, orientar a los participantes en cuanto a asuntos regulatorios durante el desarrollo de actividades, reducir los costos y el tiempo de maduración del desarrollo de productos y servicios, aumentar la visibilidad y alcance de modelos comerciales innovadores y aumentar la competición entre los proveedores de servicios financieros en el mercado de valores.

7. Ley General de Protección de Datos (LGPD)

   La Ley General de Protección de Datos (LGPD) nacional del gobierno de Brasil entró en vigor el 15 de agosto de 2020, después de una serie de retrasos y de ser anulada por el Senado brasileño. La ley se publicó por primera vez el 15 de agosto de 2018. Al principio se esperaba que las entidades bajo el alcance de la ley la cumplieran con ella antes del 1 de agosto de 2021. Sin embargo, a finales de agosto de 2020, el Senado anuló otra decisión de la cámara baja, haciendo que la ley tuviera que cumplirse de inmediato. Las únicas

disposiciones que no se harán cumplir hasta 2021 están relacionadas con la aplicación de sanciones, lo cual les da a las instituciones un poco de tiempo para prepararse. El alcance de la LGPD incluye a las entidades que operan en Brasil, así como a entidades que operan fuera de Brasil, pero brindan servicios a los residentes del país.

Aspectos destacados clave para las instituciones financieras

- **Derecho del consumidor a solicitar información sobre datos personales:** Según la ley, las partes interesadas tienen derecho a solicitar a los controladores de datos una "copia electrónica completa" de sus datos personales, lo que incluye a las instituciones financieras. Además, los consumidores tienen derecho a hacer solicitudes con respecto a cómo se procesan y utilizan sus datos personales.

  La nueva LGPD consolida varias disposiciones de protección de datos que antes estaban distribuidas en varias leyes, incluida la Ley de Internet de Brasil, y la ley también está alineada con el RGPD. De hecho, la LGPD proporciona más derechos de portabilidad de datos que el RGPD para las partes interesadas, como el derecho a solicitar acceso a información sobre terceros de compañías que han compartido información con ellos, así como el derecho a acceder a información sobre la ubicación de los datos personales en organizaciones específicas.

- **Exenciones a la LGPD:** La ley no se aplica de manera absoluta, y hay varias exenciones relacionadas con transacciones que provengan de fuera de la jurisdicción brasileña. En general, la LGPD se aplica a las entidades, incluidas las instituciones financieras, si la entidad en cuestión realiza alguna de las siguientes actividades:

  1. lleva a cabo procesamiento de datos personales en Brasil;

  2. procesa datos personales recopilados en Brasil, o

  3. procesa datos personales con el fin de proporcionar productos o servicios en Brasil.

8. Decreto número 10.474 de 2020: La estructura reguladora de la Autoridad de Protección de Datos (ANPD):

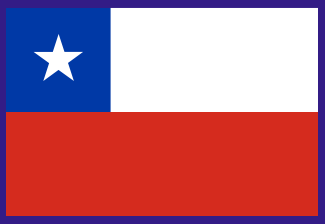
   Em 27 de agosto de 2020, o Gabinete Executivo do Governo Brasileiro publicou este decreto, aprovando a estrutura regimental da nova autoridade de proteção de dados do país (ANPD). O decreto descreve as responsabilidades e funções da ANPD, como a moderação de consultas públicas e a análise e emissão de regulamentações e normas. Um Conselho Diretor atuará como legislador responsável pelo desenvolvimento de normas e diretrizes relacionadas à governança e à proteção de dados.

Políticas y Legislación

1. Proyecto de Ley No. 5051/2019: El uso de la inteligencia artificial en Brasil

   El 16 de septiembre de 2019, el Senado brasileño presentó un proyecto de ley que describe pautas y principios para el uso de inteligencia artificial dentro del sector público brasileño. Uno de los principios básicos que se establece en el proyecto de ley es la protección de la privacidad y los datos personales.

   Más tarde, el 12 de diciembre de 2019, el Ministerio de Ciencia, Tecnología, Información y Comunicaciones (MCTIC) comenzó una consulta pública que concluyó el 2 de marzo de 2020. Gran parte de los comentarios de las partes interesadas estaban relacionados con preocupaciones sobre la competencia desleal, tanto por parte de las compañías emergentes como por parte de las grandes compañías comenzando en el mercado de servicios financieros, así como con el efecto del uso de la inteligencia artificial para la privacidad de los clientes. El proyecto de ley ha sido remitido a la Comisión de Ciencia, Tecnología, Innovación, Comunicación e Informática (CCT) para comentarios públicos. En el momento de publicación de este reporte, no se ha programado todavía una audiencia pública.



BANCO CENTRAL

Además de ser el banco principal de Chile, el **Banco Central de Chile (BCCh)** es también la principal autoridad monetaria y responsable de la creación de políticas financieras. El banco funciona de manera independiente y separada de las autoridades nacionales, tal y como lo establece la Constitución nacional.

Otros asuntos financieros:

La **Comisión del Mercado Financiero (CMF)** es la entidad principal reguladora del mercado de capitales y de seguros del país y se asocia con el Ministerio de Finanzas para formular legislación además de actuar como intermediarios de seguros.

AUTORIDAD DE PROTECCIÓN DE DATOS

Para la fecha publicación de este reporte, Chile no ha establecido una autoridad nacional dedicada a la protección de datos. Sin embargo, el Consejo para la Transparencia del país, por mandato de la Ley 20.285/2008, monitorea el cumplimiento de las normas de transparencia y divulgación de información.

El Consejo también protege los derechos de acceso a la información pública.

La Instituto Nacional de Normalización (INN) es una organización sin fines de lucro creada por la agencia gubernamental Corporación de Desarrollo Productivo para desarrollar estándares técnicos.

CHILE

Resumen general del país

Cuando la pandemia de COVID-19 llegó por primera vez a América Latina a principios del 2020, Chile ya estaba enfrentándose a los efectos del malestar social y de la depreciación de la economía nacional. Con las tensiones políticas en el país alcanzando niveles más altos que nunca y una creciente tasa de desempleo (un 8% en el momento en el que se escribió este artículo), los bancos del país ahora están lidiando con predicciones negativas para 2021 por parte de los inversores. Sin embargo, se prevé que la economía del país se mantenga relativamente intacta una vez que la pandemia vaya desapareciendo, y los bancos están encontrando formas de ayudar a sus clientes a adaptarse mediante medidas como la reestructuración de deudas y la reducción de las tasas de interés. El dinero en efectivo sigue siendo el método de pago más popular en Chile, porque, en general, las personas mayores de 45 años en el país todavía prefieren pagar en efectivo en lugar de hacerlo con tarjeta. Sin embargo, las tarjetas de débito han comenzado a ser más populares la última década y se prevé que los niveles de uso aumenten aún más como consecuencia de la pandemia de COVID-19.

Los bancos de Chile se enfrentan a un nuevo desafío en el floreciente sector de tecnología financiera del país. Chile está clasificado como el tercer centro de fintech en América Latina, después de Brasil y México.[3] Se espera que FinteChile, el grupo fintech más grande del país, crezca de 75 compañías miembro a 200 para finales del año 2020.

Las compañías de fintech han ganado terreno en varios mercados financieros a los que históricamente no se ha prestado mucha atención, específicamente en el segmento de las compañías pequeñas.

El gobierno de Chile ha dejado que el sector de servicios financieros se autorregule en gran medida. Sin embargo, el Congreso ha visto el potencial de los servicios fintech para impulsar la economía del país y en 2019 anunció planes para presentar un "proyecto de ley fintech" dedicado a regular el mercado. Ahora en 2020, los bancos, las compañías fintech, los clientes y los inversores esperan con gran expectación que el nuevo proyecto de ley se presente de forma oficial en el Congreso.

Leyes y regulaciones

1. Ley 21.236: Normativa sobre la Portabilidad Financiera

   El 9 de junio de 2020, el Congreso chileno aprobó las normativas que rigen los derechos de portabilidad financiera para clientes y para entidades legales que actúen en nombre de clientes. La ley tiene como objetivo acelerar los servicios bancarios para los clientes que quieran transferir información sobre cuentas de una institución financiera a otra. Oficialmente, la ley entró en vigor el 8 de septiembre de 2020.

   Se requería que los Ministerios de Economía y Finanzas publicaran disposiciones aclaratorias relacionadas con la Ley 21.236 en un plazo de no más de 45 días desde su entrada en vigor. A la fecha de publicación de este reporte, ninguno de los dos ministerios ha publicado disposiciones aclaratorias aún.

   Aspectos destacados clave para las instituciones financieras

   - **Sustitución de Partes Responsables:** La ley establece que la portabilidad de datos de la información financiera puede ocurrir de dos maneras: con o sin subrogación. En casos sin subrogación, un cliente desea dar por concluidos sus contratos de servicios financieros existentes con un proveedor y comenzar un nuevo contrato de servicio con un proveedor diferente. Cuando hay subrogación, el cliente contrata a un nuevo proveedor de crédito para liquidar un crédito con su proveedor inicial.

- **Responsabilidad de verificación de identidad:** La ley establece que, en cualquier caso de portabilidad de datos, es responsabilidad del nuevo proveedor "verificar la identidad y capacidad jurídica del cliente que acepta la oferta y otorga el referido mandato".
- **Verificación de identidad para el registro:** Cuando las nuevas entidades registren una solicitud de portabilidad de datos en casos de subrogación, "bastará la presentación del contrato del nuevo crédito y el respectivo comprobante de pago emitido de conformidad a las condiciones, plazos y formalidades que señale el Reglamento".

  Sin embargo, la ley establece que las entidades también podrán "solicitar los documentos que la entidad responsable estime necesarios para acreditar la representación, capacidad o identificación de la persona que solicite inscribir la constancia". El nuevo proveedor debe solicitar esta información al proveedor inicial en un plazo de 30 días desde la subrogación del crédito.
- **Requisito de firma electrónica:** El artículo 32 de la ley modifica las cláusulas existentes en el Decreto Ley No. 3.475, que a su vez es una modificación de la Ley de Sellos en el Decreto Ley No. 617. La cláusula que aborda las solicitudes de firma de constancias establece que "la solicitud de constancia se puede realizar en persona o de forma digital, debiendo emitirse, de manera digital o física, según sea solicitado, dentro de los tres días hábiles siguientes a la fecha de solicitud respectiva. En caso de que se solicite que el certificado sea emitido virtualmente, deberá ser emitido con firma electrónica de acuerdo con la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma". Una solicitud de firma de certificado es un mensaje cifrado enviado desde una entidad supervisada a la autoridad encargada del registro de certificado público (PKI, por sus siglas en inglés) solicitando la solicitud de un certificado de identidad digital.

  Además, en casos en que la solicitud de portabilidad incluya el compromiso del cliente de no incrementar las deudas correspondientes por encima de cierto monto, "ambas partes deberán firmar los contratos incluidos en la oferta, actualizados de conformidad a un nuevo certificado de liquidación o la actualización de deudas correspondientes... los contratos de apertura de línea de crédito o de productos que tengan líneas de crédito asociadas deberán estar disponibles para firma, a más tardar al día siguiente hábil bancario desde la entrega actualizada de la información de deuda del cliente por parte del proveedor inicial". Estas condiciones contractuales pueden cumplirse a través de firma electrónica conforme a la ley.

2. Ley 21.234: Limita la responsabilidad de los titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude

   El 29 de mayo de 2020, el Congreso de Chile aprobó una ley que limita la responsabilidad de los titulares de tarjetas de pago y usuarios de transacciones electrónicas que son víctimas de extravíos, hurtos, robos o fraudes (incluido el robo de identidad y el fraude de identificación), imponiendo nuevos requisitos para los emisores de tarjetas de pago y transacciones electrónicas. La ley entró en vigor ese mismo día. La responsabilidad de proteger la información de los clientes y usuarios recae claramente en los emisores de tarjetas de pago, incluidas las instituciones financieras.

   Aspectos destacados clave para las instituciones financieras

   - **Identificadores para avisos de extravío, hurto robo o fraude por parte de los clientes:** Bajo los nuevos requisitos, los emisores de tarjetas de pago y las entidades que ofrecen pagos electrónicos como parte de sus servicios financieros "deberán proveer al usuario, todos los días del año, las veinticuatro horas del día, canales o servicios de comunicación, de acceso gratuito y permanente, que permitan efectuar y registrar tales avisos [extravíos, hurtos, robos o fraudes]. Por el mismo medio de comunicación, y en el acto de recepción, el emisor deberá entregar al usuario un número, código de recepción o identificador de seguimiento, y la fecha y hora del aviso, procediendo de inmediato al bloque respectivo del medio de pago, en lo referido a su funcionalidad para efectuar pagos o transacciones electrónicas".
   - **Tipos de comportamiento malicioso que involucran credenciales de autenticación e identidad:** La ley describe varios "comportamientos" clasificados como fraudulentos. El mal uso de las credenciales de autenticación y la suplantación de la identidad de otra persona se enumeran como actos castigables que podrían resultar en encarcelamiento y multas.

Políticas y Legislación

1. Anteproyecto de ley para regular la protección y el tratamiento de los datos personales y que crea la agencia de protección de datos personales

   Aunque este proyecto de ley se presentó por primera vez al Senado en marzo de 2017, sigue siendo un anteproyecto y solo recientemente fue enviado a la Comisión de Finanzas del Senado para su primera revisión el 16 de marzo de 2020. Una vez aprobado, el proyecto de ley establecerá de manera oficial la Agencia Nacional de Protección de Datos Personales del país y establecerá también regulaciones para la protección de los datos personales mediante la actualización del marco legal existente según la Ley 19.628. Las regulaciones se alinearán con el RGPD y otros estándares internacionales de protección de datos, y proporcionarán principios rectores para la protección y el tratamiento de datos. Hay tres ministerios distintos que están desarrollando el proyecto de ley: el Ministerio de Economía, Fomento y Turismo; el Ministerio de Finanzas; y el Ministerio de la Secretaría General de la Presidencia.

   A la fecha de publicación de este reporte, el proyecto de ley no ha avanzado más allá de la revisión por parte de la Comisión para el Mercado Financiero.

   Aspectos destacados clave para las instituciones financieras

   - **Establecimiento de la Autoridad de Protección de Datos Personales:** Una de las disposiciones del anteproyecto de ley prevé la creación de una agencia de protección de datos encargada de regular y supervisar los incumplimientos de la ley.
   - **Requisitos para el tratamiento de datos personales sensible:** La nueva ley describirá los requisitos para procesar información personal sensible, como datos biométricos y de geolocalización.
   - **Requisitos para la transferencia internacional de datos:** Las instituciones financieras deberán cumplir con los nuevos requisitos para el tratamiento de datos durante las transferencias de datos a nivel internacional.

2. Reglamento del sistema de pago interbancario BCCh LBTR

   En diciembre de 2019, después de una consulta pública de dos meses, el Banco Central de Chile (BCCh) publicó un marco regulatorio para implementar el nuevo sistema de pagos interbancarios de Liquidación Bruta en Tiempo Real (LBTR) del país para pagos en dólares estadounidenses.

   Aspectos destacados clave para las instituciones financieras

   - "A título meramente enunciativo, se deja constancia que los mecanismos de seguridad de SWIFT están incluidos en los servicios SLS (Secure Login & Select) que garantizan que la institución que se está conectando a la red SWIFT, y por tanto enviando mensajes, es aquella que dice ser, y el RMA (Relationship Management Application) que permite el intercambio de mensajería SWIFT entre las partes, para autenticar el origen y destino, y verificar el contenido del mensaje. Asimismo, el software de la interfaz S.W.I.F.T. permite a cada participante discriminar los accesos que dará a cada uno de sus apoderados, limitando los montos y tipos de mensajes que pueden enviar".
   - "En el mismo carácter señalado en el número anterior, se deja constancia que los mecanismos de seguridad del BCCh incluyen, entre otros, la detección de ITF duplicadas (a través de la identificación única en el TRN de los mensajes SWIFT), los mecanismos de acceso a través de las estaciones de trabajo browser y la duplicación de la información almacenada. Asimismo, se dispone de redundancia y alta disponibilidad de equipos, aplicaciones, líneas de comunicación y sitio de procesamiento alterno".
   - **Requisitos de seguridad para la continuidad operativa y de seguridad de la red de comunicaciones:** Para facilitar las operaciones de seguridad cuando operan a través de SWIFT u otra red comparable, las entidades deben contar con "soluciones de protección avanzada sobre las estaciones que se conectan a la [red de comunicación] (por ejemplo, Multifactor de Autenticación, Sistemas de Prevención de Intrusos y Firewall de host, entre otros)".

BANCO CENTRAL

El **Banco Central de Colombia** es el principal responsable de la creación de las de políticas financieras y además es el banco central del país, el cual emite la moneda y regula los tipos de cambio. Una de las funciones principales del banco es promover la inclusión financiera. Es miembro de la organización International Financial Inclusion Alliance.

AUTORIDAD DE PROTECCIÓN DE DATOS

La Superintendencia de Industria y Comercio (SIC) es una agencia reguladora del gobierno que tiene el deber de asegurar una competencia justa y fomenta el crecimiento económico en el sector privado. Emitir normas técnicas y velar por su cumplimiento es parte de sus funciones. La SIC está dividida en seis departamentos, tres de los cuales son Protección al Consumidor, Protección de Datos Personales y Regulación Técnica.

COLOMBIA

Resumen general del país

En septiembre de 2020, el Ministerio de Hacienda y Crédito Público de Colombia dio a conocer las reglas para un entorno de pruebas regulatorio de tecnología financiera que lanzó a principios de 2019, lo cual creó una impresión muy positiva para los bancos y los consumidores. Hasta el lanzamiento de este entorno regulatorio, también llamado «sandbox», el movimiento de la política y la legislación de la tecnología financiera en el país había sido lento y limitado. Pero con la revelación de su Plan de desarrollo para 2018-2023, el gobierno de Colombia ha reafirmado su dedicación a aumentar la inclusión financiera y se ha convertido en un competidor respetable para los gigantes regionales de tecnología financiera, como Brasil y México. Tras un crecimiento del 61% en el negocio Fintech en el sector privado en el año 2019, Colombia se ha convertido oficialmente en la tercera industria de tecnología financiera más grande de América del Sur.

El crecimiento móvil en Colombia en el año 2019 llegó hasta un increíble 147%, según las cifras de la Superintendencia Financiera de Colombia (SFC).[4] En contraste, el uso de cajeros automáticos y terminales de pago aumentaron en un 13 y 22%, respectivamente. Y antes de la pandemia, aproximadamente el 80% de los adultos colombianos tenía cuentas de depósito en un banco.

En este momento existe gran acceso a cuentas bancarias, y más colombianos se incorporaron durante la pandemia de COVID-19 que en todo el año 2019.[5] Gran parte de este aumento se debió a un mandato que exigía que las personas tuvieran cuentas bancarias para recibir ayuda federal por la pandemia. Los bancos más grandes del país, así como los recién llegados a la tecnología financiera, respondieron a la demanda, lo que representó la mayor parte de la adquisición de nuevos clientes. El sector privado de Fintech parece estar expandiéndose muy rápidamente, tanto que las autoridades nacionales parecen no poder crear regulaciones y normativas para seguir el ritmo, con más de 120 jóvenes compañías registradas para el entorno regulatorio de pruebas (también llamado «sandbox») en 2020.[6] En la fecha de la publicación de este reporte, ninguna autoridad financiera ha anunciado una ley especializada en tecnología financiera. Sin embargo, parece haber un enfoque en subsectores dentro de la tecnología financiera, junto con pautas específicas para esos subsectores, tales como pagos y financiación colectiva (esta última también conocida como «crowdfunding»).

Otros asuntos financieros:

La SFC es una agencia gubernamental independiente que monitorea y supervisa los mercados financieros, de seguros y de valores en Colombia, lo que incluye la implementación y el cumplimiento de medidas de protección de datos financieros. La agencia también ofrece protección a inversionistas.

El Ministerio de Hacienda y Crédito Público es el ministerio de gobierno responsable de implementar las políticas financieras aprobadas por el Congreso y de desarrollar sus propias políticas con el objetivo de alcanzar la inclusión financiera.

Leyes y regulaciones

1. Circular 026 de 2019

   El 8 de noviembre de 2019, la SFC emitió una circular que describía los nuevos requisitos para el uso de dispositivos celulares y las medidas de seguridad para proteger la información financiera del consumidor. La circular está alineada con el objetivo de la Superintendencia de promover nuevas tecnologías digitales para reducir los riesgos asociados con el uso de dinero en efectivo.

   Con la circular, la SFC derogó las instrucciones emitidas en la Circular 093 de 2010, añadiendo cuatro nuevos requisitos:

   - **Mitigación de la seguridad cibernética en las instalaciones físicas:** "1) Restringir el uso de teléfonos celulares o de elementos de comunicación personales a los funcionarios de las áreas de caja en las oficinas donde se realicen depósitos, pagos y retiros, o en cualquier área donde la institución financiera identifique la necesidad de restringir el horario comercial al público;
   - **Uso móvil del consumidor:** 2) Autorizar el uso de dispositivos celulares por parte de consumidores financieros mientras se encuentren en instalaciones de instituciones financieras, como sucursales bancarias;
   - **Divulgación del consumidor para expresar inquietudes:** 3) Exigir la publicación de instrucciones precisas visibles sobre los funcionarios o áreas responsables de recibir depósitos, pagos y retiros, sin perjuicio de que se disponga de un punto de información para absolver las inquietudes de los consumidores financieros;
   - **Escolta policial para retiros de efectivo:** 4) Informar a los consumidores sobre la posibilidad de contar con el servicio de escolta de la Policía Nacional en casos de ciertos retiros de efectivo".

2. Circular 029 de 2019

   El 11 de diciembre de 2019, la SFC emitió una circular promoviendo la adopción de tecnologías como blockchain, inteligencia artificial y realidad aumentada, con el objetivo de ofrecer mejores servicios financieros a los consumidores. La circular también describe los requisitos de seguridad para la autenticación biométrica y solicita modificaciones a varios capítulos de la Circular Básica Jurídica existente en el país, que es el conjunto de reglas generales por las que se rigen las instituciones financieras en Colombia.

   Las instituciones financieras tienen hasta junio de 2021 para cumplir con los nuevos estándares de seguridad. Antes de eso, las instituciones financieras tienen hasta diciembre de 2020 para notificar a los clientes acerca de la posibilidad de habilitar un registro de pagos recurrentes con tarjetas de débito o con terceros que carguen ahorros, cheques y/o tarjetas de crédito.[7]

   La circular también cubre:

   - **Recopilación de datos de computación en la nube:** La primera modificación requiere cambios en el subnumeral 3.5 del Capítulo VI, sección "Reglas relativas al uso de los servicios de computación en la nube" de la Circular Básica Jurídica. Los cambios abordan el tipo de servicios disponibles en la nube, el tipo de información recopilada para su procesamiento y los controles de seguridad para la protección de datos en "contextos virtualizados" o aplicaciones en la nube.
   - **Uso biométrico en los servicios financieros:** La circular exige la integración de instrucciones para implementar y utilizar la tecnología biométrica como parte de los servicios financieros. El cambio específico modifica el Capítulo 1, Título 2 de la Parte 1 de la Circular Básica Jurídica.
   - **Portabilidad de datos:** La circular también exige estándares para el intercambio de información cuando se llevan a cabo operaciones monetarias como transacciones electrónicas. Este cambio requiere modificaciones a los Subnumerales 3.2.3.4 y 3.2.4.6. del Capítulo 1, Título 3 de la Parte 1 de la Circular Básica Jurídica.

3. Circular número 5 de 2020

   El 17 de junio de 2020, la SIC emitió una circular relacionada con el Decreto 682 de 2020, la cual contiene instrucciones sobre la recopilación y el procesamiento de datos personales en los días en los que el impuesto al valor agregado está exento. El Decreto 682, emitido en respuesta a la pandemia de COVID-19, se aplica principalmente a los consumidores minoristas o "consumidores finales" y excluye transacciones como el arrendamiento de oficinas.

   La Circular 5 complementa el decreto y entró en vigencia de manera inmediata.

   Esta circular exige que las entidades:

   - Cumplan con todas las regulaciones y leyes de protección de datos personales aplicables.
   - Implementen las recomendaciones de la SIC acerca de la publicidad, marketing y comercio electrónico, incluida la Guía sobre el Tratamiento de Datos Personales para Fines de Comercio Electrónico y la Guía sobre el Tratamiento de Datos Personales con Fines de marketing y publicidad;
   - Informen a los consumidores acerca de la recopilación de datos personales;
   - Garanticen una mayor responsabilidad en cuanto al tratamiento de datos personales sensibles y no hagan que ningún servicio al consumidor tenga como condición el consentimiento para la recopilación de datos personales sensibles.

4. Resolución 32821 de 2020

El 1 de julio de 2020, la SIC publicó una resolución relacionada con la implementación de múltiples medidas legales en respuesta a la pandemia de COVID-10. La resolución ordena la reanudación de los procedimientos de verificación establecidos en el inciso 11 del artículo 58 de la Ley 1480 de 2011. Este artículo describe los requisitos relacionados con el cumplimiento de los procesos de verificación y los medios de comunicaciones electrónicas que se utilizarán para garantizar el cumplimiento.

- **Uso de comunicaciones y firmas electrónicas:** "Los servidores y contratistas de la Delegatura utilizarán los medios tecnológicos en todas las acciones, comunicaciones, notificaciones, y permitirán a las partes, abogados, terceros e intervinientes actuar en el trámite de verificación del cumplimiento mediante los medios tecnológicos disponibles, sin exigir formalidades innecesarias.
- Los memoriales, poderes y demás comunicaciones podrán ser enviados y recibidos por correo electrónico evitando presentaciones o autenticaciones personales o adicionales de algún tipo. Se usará el formato PDF para los documentos escritos enviados o recibidos por medios electrónicos. Las partes, abogados, terceros e intervinientes en los trámites de verificación del cumplimiento deberán suministrar la dirección de correo electrónico para recibir comunicaciones y notificaciones. Para las firmas de las providencias y demás actuaciones por parte del juez, funcionarios y secretario, se empleará firma digital".

5. Circular 008 of 2020

OEl 18 de agosto de 2020, la SIC emitió una circular con instrucciones detalladas para la recolección y tratamiento de datos personales dentro del marco de los protocolos de bioseguridad ordenados por el Ministerio de Salud y Protección Social. La circular se aplica a las entidades supervisadas, incluidas las instituciones financieras, en situaciones en las que se deben realizar determinados protocolos de bioseguridad.

La circular también cubre:

- **Estándares de recolección y tratamiento de datos personales:** Hay cinco estándares para la recolección y el tratamiento de datos:

1. "No se pueden utilizar medios engañosos o fraudulentos para recolectar y realizar tratamiento de datos personales.

2. Se debe informar a la persona la finalidad específica de la recolección de sus datos. 3) No se puede recolectar cualquier dato sino solo aquel o aquellos que sean pertinentes y adecuados para la finalidad para la cual son requeridos.

3. No se deben recolectar datos diferentes a los exigidos expresamente por el Ministerio de Salud y Protección Social.

4. Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin la autorización previa, expresa e informada del titular".[8]

Leyes y regulaciones

1. Reglas regulatorias del entorno de pruebas de Fintech: Decreto 1234 de 2020

En septiembre de 2020, el Ministerio de Hacienda y Crédito Público emitió un decreto para «promover la innovación en los servicios financieros a través del establecimiento de un sandbox regulatorio para las empresas dedicadas a implementar la innovación en tecnología financiera".[9] El Decreto permite exenciones de los requisitos generales del Estatuto Orgánico del Sistema Financiero, Decreto 2555 de 2010. Una de las exenciones permitiría operaciones relacionadas con créditos financieros para compañías sin licencia.

BANCO CENTRAL

El **Banco Central de Costa Rica (BCCR)** es la principal autoridad monetaria y creadora de políticas en Costa Rica.

Otras autoridades financieras incluyen:

La **Superintendencia General de Instituciones Financieras (SUGEF)** es la agencia nacional encargada de supervisar a las instituciones financieras para asegurar el cumplimiento de las regulaciones financieras nacionales e internacionales.

AUTORIDAD DE PROTECCIÓN DE DATOS

La **Agencia de Protección de Datos de los Habitantes (PRODHAB)** es la autoridad nacional en protección de datos, encargada del cumplimiento de la ley y del desarrollo normativo en relación con los datos.

El **Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT)** es un organismo estatal que rige y promueve el cumplimiento de una serie de políticas públicas, lo que incluye la creación de un marco de transformación digital.

COSTA RICA

Resumen general del país

Aunque la mayoría de los países de América Central han logrado mantener economías estables a la entrada del año 2021, Costa Rica enfrenta una tasa de desempleo del 23%, la cifra más alta registrada en décadas. La pandemia de COVID-19 ha afectado al país de manera especialmente dura en comparación con países con una población y clasificación del PIB comparables, y algunas medidas gubernamentales recientemente derogadas, incluido el aumento de los impuestos sobre la renta y la propiedad, han exacerbado el malestar general de la población en cuanto a este tema. El país ha experimentado una gran agitación social y existe una cierta desazón y desconfianza entre las partes interesadas del sector privado.

Esto podría resultar sorprendente tratándose de un país recientemente reconocido por la Organización internacional para la Cooperación y el Desarrollo Económico por su progreso en la transformación digital.[10] Según la OCDE, el uso de tecnologías digitales en Costa Rica está muy por encima del promedio en comparación con otros países de América Latina, y el gobierno nacional ha estado bien informado al implementar políticas de transformación digital para optimizar las operaciones del sector público, al tiempo que se promueve la innovación en el sector privado. En solo los últimos dos años, el gobierno ha creado una estrategia nacional de transformación digital e implementado planes de modernización para varias agencias gubernamentales.

Además, el sector de tecnología financiera en Costa Rica sigue creciendo, con 25 nuevas compañías fintech en el país, la mayoría de ellas empresas SaaS que ofrecen servicios a las instituciones financieras.[11] Al igual que la mayor parte de los gobiernos de la región, Costa Rica no tiene regulaciones específicas que establezcan reglas de banca abierta y no ha anunciado planes para desarrollarlas para la fecha de publicación de este reporte. Esto es algo desconcertante, porque, a pesar de que la innovación digital es alta, abrir una cuenta bancaria en Costa Rica puede ser difícil. La apertura de una cuenta personal implica ciertas barreras, ya que se requiere una copia del pasaporte, extractos bancarios actuales y una explicación del origen de los fondos.[12] Los consumidores podrían beneficiarse de reglas que disminuyeran la cantidad de regulaciones relacionadas con el proceso de apertura de cuentas para adultos.

Por el momento, Costa Rica está priorizando modernizar sus servicios y operaciones públicos, y no hay mucha información para las instituciones financieras que estén buscando orientación sobre transformación digital, innovación y ciberseguridad.

Leyes y regulaciones

1. INTE/ISO/IEC 27103: Orientación sobre estándares de ciberseguridad: Técnicas de seguridad y seguridad en las aplicaciones

   El 21 de febrero de 2020, el Comité de Seguridad de la Información de INTECO aprobó una guía para facilitar el cumplimiento de la Norma ISO 27103 de 2018 existente, la cual incluye las mejores prácticas y técnicas para aplicaciones de seguridad cibernética.

Políticas y Legislación

1. Ministerio de Hacienda - Hacienda Digital para el Bicentenario

   El 19 de febrero de 2020, el Ministerio de Hacienda publicó la Hacienda Digital para el Bicentenario: su plan oficial para modernizar sus procesos y servicios como parte de la estrategia de transformación digital nacional. El Ministerio de Hacienda específicamente está tratando de "fortalecer la estabilidad fiscal mejorando la eficiencia de la gestión del gasto público y el desempeño operativo en la administración tributaria y la facilitación del comercio".

2. Comunicado de PRODHAB sobre la Estrategia Nacional de Privacidad

   - El 20 de julio de 2020, PRODHAB emitió un comunicado de prensa actualizando a las partes interesadas y al público sobre el desarrollo de su Estrategia Nacional de Privacidad, la cual tiene como objetivo implementar recomendaciones emitidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) a finales de 2017.

     Según el comunicado de prensa, la estrategia describe posibles soluciones a problemas de privacidad, lo que incluye disposiciones de puerto seguro y disposiciones de protección de datos personales en casos de transferencias de datos a otros países.

     PRODHAB anunció planes para presentar la estrategia para ser revisadas por las partes interesadas y para consulta pública. En el momento de publicación de este reporte, no se ha anunciado aún un cronograma de consultas.

BANCO CENTRAL

El **Banco Central de Reserva de El Salvador** es el banco central de El Salvador. El banco era privado hasta que se convirtió en una entidad pública con la Ley de Reorganización de la Banca Central. El Banco es miembro de la Alianza para la Inclusión Financiera.

Otras autoridades financieras incluyen:

La **Superintendencia del Sistema Financiero (SSF)** es la entidad supervisora principal y la encargada de hacer cumplir todas las disposiciones del Banco Central que rigen las instituciones operating in El Salvador.

AUTORIDAD DE PROTECCIÓN DE DATOS

Para la fecha de publicación de este reporte, El Salvador no ha establecido una autoridad de protección de datos.

EL SALVADOR

Resumen general del país

Quizás sea porque es el país más pequeño de Centroamérica, o porque es uno de los países más densamente poblados del mundo, pero las palabras "fintech" e "inclusión financiera" no suelen ser lo primero que viene a la mente cuando se piensa en El Salvador, un país conocido principalmente por la producción de materias primas. Aunque el país ha estado lidiando con un bajo crecimiento del PIB y tendrá que enfrentarse a cierta contracción del PIB en 2021, el desarrollo fintech y la dedicación del gobierno nacional a la hora de crear una economía más inclusiva a nivel financiero, hacen que El Salvador sea un lugar emocionante en cuanto a los desarrollos en la banca digital.

De los 6.5 millones de habitantes de El Salvador, aproximadamente el 30% tiene una cuenta bancaria formal, lo que significa que el 70% de la población solo tiene acceso limitado a servicios financieros.[13] Sin embargo, del 30% de las personas que sí tienen cuentas bancarias, el 34% prefiere llevar a cabo transacciones de forma digital y otro 9.2% prefiere métodos de pago alternativos. Aun así, el 44% prefiere realizar transacciones de manera presencial en sucursales bancarias. Aunque las cifras muestran una creciente preferencia por la banca digital, también reflejan el desafío específico que enfrentan los bancos y otros proveedores de servicios financieros digitales: ofrecer servicios a personas de bajos ingresos o a personas que viven en áreas rurales, las cuales pueden no tener la tecnología necesaria para realizar transacciones digitales o abrir una cuenta bancaria digital.

Sin embargo, los bancos de El Salvador continúan haciendo la transición a lo digital, y el gobierno nacional y el Banco Central de Reserva están tratando de mantener el ritmo. Se han anunciado varias iniciativas, incluyendo planes para una ley nacional de protección de datos y computación en la nube.

Como la mayoría de los países que lidian con la gran velocidad de los servicios financieros digitales, El Salvador no tiene una ley dedicada a la tecnología financiera para guiar a los interesados del sector público como el privado. La aprobación de una ley de tecnología financiera será crucial para la iniciativa de inclusión financiera del país.

Leyes y regulaciones

1. Normas Técnicas para el Registro, Obligaciones y Funcionamiento de Entidades que realizan operaciones de envío o recepción de dinero a través de subagentes o administradores de subagentes (NRP-19)

   El 20 de septiembre de 2019, el Comité de Normas del Banco Central aprobó estas nuevas normas técnicas, las cuales derogaron las Normas Técnicas para el Registro, Obligaciones y Funcionamiento de Entidades que realizan operaciones de envío o recepción de dinero (NRP-12). Los estándares establecen el marco legal para las transferencias de dinero y fomentan la inclusión financiera, además de promover las mejores prácticas de lavado de dinero y financiamiento al terrorismo mediante la integración de un "administrador de subagentes y su red de subagentes", refiriéndose específicamente a las compañías que realizan operaciones para empresas que realizan transferencias de dinero. Las regulaciones tienen como objetivo final establecer disposiciones para las partes que realicen operaciones de transferencia de dinero en nombre de una parte obligada, con el fin de promover la disponibilidad de servicios fintech.

Los nuevos estándares se aplican a las "personas jurídicas" en El Salvador que realicen transferencias de dinero, por sí mismas o con entidades comerciales "sistemática o sustancialmente, por cualquier medio, a nivel nacional e internacional". Esto significa actividades de transferencia de dinero que representen "una actividad importante dentro de las operaciones del negocio de la entidad".

2. Ley de Comercio Electrónico

El 29 de octubre de 2019, la Asamblea Legislativa Nacional introdujo la Ley de Comercio Electrónico, que tiene como objetivo establecer un marco legal para las "relaciones electrónicas de índole comercial, contractuales" que se realizan digitalmente, tales como las transacciones comerciales electrónicas. La ley se aplica tanto a las entidades del sector público como a las privadas e incluye el intercambio de bienes o servicios contractuales a través de canales digitales. Las compañías aplicables que operen fuera del territorio nacional serán reguladas por las autoridades de El Salvador según convenios o tratados internacionales. La ley incluye 29 disposiciones y establece 3 disposiciones de gobierno legal: los principios de equivalencia funcional, neutralidad tecnológica y no repudiación, algo que básicamente otorga la misma legalidad y valor a los documentos electrónicos que a los físicos.

Oficialmente, la ley entró en vigor el 29 de octubre de 2020.

Aspectos destacados clave para las instituciones financieras

- **Uso de tecnología para la verificación escrita:** El artículo 8 de la nueva ley establece que el requisito de constatación por escrito en el contexto del comercio electrónico "se tendrá por cumplido cuando se realice a través de soporte electrónico" y se almacene para su posterior consulta. Para los contratos que deben ser firmados por "intervinientes", se cumple el mismo requerimiento mediante el uso de firma electrónica, de acuerdo con la Ley de Firma Electrónica.
- **Errores en las comunicaciones comerciales electrónicas:** El artículo 10 establece derechos relacionados con errores durante las comunicaciones de comercio electrónico. Establece que cuando ocurre un error "al momento de introducir los datos en una comunicación comercial", el pagador o iniciador tiene derecho a "retirar dicha comunicación o enviar un mensaje comunicando la equivocación al destinatario" o beneficiario siempre y cuando no se haya aceptado la transacción o pago.
- **Validez y eficacia de los contratos celebrados por vía electrónica:** El artículo 14 de la ley establece que los contratos celebrados por medios electrónicos "producirán todos los efectos previstos por el ordenamiento jurídico para los contratos, cuando concurran el consentimiento y los demás requisitos legales necesarios para su validez". También dice que el consentimiento debe obtenerse a través de un sistema "automatizado".
- **Proceso de confirmación y verificación de datos personales:** El artículo 16 de la ley establece que los clientes deben tener la oportunidad de "verificar, modificar y confirmar" órdenes o transacciones comerciales mediante el establecimiento de una serie de variables, como el pago o el destino de la orden y la verificación de los datos personales.
- **Obligación de entregar comprobante de transacción:** El artículo 17 de la ley establece la obligación de las entidades de proporcionar comprobantes de pago a los usuarios. Establece que "una vez realizada la transacción, [el proveedor] enviará al usuario por vía electrónica un comprobante de pago".

3. Normas Técnicas revisadas para el Inicio de Operaciones y Funcionamiento de los Proveedores de Dinero Electrónico (NASF-07)

El 19 de agosto de 2020, el Comité de Normas del Banco Central de Reserva aprobó normas técnicas para el registro y operación de proveedores de dinero electrónico que operan dentro del territorio nacional. Las nuevas normas regulan los requisitos y procesos para la autorización de servicios de proveedores de dinero electrónico y a la vez facilitan la inclusión financiera. Las entidades que deben cumplir con las reglas incluyen compañías proveedoras de dinero electrónico, así como bancos, bancos cooperativos y compañías de ahorro y crédito interesadas en ofrecer servicios de dinero electrónico.

Aspectos destacados clave para las instituciones financieras

- **Autorización de inicio de operaciones y registro de los Proveedores de Dinero Electrónico:** El artículo 4 de las nuevas normas describe varios requisitos relacionados con la incorporación para el registro de compañías proveedoras de dinero electrónico, y exige 11 tipos diferentes de documentos contractuales y comerciales que deben ser notarizados o firmados.
- **Requisitos del modelo operativo:** El artículo 5 de las reglas describe ocho requisitos mínimos para el funcionamiento de un servicio de dinero electrónico. Estos requisitos incluyen:
  - Una descripción técnica general de la tecnología a utilizar en las operaciones;
  - Un mecanismo de identificación y un método de registro de la información del cliente en los servicios prestados;
  - Un método para proporcionar claves de seguridad a los clientes y un procedimiento de notificaciones para la denegación de servicio;
  - Un mecanismo que asegure la vinculación de un registro de dinero electrónico a una sola persona física.

- **Seguridad de la información:** El artículo 6 establece que los proveedores de servicios de dinero electrónico están obligados a gestionar la seguridad de la información según lo establecido en dos grupos de normas técnicas existentes aprobadas por el Comité de Normas del Banco Central: las Normas Técnicas para la Gestión de la Seguridad de la Información (NRP-23) y las Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio (NRP-24).
- **Obligaciones de los proveedores de servicios de dinero electrónico:** El artículo 28 establece que los proveedores deben cumplir con varias obligaciones, algunas de las cuales están relacionadas con la identidad del participante.
  - El apartado A establece que los proveedores deben "acatar los procedimientos, medidas y controles internos" que le sean instruidos por los proveedores o los bancos que brindan el servicio, incluidas las políticas de Debida Diligencia para el Conocimiento del Cliente.
  - El apartado B agrega el requisito de confidencialidad del cliente.
- **Contratación de servicios:** El artículo 41 describe la responsabilidad específica con respecto a las obligaciones de los proveedores de dinero electrónico con respecto a la contratación de servicios, incluida la seguridad de la información de los clientes, y se refiere a las Normas Técnicas para la Gestión de la Seguridad de la Información (NRP-23).
- **Contenido mínimo de los contratos con proveedores de dinero electrónico y participantes:** El artículo 30 de las nuevas normas establece requisitos mínimos cuando los participantes firman contratos de servicios de dinero electrónico, lo que incluye la identificación de las partes contratantes, brindar una plataforma electrónica que soportará el servicio por medio de dispositivos móviles, y la obligación de cumplir con los marcos legales y regulatorios en materia de lavado de dinero y de activos y financiamiento al terrorismo.

Políticas y Legislación

1. Actualización de la Ley Especial contra Delitos Cibernéticos

   El 27 de octubre de 2020, la Comisión de Seguridad Pública y Combate a la Narcoactividad anunció planes para crear una mesa técnica interinstitucional como parte de una iniciativa para actualizar la Ley Especial Contra Delitos Cibernéticos. Estas noticias surgieron después de que la Comisión recibiera un informe sobre delitos violentos del Instituto de Medicina Legal de la Corte Suprema de Justicia.

   El informe sugirió la clasificación de nuevos tipos de delitos digitales, entre ellos la "exposición indebida o ilícita de información personal, suplantación de sitios web para extracción de datos personales, transferencia no consentida de activos, delitos relacionados con la firma electrónica, acoso digital contra personas naturales y jurídicas, secuestro de datos y usurpación de identidad".

   La Comisión también anunció planes para establecer un equipo técnico que represente al Comité de Ciberseguridad y a otras instituciones públicas y privadas. El equipo se encargará de presentar un proyecto de reformas de ley a la Comisión.

BANCO CENTRAL

El Banco de Guatemala es el banco central de Guatemala.

Otras autoridades financieras incluyen:

La **Superintendencia de Bancos (SIB)** es el principal regulador de servicios financieros de Guatemala. El banco emite decretos y normas legislativas destinados a aumentar la inclusión financiera y a proteger a los consumidores.

AUTORIDAD DE PROTECCIÓN DE DATOS

Para la fecha de publicación de este reporte, Guatemala no cuenta con una autoridad dedicada de privacidad o una ley de protección de datos que rija los principios básicos de privacidad de los datos. Hasta ahora, no se han anunciado planes para el desarrollo y la aprobación de una ley de protección de datos.

GUATEMALA

Resumen general del país

Debido a que comparte fronteras con otros tres países latinoamericanos, incluido México, y a que es el país más poblado de Centroamérica, Guatemala cuenta con la economía más grande de Centroamérica. Su economía se basa principalmente en la producción agrícola y la exportación de café, plátanos y azúcar en bruto, además de otros cultivos. Sin embargo, aunque la economía es estable, el panorama económico del país es complejo y sus ciudadanos enfrentan problemas relacionados con la desigualdad de ingresos, las prácticas de trabajo no reguladas y los estándares de remesas. El gobierno nacional no está tan bien equipado ni financiado como otras administraciones comparables, ya que solo recibe como promedio entre el 9 y el 11% de los ingresos anuales del PIB.[14] Las limitaciones del gobierno a la hora de ofrecer servicios de calidad, algo que incluye a los servicios financieros, hacen que no haya suficientes incentivos para promover la auto regulación o el pago de impuestos.

En este contexto, quizás no sea sorprendente que el uso de servicios financieros, especialmente de servicios financieros digitales, aún no esté generalizado en Guatemala, aunque sí está creciendo a un ritmo acelerado. Según los datos del plan de inclusión financiera del país, solo el 44% de los adultos tiene una cuenta de depósito y poco más del 13% cuenta con un préstamo bancario, lo que significa que más de la mitad de la población no utiliza productos de servicios financieros regulados. Aproximadamente medio millón de personas utilizan servicios financieros móviles, una cantidad pequeña si se considera que el país tiene 17 millones de habitantes.

Además, los migrantes de Guatemala son responsables de una gran parte de las transferencias electrónicas de dinero al país y no hay un sistema nacional centralizado de transferencias de remesas disponible para los migrantes. Principalmente utilizan aplicaciones de tecnología financiera. De hecho, según investigaciones del Laboratorio Digital de MIT publicadas en mayo de 2020, existe una gran oportunidad para que los servicios financieros digitales satisfagan las necesidades financieras de los pequeños agricultores si los proveedores son capaces de establecer relaciones de confianza.[15]

El año pasado, el gobierno nacional lanzó un plan de inclusión financiera cuyo objetivo es agilizar los servicios financieros y ofrecer mejor acceso a los servicios financieros digitales, por ejemplo, fomentando las transferencias de remesas a través de aplicaciones de cupones digitales. Además, se ha lanzado un plan de digitalización para empresas micro, pequeñas y medianas, ya que una de las barreras más importantes para el uso de transacciones electrónicas es la falta de un sistema de punto de venta (POS, por sus siglas en inglés) digital para realizar transacciones. Los reguladores financieros gubernamentales han afirmado que continuarán implementando varias iniciativas regulatorias y legislativas en 2021, con el objetivo de lograr una mayor inclusión financiera para los consumidores.

Leyes y regulaciones

1. Decreto 6- 2020: Autorización de uso de cheques electrónicos

   El 18 de marzo de 2020, el Congreso de la República de Guatemala emitió un decreto que autorizaba el uso de cheques electrónicos en respuesta a la pandemia de COVID-19. Este decreto contiene varias enmiendas al Código Nacional de Comercio, permitiendo el uso de cheques electrónicos, con el fin de fomentar las mejores prácticas internacionales y modernizar el sistema financiero. Además, algo muy significativo, las enmiendas otorgan la misma validez legal a los cheques electrónicos que a los físicos, particularmente en transacciones de cámaras de compensación.

Aspectos destacados clave para las instituciones financieras

- **Autorización de cheques electrónicos:** El artículo 611 aborda la validez legal de los cheques electrónicos. Señala que "la copia del cheque digital pagado que extienda el banco, con la constancia de que es copia fiel, tendrá los mismos efectos legales, validez, fuerza obligatoria y probatoria que los cheques físicos". El artículo 611 también clarifica el procesamiento del truncamiento de cheques y estipula que los bancos deben adquirir copias digitalizadas de los cheques físicos pagados antes de destruirlos.

2. Resolución de la Junta Monetaria JM 42-2020: Modificaciones al Reglamento para la Administración del Riesgo Tecnológico

   El 24 de abril de 2020, el Banco Central de Guatemala emitió una resolución aprobada por su Junta Monetaria que describe los requisitos de riesgo tecnológico para las compañías que ofrecen servicios financieros. Los nuevos requisitos se aplican a bancos, instituciones financieras y compañías extranjeras que prestan servicios financieros.

   Aspectos destacados clave para las instituciones financieras

   Introducción de información seudonimizada: Políticas y procedimientos de riesgo tecnológicos: En cuanto al riesgo tecnológico (definido como "la contingencia de que la interrupción, alteración o falla de los sistemas de estructura de TI" provocando pérdidas a las financieras públicas y privadas), el artículo 3 de la resolución establece que "las políticas y procedimientos deberán comprender, como mínimo, las metodologías, herramientas o modelos de medición del riesgo tecnológico", además de los sistemas de TI, seguridad de TI, ciberseguridad, planes de recuperación frente a desastres y procesamiento y externalización de la información.

   - **Gestión de la seguridad de la información:** El artículo 17 de la resolución describe métodos de seguridad de la información con el objeto de "garantizar la confidencialidad, integridad y disponibilidad de los datos, así como mitigar los riesgos de pérdida, extracción indebida y corrupción de la información".
     Los métodos incluyen la "identificación y clasificación de la información de acuerdo a criterios de sensibilidad y criticidad".
   - **Operaciones y servicios financieros a través de canales electrónicos:** El artículo 19 de la resolución establece que las instituciones financieras que ofrecen servicios financieros digitales deben implementar medidas de seguridad básicas para proteger la información y los sistemas de TI.
     - Mecanismos de protección y control de infraestructura de TI, sistemas de información y bases de datos con respecto a la gestión de la seguridad cibernética.
     - Medidas de seguridad para la comunicación de información que esté respaldada por un certificado digital, cifrado de datos u otros mecanismos que puedan asegurar la autenticidad, confidencialidad, integridad y disponibilidad de la información.

Políticas y Legislación

1. Plan de Digitalización de MSME 2019-2022

   El 23 de octubre de 2019, el Ministerio de Economía público un plan de digitalización que tiene como objetivo apoyar a aproximadamente 15,000 empresas micro, pequeñas y medianas para que estas adopten las mejores prácticas digitales para mejorar los productos y servicios. El plan pide que el Ministerio y sus socios tecnológicos respalden a tales compañías hasta finales de 2022.

2. Estrategia Nacional de Inclusión Financiera (ENIF), Guatemala 2019-2023

   El 31 de octubre de 2019, el Ministerio de Economía, actuando de forma conjunta con la SIB y el Banco de Guatemala, público planes para la Estrategia Nacional de Inclusión Financiera de Guatemala. La estrategia, que se implementará hasta 2023, tiene como objetivo desarrollar un crecimiento económico sostenible y mejorar la calidad de vida promoviendo un mejor acceso a productos y servicios financieros.

   El documento presenta una descripción general de los planes de inclusión financiera y describe las leyes y reglamentos aprobados que respaldan la inclusión financiera, analiza la aprobación de la Junta Monetaria para la creación de la Comisión Nacional de Inclusión Financiera (COMIF), detalla los elementos estratégicos de la puesta en marcha de la estrategia y presenta un cronograma para la implementación de múltiples iniciativas de inclusión financiera. Estas iniciativas incluyen modificaciones a las regulaciones de servicios financieros móviles, un proyecto de ley sobre dinero electrónico y las regulaciones sobre su implementación, una campaña de divulgación de firmas electrónicas y un marco general para el desarrollo de las tecnologías financieras.

   Sin embargo, hasta la fecha de publicación de este reporte, no ha habido ningún movimiento legislativo relacionado con las iniciativas antes mencionadas (por ejemplo, consultas públicas, etc.) y no se han anunciado actualizaciones al cronograma de implementación.

3. Carta de entendimiento en materia de cooperación para la creación del Timbre Electrónico Notarial y Forense

   El 10 de enero de 2020, el Ministerio de Economía y el Colegio de Abogados y Notarios de Guatemala suscribieron una carta de entendimiento para crear timbres electrónicos notariales y forenses. Los nuevos timbres permitirán que los abogados y notarios registrados y activos utilicen una billetera virtual, a la cual se podrá acceder a través de un portal del Colegio de Abogados y Notarios, y donde se podrán comprar juegos de timbres electrónicos que luego podrán utilizarse en documentos electrónicos. Los titulares de las billeteras virtuales tendrán que depositar más dinero cuando se agoten los timbres. Los timbres serán identificados por un color específico según el mundo adquirido.

   En última instancia, el uso de timbres electrónicos eliminaría los requisitos judiciales que se aplican a los documentos impresos y podría ser un precursor de un uso más amplio para transacciones en el sector comercial.

4. Implementación de Firma Electrónica Avanzada Institucional (Certificado Digital)

   El 1 de septiembre de 2020, el Ministerio de Economía anunció un requisito que exige que el Registro de Garantías Mobiliarias comience a enviar y recibir documentos utilizando la Firma Electrónica Avanzada Institucional, el certificado digital público que se puede utilizar además de un código QR para aumentar la robustez de la seguridad de las transacciones, con efectividad inmediata. Los documentos incluidos en estos planes incluyen los registros de incorporación, modificación, extensión, cancelación y ejecución de garantías reales, emisión de reportes de consulta y emisión de certificaciones.

BANCO CENTRAL

El **Banco Central de Honduras** es responsable de mantener la estabilidad de la moneda nacional y de desarrollar la política monetaria.

AUTORIDAD DE PROTECCIÓN DE DATOS

El **Registro Civil Nacional** es la agencia gubernamental encargada de emitir documentos de identificación a los hondureños y de proteger la información personal sensible. La agencia gestiona el sistema de registro civil.

El **Instituto de Acceso a la Información Pública** es una agencia gubernamental reguladora que garantiza el acceso público a la información y protege los derechos de los ciudadanos con respecto a sus datos.

HONDURAS

Resumen general del país

Honduras, un país conocido entre sus socios internacionales como un gran exportador de textiles y otros recursos naturales, está pasando por un período de relativa estabilidad financiera y política después de años de promulgar reformas a varias leyes creadas para fomentar la inversión extranjera y alinearse con los estándares internacionales, tales como la Principios básicos de Basilea. Los bancos no estaban sujetos a muchas regulaciones antes de la llegada del huracán Mitch en 1998, pero eso cambió gracias a su importante contribución al sistema financiero general, proporcionando el 95% de los activos totales.[16] El sector bancario del país es relativamente pequeño en comparación con el de otros países latinoamericanos de tamaño y estatus económico comparables, y está compuesto por 15 bancos regionales privados que han sido recipientes de la mayor parte de la inversión extranjera. Las funciones de supervisión y ejecución del Banco Central se fortalecieron con la adopción de un modelo de supervisión basado en el riesgo que modificó las leyes del sector financiero entre 2004 y 2013.[17] El proyecto modernizó el Banco Central, introduciendo nuevas tecnologías, y ayudó a que Honduras volviera a tener una situación económica estable.

Sin embargo, el desarrollo regulatorio reciente en cuanto a la tecnología financiera y la transformación digital ha sido muy limitado. El país no tiene una ley dedicada a las compañías de tecnología financiera o una ley nacional de protección de datos, aunque sí ha lanzado una promoción para su iniciativa de inclusión financiera dirigida a las mujeres. A principios de 2019, el Congreso Nacional de Honduras había anunciado planes para desarrollar y aprobar una Ley de Protección de la Información Personal Confidencial pronto, pero para la fecha de publicación de este reporte, no se ha avanzado en el desarrollo legislativo y no se ha anunciado nada al respecto. De hecho, algunos expertos legales han concluido que el "principio del secretismo bancario de Honduras" suprime el desarrollo de la banca abierta en el país. Además, la Autoridad de Servicios Financieros, la agencia reguladora que potencialmente podría supervisar las operaciones de tecnología financiera y hacer cumplir las reglas en el país, no ha llevado a cabo ninguna actualización legislativa en relación con los servicios financieros digitales en 2020.

La falta de acción regulatoria por parte de las autoridades nacionales es difícil de entender, considerando que una gran parte de la población hondureña comprende el valor de los servicios financieros digitales. Para 2017, el uso de la billetera digital en Honduras había aumentado un 71% en comparación con los dos años anteriores. La mayoría de las transacciones eran remesas entre áreas urbanas y rurales.

Aunque el panorama económico del país sigue siendo estable tras la pandemia de COVID-19, la rentabilidad ha sufrido un impacto económico en todos los sectores, incluido el sector de la banca comercial.[18] Los bancos y las instituciones financieras en Honduras pueden conseguir nuevos clientes e incorporar nuevas tecnologías si el gobierno nacional y las autoridades reguladoras dan prioridad a la transformación digital y a la inclusión financiera en 2021 y más allá.

Otras autoridades financieras

La **Comisión Nacional de Bancos y Seguros (CNBS)** es la autoridad principal que rige el sector financiero y el sector de seguros en Honduras. Las funciones de la Comisión incluyen la redacción de reglamentos y la promoción de la inclusión financiera. El Comité Fintech e Innovaciones Tecnológicas (CFIT) trabaja bajo la supervisión de la Comisión para apoyar iniciativas regulatorias y técnicas relacionadas con las tecnologías financieras.

La **Autoridad de Servicios Financieros (Financial Services Authority «FSA»)** es la agencia reguladora principal para la industria de servicios financieros que no entren dentro del alcance de la Ley Bancaria y la Ley de Seguros. La agencia también es el principal organismo regulador que desarrolla normas contra el lavado de capitales en Honduras.

Leyes y regulaciones

1. Decreto número 33- 2020: Ley de auxilio al sector productivo y a los trabajadores ante los efectos de la pandemia provocada por el COVID-19: Reforma de las firmas electrónicas

   El 3 de abril de 2020, el Congreso Nacional promulgó una ley para ofrecer diferentes tipos de asistencia a los trabajadores del sector de la producción en respuesta a la pandemia de COVID-19. La nueva ley modifica los artículos 7 y 27 de la Ley de Firma Electrónica para permitir que las instituciones gubernamentales utilicen tecnologías equivalentes a las firmas electrónica avanzadas para la firma de documentos.

   La ley entró en vigor el mismo día que se publicó.

   Aspectos destacados clave para las instituciones financieras

   - **Enmienda al artículo 7:** Requisito de firma electrónica avanzada: La modificación del artículo 7 de la Ley de Firma Electrónica otorga equivalencia a otros tipos de firma electrónica distintos a la firma electrónica avanzada certificada. Este tipo de tecnología podría incluir:

     1. Un híbrido de tecnologías basadas en la Infraestructura de Llave Pública («PKI», por sus siglas en inglés), firma biométrica o equivalente;
     2. Sistemas de firma electrónica que operan en la nube;
     3. Sistemas de autenticación de doble factor;
     4. Sistemas biométricos, incluyendo medios fotográficos;
     5. Otras tecnologías de firma electrónica que puedan ir desarrollándose en el futuro.

   - **Enmienda al artículo 27:** Reconocimiento de Identidades, Firmas Electrónicas y Certificados Extranjeros: La reforma al artículo 27 de la Ley de Firma Electrónica ha cambiado la ley y otorga equivalencia legal a las firmas electrónicas "creadas o utilizadas" fuera del territorio nacional; esto significa que ahora tienen el mismo estatus que las firmas "creadas o utilizadas" en Honduras, siempre que la firma se pueda considerar confiable. Este mismo efecto legal se aplica a los certificados de firma electrónica emitidos por Autoridades de Certificación extranjeras. Cualquier acuerdo entre las partes para usar un tipo de firma electrónica específico será suficiente para el reconocimiento transfronterizo. La ley proporciona una lista de entidades "confiables" que serían consideradas proveedores o usuarios de firma electrónica confiables.
   - "Las entidades del sector público o privado podrán designar a uno o más responsables de certificar las autorizaciones que correspondan para asegurar la fluidez de sus operaciones por medios electrónicos. Estas personas tendrán el carácter de fedatarios. Las personas designadas deben ser comunicadas al Instituto de la Propiedad. Las entidades del Estado deberán tener por válidas las certificaciones realizadas por estos medios y surtirán los efectos señalados en el artículo 7 de la Ley Sobre Firmas electrónicas".

2. Circular CNBS No. 023/2020

   El 12 de junio de 2020, la CNBS emitió una circular sobre varios asuntos regulatorios en conexión con la gestión de tecnologías de información y comunicación. Algunos de los elementos de la circular clarifican las nuevas modificaciones, así como los requisitos de firma electrónica existentes.

   Aspectos destacados clave para las instituciones financieras

   - **Normas para regular la firma en formato electrónico de la Comisión Nacional de Bancos y Seguros (Resolución GTI número 977):** El 6 de marzo de 2020, la Comisión Nacional de Bancos y Seguros aprobó las normas para regular la firma en formato electrónico de la Comisión.
   - **Estándares del Sistema de Gestiones Electrónicas de la Comisión Nacional de Bancos y Seguros (Resolución GTI número 978):** Junto con las normas para regular la firma electrónica de la CNBS, la Comisión también aprobó normas para las operaciones de su Sistema de Gestión Electrónica (SGE).

3. Recomendación a la CNBS para la habilitación de las firmas electrónicas avanzadas

   El 8 de junio de 2020, la agencia de Gerencia de Tecnología de Información y Comunicación envió un memorando a la Comisión Nacional de Bancos y Seguros recomendando la habilitación de una "ventanilla electrónica de correspondencia" como "canal digital para la recepción de la documentación remitida por las instituciones supervisadas, así como demás personas naturales y jurídicas que todavía no han sido capacitadas en el uso del Sistema de Gestiones Electrónicas (SGE)".

   Para mantener la validez jurídica de los documentos y verificar la autenticidad del emisor, la ventanilla "firmará la recepción de esta correspondencia con una firma electrónica avanzada y autenticará al remitente con un sistema de doble factor" que otorgaría la equivalencia de una firma electrónica avanzada.

   El uso de la Ventanilla Electrónica de Correspondencia como canal digital para la recepción de la documentación enviada por las instituciones supervisadas se aprobó el 18 de junio de 2020.

BANCO CENTRAL

El **Banco de México (Banxico)** es el banco central de México y la principal autoridad monetaria del país. Como la mayoría de los bancos centrales, mantiene la estabilidad financiera del país y fomenta el uso de la moneda nacional.

AUTORIDAD DE PROTECCIÓN DE DATOS

El **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)** es la agencia de protección de datos independiente de México. El INAI tiene el deber constitucional de defender y ampliar el derecho de acceso a la información pública y de mantener la protección de datos personales.

La **Secretaría de Economía (SE)** es la oficina del gobierno federal responsable de todo lo relacionado con la economía y las industrias comerciales de México. Además, la SE publica pautas relacionadas con los requisitos de notificación de privacidad en colaboración con el INAI.

MEXICO

Resumen general del país

El vecino del sur de Estados Unidos es también un punto regional importante para el desarrollo de compañías de tecnología y servicios financieros. México cuenta con una inversión récord de $8 mil millones en nuevas compañías Fintech, con más del 16% de la inversión en tecnología financiera en la región. Al igual que Brasil, México atrae a inversionistas de tecnología financiera debido a su gran población y a la gran importancia que tiene la inclusión financiera para los clientes mexicanos. Según el Banco Interamericano de Desarrollo, que reportó 441 nuevas compañías Fintech operando en el país a fecha de septiembre de 2020, esta tendencia Fintech solo puede ir en aumento.[19]

Por otro lado, los bancos han tenido que enfrentarse a resultados inesperados debido a los efectos de la pandemia de COVID-19. El sector bancario sufrió los primeros daños significativos en junio de 2020, cuando el Banco Ahorro Famsa declaró bancarrota según capítulo 1 de los Estados Unidos 21, y el Banco de México expresó su preocupación de que la economía del país continuara estando negativamente afectada en 2021.[20]

Además de estos desafíos, el contexto de la inclusión financiera es extremadamente variado en México y hay bajos niveles de acceso financiero para un gran porcentaje de la población. Según la aceleradora de compañías de tecnología financiera Catalyst Fund en un reporte de abril de 2020, el 50% de los adultos mexicanos no tiene cuentas bancarias y el mismo porcentaje no tiene acceso a Internet. Los bancos y las compañías de Fintech en México tampoco parecen estar colaborando para trabajar en soluciones, lo que crea un mercado de servicios financieros fragmentado. Esta podría ser la razón por la que el dinero en efectivo sigue siendo el medio más importante de pago en México: aproximadamente solo el 4.1% de los adultos ha usado una cuenta de dinero móvil en el último año.[21] Y aunque el gobierno federal publicó una Estrategia Digital Nacional en 2013, se han lanzado pocas iniciativas para lograr sus objetivos.

Sin embargo, el contexto regulatorio para el sector de servicios financieros en México sigue siendo sólido, y el Banco Central de México ha aprobado docenas de regulaciones en los últimos años, muchas de las cuales regulan al creciente sector de la tecnología financiera. Se espera que los efectos de la pandemia de COVID-19 se agraven para los bancos del país en 2021, por lo tanto, el sector de servicios financieros de México depende de la rápida recuperación de la economía y de la dedicación de los bancos para modernizar y digitalizar sus servicios.

Otros asuntos financieros:

La **Secretaría de Hacienda y Crédito Público (SHCP)** alberga el Ministerio de Finanzas del país y opera como miembro de la consejería del ejecutivo federal. La SHCP supervisa la Oficina de Hacienda y Crédito Público.

La **Comisión Nacional Bancaria y de Valores (CNBV)** es una agencia independiente que opera bajo la supervisión de la Secretaría de Hacienda y Crédito Público y es la autoridad ejecutiva que supervisa el sistema financiero en México. La CNBV es autónoma y regula las instituciones financieras y los bancos para garantizar la estabilidad del sistema financiero nacional.

Leyes y regulaciones

1. Reglamento de la Ley Fintech 2020

   En abril de 2018, México promulgó su Ley para Regular las Instituciones de Tecnología Financiera de forma oficial. Esta ley requiere que las instituciones financieras y las compañías de tecnología financiera establezcan APIs para permitir el intercambio de datos y extender el acceso a los datos para los consumidores. En junio de 2020, el gobierno federal amplió la ley Fintech,

añadiendo nuevos requisitos de comunicación de datos que garantizarán una interoperabilidad segura entre bancos e instituciones de dinero electrónico. Los tipos de datos cubiertos por la ley son datos agregados, datos abiertos y datos transaccionales.

Aspectos destacados clave para las instituciones financieras

- **Circular 2/20: Disposiciones generales aplicables a agencias de reporte y conmutadores de API:** El 2 de junio de 2020, el Banco de México publicó un reglamento que establece estándares para el uso de APIs por parte de las instituciones de crédito, lo que incluye estándares técnicos de interoperabilidad. Es importante señalar que la mayoría de las regulaciones se aplican únicamente a la comunicación de datos abiertos y agregados, no a los datos transaccionales. Sin embargo, ya que los requisitos exigen la aprobación de los API, independientemente del tipo de datos comunicados, existe una excepción para los datos transaccionales.
  Todos los tipos de operaciones de comunicación de datos deben contar con un certificado digital aprobado por el Banco de México.
- **Excepción para los datos transaccionales:** La normativa establece que las entidades financieras bajo su ámbito de aplicación que deseen una certificación oficial para la comunicación de datos transaccionales deben cumplir dos condiciones:
  1. Obtener la aprobación del Banco de México para las operaciones de comunicación de datos transaccionales.
  2. Enviar propuestas que presenten diferentes tipos de datos transaccionales al Banco de México en un periodo de 360 días desde la publicación de la Circular 20/20 (mayo de 2021). Más tarde, el Banco de México publicará disposiciones generales sobre la comunicación de datos transaccionales entre entidades financieras a través de APIs. Las nuevas disposiciones también abordarán el consentimiento por parte de los clientes.
- **Mecanismos de autenticación e identificación:** Como parte de las propuestas en relación con los datos transaccionales, las entidades financieras deben incluir en un plan de trabajo, métodos de autenticación e identificación de clientes durante las transacciones aplicables. La normativa establece que los planes de trabajo deben incluir:
  "Las medidas para evitar que la transmisión de Datos Agregados permita la identificación de los datos personales o transacciones de las personas" y "los mecanismos de autenticación para verificar que los terceros que pretendan acceder a la API son Entidades Reconocidas con las que tengan formalizados Contratos de Interconexión".
- **Autorización de datos transaccionales:** En cuanto a los datos transaccionales, la normativa establece que "una vez que la cámara de compensación o SIC de que se trate haya obtenido autorización del Banco de México para intercambiar los Datos Agregados y, en su caso, los Datos Financieros Abiertos conforme al artículo anterior, esta deberá presentar una solicitud de autorización adicional para intercambiar los Datos Transaccionales que resulten procedentes de conformidad con los requisitos que el Banco de México establezca mediante resoluciones de carácter general que emita al efecto, en las cuales podrá establecer requisitos adicionales para dicho intercambio".

2. Comunicación 18/2020 del CNBV sobre la obligación de establecer mecanismos de verificación de la identidad de sus clientes

   El 31 de marzo de 2020, la CNBV publicó una circular sobre las obligaciones de las instituciones financieras y de crédito en cuanto a establecer la identidad de ciertos clientes. La circular no proporciona nuevas pautas ni consejos; extiende el plazo para cumplir con los requisitos de verificación de identidad hasta el 30 de noviembre de 2020.

   Inicialmente, se había exigido que las instituciones cumplieran antes del 31 de marzo de 2020.

3. Disposiciones de la SHCP y CNBV relativas a las API estandarizadas a que hace referencia la ley para regular las instituciones de tecnología financiera

   El 4 de junio de 2020, la SHCP y la CNBV publicaron disposiciones generales que establecen reglas para las operaciones API de las instituciones financieras, con el objetivo de fomentar la inclusión financiera, mejorar la protección al consumidor y promover la competencia en el mercado. Las disposiciones abordan el acceso a datos para los interesados y controladores de datos y proporcionan pautas técnicas para la seguridad y el acceso a los datos relacionados con la identificación de usuario.

   Aspectos destacados clave para las instituciones financieras

   - **Protección de Datos:** Se exige que los controladores de datos establezcan una política de seguridad que integre el cifrado de datos para minimizar el riesgo en cuanto a los datos personales. El capítulo 3, artículo 4 de las disposiciones establecen que una política de seguridad debe incluir procesos de "cifrado de la información almacenada y de los canales a través de los que se envíen los datos, así como mecanismos de autenticación e identificación" que cumplan con las pautas técnicas de las nuevas disposiciones. Las pautas de los Anexos 1 y 2 no describen los tipos de mecanismos de autenticación y verificación de identidad que cumplen con la ley, pero cualquier método utilizado debe cumplir con los requisitos descritos en los Anexos 1 y 2 de las disposiciones.
   - **Certificados de llaves públicas:** "El proveedor de datos debe utilizar el protocolo HTTPS, con el objetivo de garantizar el cifrado de la información durante el intercambio de la misma". Los proveedores de datos deben utilizar certificados digitales emitidos por autoridades certificadas. El certificado digital

debe basarse en el estándar internacional X.509 de infraestructura para llaves públicas, utilizando el protocolo de criptografía TLS, en la versión que se encuentre en el momento de la implementación.

- **Seguridad de acceso:** Según las nuevas disposiciones, los controladores de datos pueden usar tokens digitales para identificar a los solicitantes por un máximo de 30 días después de la solicitud inicial de servicios. Dice que los controladores de datos "pueden identificar al solicitante de datos manteniendo la vigencia del token de acceso por un máximo de 30 días para la consulta de datos" mediante el uso de claves API o llaves API estandarizadas OAuth 2.0.
- **Identificación y autenticación de empleados:** Las disposiciones generales requieren que los responsables del tratamiento establezcan "mecanismos de identificación y autenticación del personal responsable del manejo de APIs bajo el principio de mínimo privilegio". Según ese principio, los administradores de APIs solo deberían tener acceso a la información necesaria para el manejo de los sistemas de API.

4. Comunicado No. 45/2020 de la CNBV acerca de las Facilidades Regulatorias en materia de identificación presencial para instituciones de crédito

   El 20 de junio de 2020, en respuesta a la pandemia de COVID-19 y sus efectos en los clientes de las instituciones de crédito, la CNBV emitió una comunicación con vigor inmediato en la que se describen las especificaciones regulatorias en cuanto a la identificación presencial para las instituciones de crédito. Las especificaciones se aplican a cualquier institución de crédito, independientemente de si está afiliada a una asociación comercial.

   Aspectos destacados clave para las instituciones financieras

   - **Aplicabilidad a las instituciones legales:** Las entidades legales que actúan en nombre de los solicitantes ahora están cubiertas por el servicio. Esto significa que a partir de ahora las entidades legales podrán, de manera independiente, autorizar la apertura de cuentas y solicitudes de crédito de forma no presencial. La facilidad establece que, "la apertura de cuentas y el otorgamiento de créditos de forma no presencial apliquen también a las personas morales, en adición a personas físicas para quienes ya era aplicable".

     Además, las personas morales que actúen como solicitantes estarán sujetas al mismo proceso de verificación de identidad que las personas físicas y deberán utilizar FIEL, la plataforma nacional de firma electrónica del país, para verificar su identidad.
   - **Categorización de clientes «Conozca a su cliente» (KYC):** La identificación remota, o no presencial, categoriza a los clientes, distinguiendo entre clientes existentes de una institución de crédito aplicable y quienes aún no son clientes, o son nuevos clientes. Esto es porque los clientes se clasifican en niveles basados en el riesgo según el sistema de niveles KYC de México. La comunicación señala: "El proceso de identificación y contratación no presencial se divide entre quienes ya sean clientes de la entidad de crédito y aquellos que no lo sean, haciéndolo más expedito para quienes ya sean clientes de la institución, en virtud de que ésta ya cuenta con el expediente del cliente y solo tendría que actualizarlo, dependiendo del producto financiero que contrate"

     Adicionalmente, la identificación remota durante la apertura de la cuenta "se acota a cuentas bancarias nivel 4, dejando de lado las cuentas nivel 3 que refiere **la regla** vigente, teniendo así una desregulación". Las cuentas nivel 3 y 4 tienen diferentes requisitos para los tipos de documentos de identificación requeridos, así como una diferencia en los límites para las transacciones mensuales.
   - **Validación biométrica para clientes existentes:** Para agilizar el proceso de solicitud de crédito para quienes ya son clientes de la institución de crédito, la normativa estipula que los clientes deberán proporcionar solo información biométrica para que esta se verifique contra los registros de alguna autoridad que proporcione el servicio de información biométrica del cliente, como el Instituto Nacional Electoral.
   - **Cumplimiento normativo ALD/CTF para no clientes:** El proceso de verificación de identidad para nuevos solicitantes que aún no son clientes de la institución de crédito a la que están solicitando debe cumplir con las regulaciones de Prevención de Lavado de Dinero y de Financiamiento al Terrorismo (ALD/CTF, por sus siglas en inglés). Según el reglamento, "Cuando se identifique que el solicitante no es cliente de la institución, será necesario realizar el proceso para poder cumplir con la regulación en materia de Prevención de Lavado de Dinero y Financiamiento al Terrorismo".
     Además, los solicitantes que aún no sean clientes de una institución de crédito deben realizar una videollamada como parte del proceso de verificación de identidad. La regulación también permite que la videollamada pueda grabarse para su uso posterior utilizando inteligencia artificial.

5. Circular 37/2020 acerca de los activos virtuales en instituciones de crédito y de tecnología financiera

   - El 30 de septiembre de 2020, el Banco de México emitió una circular relacionada con operaciones de activos virtuales dirigida a instituciones de crédito y de tecnología financiera. La circular modifica una circular anterior, la Circular 4/2019, la cual contenía reglas generales para las operaciones de activos virtuales. Después de un período de análisis en el cual el banco emitió una consulta pública y recibió comentarios, modificó la circular, estipulando que las instituciones relevantes reguladas por las disposiciones generales deben cumplir con ciertas especificaciones al hacer contratos con terceros. Además, las instituciones deben buscar orientación y aclaraciones sobre la participación de terceros en operaciones de activos virtuales.

Políticas y Legislación

1. Ley de Servicios de Pago (PSA, por sus siglas en inglés) 2019

   Comunicado 344/19 sobre el refuerzo normativo de la protección de datos con adhesión a instrumentos europeos.

   El 23 de septiembre de 2019, el INAI publicó una comunicación que refuerza la dedicación de la agencia en cuanto a alinear las regulaciones nacionales de protección de datos personales con los estándares y convenios europeos, lo que incluye el Convenio 108 y el RGPD.

2. Plataforma de Cobros y Pagos Digitales Cobro Digital (CoDi)

   En octubre de 2019, el Banco de México lanzó de manera oficial su plataforma de "solicitudes de pago" para dispositivos celulares, llamada Cobro Digital o CoDi. La plataforma permitirá que los usuarios realicen transferencias bancarias en dispositivos celulares a través del Sistema de Pagos Electrónicos Interbancarios (SPEI) del país. Los usuarios utilizan códigos QR o terminales físicos habilitados con tecnología de Comunicación de Campo Cercano (NFC, por sus siglas en inglés) para realizar transferencias o compras de hasta $8,000 pesos ($400 USD). Con el lanzamiento de CoDi, el banco tiene como objetivo incrementar la inclusión financiera en México.

   La adopción de CoDi ha sido un proceso lento hasta ahora. De los más de 5 millones de usuarios que descargaron la aplicación, aproximadamente 250,000 la habían utilizado para realizar pagos para principios de octubre de 2020.[22] Dicho esto, las cifras han ido aumentando lenta pero constantemente desde que fue lanzado.

3. Orientación de la UIF en materia de nuevas actividades vulnerables

   Operaciones con Activos Virtuales: En octubre de 2019, la Unidad de Inteligencia Financiera (UIF) emitió orientaciones en relación con las operaciones con activos virtuales, algo que se considera una "nueva actividad vulnerable" según el artículo 17 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, que fue actualizada en 2018. La guía proporciona instrucciones técnicas para las operaciones de activos virtuales y define las operaciones de activos virtuales como una actividad vulnerable que requiere sus propias obligaciones de seguridad por parte de las instituciones.

4. Acuerdo INAI acerca del acceso a la información y protección de datos personales

   El 28 de noviembre de 2019, el INAI publicó un acuerdo en el que se detalla el código ético en cuanto a la protección de los datos personales. Al mismo tiempo, se derogó el acuerdo anterior, el cual había modificado las directrices relacionadas con la protección de datos personales. Este acuerdo entró en vigor el 29 de noviembre de 2019.

5. Orientación para las instituciones de tecnología financiera

   El 2 de diciembre de 2019, el gobierno federal publicó una sección de preguntas frecuentes para ofrecer al público más claridad en cuanto a un entorno de pruebas regulatorio (también conocido como «sandbox») para las instituciones de tecnología financiera, así como orientación sobre cómo los clientes pueden solicitar una autorización temporal para participar en él.

   Las preguntas frecuentes estipulan que todas las compañías que participen en el sandbox regulatorio deben obtener el consentimiento de sus clientes e informarlos acerca de los riesgos inherentes de la participación.

6. Opinión del INAI relativa a la necesidad de realizar evaluación de impacto sobre intención de transferencia de datos personales

   El 23 de enero de 2020, el INAI emitió su opinión sobre la transferencia de datos personales y la interoperabilidad entre autoridades que procesan datos. En su declaración de opinión, el INAI destaca 10 puntos relacionados con la autoridad de protección de datos del INAI y con las obligaciones de protección en cuanto a datos personales. El INAI afirma en esta declaración que la Secretaría de Economía denegó su solicitud de permitir la transferencia de datos personales entre autoridades financieras públicas.

   En el momento de publicación de este reporte, no se ha anunciado una línea de tiempo para la evaluación de impacto.

7. Comunicado de la UIF No. 074 sobre la evaluación nacional de riesgo y la estrategia para combatir el lavado de dinero y financiamiento al terrorismo

   El 21 de septiembre de 2020, el gobierno federal publicó un comunicado en el que se describen los beneficios y objetivos de la estrategia y evaluación de riesgos nacionales (ENR) para combatir el lavado de dinero y el financiamiento al terrorismo. La estrategia fue presentada por la Unidad de Inteligencia Financiera (UIF), que depende de la Secretaría de Hacienda y Crédito Público (SHCP).

   El comunicado destaca la dedicación de las autoridades financieras mexicanas en lo que respecta a fomentar las iniciativas ALD/CTF mediante la expansión de la autoridad provisional, el desarrollo y la emisión de normas para el cumplimiento de las protecciones ALD/CTF, dando respuesta a las amenazas de corrupción y alineando los objetivos nacionales con las iniciativas internacionales mediante la firma de tratados y convenciones.

8. Panorama anual de inclusión financiera 2020 de la CNBV

   El 27 de septiembre de 2020, la Comisión Nacional Bancaria y de Valores (CNBV) dio a conocer su panorama anual de inclusión financiera en México. Además de ofrecer datos que exploran más a fondo la infraestructura financiera y la protección del consumidor, el resumen describe las actualizaciones normativas recientes relacionadas con la apertura de cuentas remotas y la banca abierta.

BANCO CENTRAL

El **Banco Central de Paraguay** es la principal autoridad monetaria del país y es la entidad que emite la moneda del país. Uno de sus principales objetivos es fomentar y ampliar la inclusión financiera. Este Banco es único, ya que su oficina alberga a la Superintendencia de Bancos del país.

AUTORIDAD DE PROTECCIÓN DE DATOS

Para la fecha de publicación de este reporte, Paraguay no ha establecido una autoridad de protección de datos. Las actividades relacionadas con el comercio electrónico según la Ley de Comercio Electrónico están bajo la jurisdicción de la **Dirección General de Firma Digital y Comercio Electrónico del Ministerio de Industria y Comercio (MIC)**.

PARAGUAY

Resumen general del país

Durante la pandemia de COVID-19, las instituciones financieras en Paraguay tienen una ventaja en los asuntos regulatorios relacionados con la banca digital, la apertura de cuentas y la moneda digital, en gran parte gracias a la regulación favorable al mercado y a los bajos impuestos. Los bancos comerciales son los principales prestadores de servicios financieros del país, pero, en particular, las instituciones cooperativas también impulsan el mercado para el desarrollo de monederos electrónicos. Los bancos cooperativos también tienen un rol significativo en la implementación del marco regulatorio para las instituciones financieras que ofrecen dinero electrónico y servicios de transferencias no bancarias.[23]

La economía de un país tiende a estar en un buen estado cuando sus bancos también lo están. La economía de Paraguay, que ya estaba en una trayectoria sólida hacia la recuperación, ha experimentado una caída del PIB de tan solo 1.2% en 2020, y los expertos predicen un aumento del PIB del 4% para 2021.[24] La estimación de pobreza de Paraguay oscila entre el 30 y el 50%, y los esfuerzos de inclusión financiera en el país parecen ser mínimos. Menos del 32% de la población adulta tiene cuentas bancarias y solo el 7% tiene tarjetas de crédito.[25] Y con solo el 65% de la población con acceso a Internet, no es de extrañar que la banca digital y la industria fintech no hayan prosperado todavía en Paraguay como lo han hecho en otros países de América Latina, tal y como ha sucedido, por ejemplo, en su país vecino, Brasil, que ha convertido en un centro regional de fintech.

Sin embargo, en junio de 2020, la Cámara Paraguaya de Fintech anunció planes para llevar a cabo un estudio sobre el sector fintech del país y sobre las posibilidades de crear un marco regulatorio para las tecnologías financieras. El estudio ha estado pendiente desde que se creó la Cámara en 2017, pero Paraguay aún carece de una regulación fintech que ayude a las pequeñas compañías emergentes que ya han estado operando durante años pero que no pueden ampliar sus servicios debido a la ausencia de disposiciones específicas. Según S&P Global, el contexto regulatorio y el alcance de la supervisión en el sector bancario de Paraguay es "limitado" y los estándares de riesgo operativo nacionales no se han puesto al día con otros marcos regulatorios en regiones comparables.[26]

Las autoridades paraguayas reaccionaron rápidamente a los efectos de la pandemia de COVID-19, legislando activamente en asuntos como transacciones electrónicas, firmas electrónicas y la protección de los datos personales. Sin embargo, Paraguay aún no ha mostrado un compromiso con la inclusión financiera que pueda reducir aún más su tasa de pobreza, lo que queda claro dada su falta de acción en cuanto a la regulación de las tecnologías financieras.

Leyes y regulaciones

1. Comunicado sobre entrega y seguimiento de expedientes

   El 30 de junio de 2020, el Banco Central de Paraguay emitió un comunicado sobre la entrega y seguimiento de documentos durante su tramitación. El comunicado señala que el Banco, junto con la Superintendencia de Bancos y la Superintendencia de Seguros implementarán cinco requisitos para la tramitación de documentos. El requisito número 2 exige el uso de firmas digitales por parte de los operadores bancarios:

1. “La tramitación y/o gestiones deberán ser canalizados a través de medios electrónicos (correo electrónico), adjuntando al mismo la documentación en formato PDF, con imágenes claramente legibles. El legajo deberá estar escaneado, contar con nota de presentación, debidamente firmada y aclarada por los responsables remitentes, foliada (por expediente) con número y letra, en el ángulo superior derecho de la hoja, a partir de la nota, y hasta un máximo de 10 megas. Si la documentación requiere de mayor capacidad, deberán fraccionar y remitir en otro envío, dando continuidad a la foliatura y en el cual se aclare la referencia de la presentación que está siendo complementada.
2. Al recibirse el documento se notificará al remitente, vía correo electrónico, sirviendo como acuse de recibido la fecha y la firma [digital] electrónica del operador responsable del registro remitido por la misma vía.
3. Las solicitudes recibidas luego de las 12:30 serán registradas a partir de las 8:30 del día hábil siguiente. Para el seguimiento del expediente, se deberá utilizar el mismo procedimiento establecido en el numeral 1 (al que se hizo referencia antes). La presentación en formato impreso de todo lo remitido electrónicamente, deberá realizarse conforme a lo acostumbrado, una vez que se hayan levantado las medidas preventivas adoptadas”.

Políticas y Legislación

1. Proyecto de Ley de Protección de Datos Personales

El primer proyecto de ley de protección de datos personales de Paraguay, S-198418, fue presentado al Senado nacional el 21 de marzo de 2019. Desde entonces, el proyecto de ley ha sido objeto de docenas de discusiones en el Senado y de varias revisiones por parte de comisiones. La Ley de Protección de Datos Personales describe los principios básicos para la protección de los datos personales y los derechos básicos relacionados con la protección de datos personales, como los derechos al consentimiento informado y al acceso de las personas a sus datos personales. El proyecto de ley se distingue de otros proyectos de ley de protección de datos personales nacionales porque establece derechos con respecto al acceso y uso de la información crediticia de manera explícita. Pero, como la mayoría de los proyectos de ley de protección de datos, también establecerá la primera autoridad dedicada a la protección de datos personales del país.

Para el momento de publicación de este reporte, no hay planes con fechas específicas para la finalización del proyecto de ley y este sigue estando en desarrollo legislativo con el Senado.

Aspectos destacados clave para las instituciones financieras

- **Disposiciones sobre información de crédito:** La ley establece dos disposiciones acerca de los derechos básicos relacionados con la información crediticia en casos en los que se procesan datos personales. En primer lugar, la información crediticia se define como información positiva o negativa “relacionada con el historial crediticio de personas físicas y jurídicas, acerca de actividades crediticias, comerciales y otras de naturaleza análoga, que sirva para identificar correcta e inequívocamente a la persona, su domicilio, actividad comercial”. Las fuentes de información crediticia incluyen “organismos y entidades del estado”, así como administradoras de fondos previsionales. En otras palabras, la ley se aplica tanto a las entidades del sector público como a las compañías privadas, tales como las instituciones financieras.

  El proyecto de ley establece el derecho al acceso a la información almacenada por compañías de información crediticia como, por ejemplo, las instituciones financieras. Las compañías, cuando se solicite, están obligadas a proporcionar a los interesados la siguiente información:

  - Consulta realizada en cuanto a su información crediticia;
  - La compañía que proporcionará los datos;
  - El propósito del uso de los datos de información crediticia;
  - Los derechos que tienen los interesados.

  Además, el proyecto de ley también establece un límite de tiempo de cinco años para el almacenamiento de información crediticia.

2. Proyecto de ley de los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos

El 18 de septiembre de 2020, el gobierno federal presentó el anteproyecto de ley sobre servicios de confianza para transacciones electrónicas, documento electrónico y documentos transmisibles electrónicos. Si se aprueba, la ley derogará la Ley N° 4017/2010 existente, llamada la Ley de Firma Digital, con el objetivo de integrar las regulaciones relacionadas con los servicios electrónicos de confianza, como la prueba de identidad digital, el sello digital, la marca de tiempo digital y la certificación de servicios de entrega. El proyecto de ley es parte de la Agenda Digital del Gobierno del país, que requiere leyes para aumentar la confianza pública en las transacciones electrónicas y que, en gran parte, se aceleró debido a los efectos de la pandemia de COVID-19 y las preocupaciones por el medio ambiente.

Aspectos destacados clave para las instituciones financieras

- **Influencia de eIDAS:** El proyecto de ley establece que las nuevas normativas tomarán como referencia varias regulaciones relacionadas con las transacciones y con los documentos electrónicos: El Reglamento eIDAS de la Unión Europea, la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y la Ley Modelo de la CNUDMI sobre Documentos Transmisibles Electrónicos.
- **La legalidad de las firmas electrónicas:** El proyecto de ley establece que las firmas electrónicas están legalmente reconocidas. Por ejemplo, las compañías, como las instituciones financieras, que ofrecen servicios de firma electrónica a distancia, "deben aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante".
- **Artículo 102:** Operaciones electrónicas en el ámbito financiero y otros: El artículo 102 del proyecto de ley describe disposiciones específicas con respecto a las operaciones electrónicas en el sector financiero. El artículo establece que las operaciones que impliquen pagos, transferencias de dinero, apertura de cuentas, financiación, gestión de patrimonio y administración de dinero electrónico están sujetos a identificación electrónica mediante "medios de identificación electrónica con un nivel de seguridad alto".
- Supervisión de las firmas electrónicas: Además, las firmas electrónicas calificadas estarán reguladas por el Banco Central o por otra autoridad financiera como la Comisión Nacional de Valores.

3. Pago digital MIC para minoristas - Acuerdo con Bancard

   En septiembre de 2020, el Ministerio de Industria y Comercio (MIC) anunció planes para trabajar con la compañía de adquisición de pagos Bancard con el objetivo de facilitar las operaciones de pago digital

   para pequeños comerciantes. Las pequeñas compañías ahora podrán aceptar pagos a través de un código QR, que será generado por una aplicación asociada.

4. Proyecto de ley de inclusión financiera

   El 12 de octubre de 2020, la Comisión de Legislación y Codificación del Congreso rechazó un proyecto de ley que habría ofrecido a las "personas domiciliadas" en Paraguay la posibilidad de abrir cuentas bancarias en moneda local.

   La opinión de rechazo supone un obstáculo para los defensores de la inclusión financiera. Sin embargo, las instituciones financieras del país pueden alegrarse del hecho de que, en gran parte, el proyecto de ley fue rechazado para darles más control sobre quién puede y no puede abrir cuentas bancarias, particularmente cuentas de ahorro. Las autoridades de la Comisión declararon que exigir la apertura de cuentas por ley podría tener un efecto negativo en los servicios financieros privados.

   El rechazo del proyecto de ley sugiere que las autoridades y los legisladores de Paraguay prefieren adoptar una actitud de no intervención en cuanto a la inclusión financiera y a la imposición de requisitos de apertura de cuentas.

BANCO CENTRAL

El **Banco Central de Uruguay** es la principal autoridad monetaria y la entidad que emite la moneda del país, así como el principal supervisor del sistema bancario nacional. El Banco regula y supervisa a todas las instituciones financieras en Uruguay. La Superintendencia de Servicios Financieros opera bajo el control del Banco Central y rige todas las instituciones financieras del país.

AUTORIDAD DE PROTECCIÓN DE DATOS

La **Unidad Reguladora y de Control de Datos Personales (URCDP)** es la autoridad nacional de protección de datos en Uruguay.

URUGUAY

Resumen general del país

Considerando que es uno de los países más pequeños de América del Sur, tanto en extensión como en población, Uruguay se ha establecido a nivel internacional como un centro tecnológico y culturalmente progresista con grandes planes para el futuro. Según la Embajada de los Estados Unidos en Uruguay, ocupa el primer lugar en una serie de características positivas, que incluyen prosperidad, seguridad, la ausencia de corrupción y paz. Más de la mitad de sus 3.5 millones de habitantes vive en la capital metropolitana de Montevideo o en los alrededores, y es en esta ciudad donde se encuentran la mayoría de los bancos que operan en el país. Gracias a un sector agrícola próspero, el sistema bancario del país se ha estabilizado en los últimos años, y Uruguay está clasificado como un país de altos ingresos por el Banco Mundial.

La pandemia de COVID-19 ha tenido un efecto no muy significativo en la economía de Uruguay[27]. Durante las últimas décadas, el país ha mejorado enormemente su marco de inclusión financiera, y al mismo tiempo ha reducido significativamente el número de ciudadanos que viven en la pobreza extrema. En 2016, la línea de pobreza era del 6%, una cifra sin precedentes para el país.

Las iniciativas económicas progresistas y el crecimiento estable de Uruguay lo han convertido en lo que algunos llaman "el Silicon Valley de América del Sur".[28] Por cada 100 habitantes, hay 147.3 teléfonos celulares y más del 70% de los uruguayos usa Internet. Probablemente, esto es lo que tenía en mente el gobierno cuando aprobó la Ley de Inclusión Financiera en 2014, pero algunas instituciones financieras han tratado de evitar que se implementen los requisitos de la ley.[29] Sin embargo, estas instituciones parecen estar en minoría: a día de hoy, muchas instituciones financieras se están asociando con compañías fintech, como proveedores de SaaS, para crear soluciones digitales que sean más compatibles con la inclusión financiera y los objetivos de seguridad.

A fin de cuentas, el gobierno de Uruguay es partidario del mercado y la innovación, una combinación ganadora para las instituciones financieras que desean modernizar sus servicios mientras siguen cumpliendo con las normativas.

Leyes y regulaciones

1. Decreto 64/2020: Reglamentación referente a protección de datos personales

   El 21 de febrero de 2020, el gobierno uruguayo emitió un decreto que introduce nuevas reglas relacionadas con la privacidad de los datos personales. Estas complementan la Ley N° 19.670 (artículos 37, 38 y 40), que fue emitida en 2017 y se conoce como la Ley de rendición de cuentas y balance de ejecución presupuestal. El decreto realiza cambios en las medidas de seguridad y la notificación de incidentes, y establece el requisito de un oficial de protección de datos para las compañías que procesan grandes cantidades de datos personales. También deroga los artículos 7 y 8 del Decreto No. 414/009, aprobado en agosto de 2009. El decreto obliga a la URCDP a actuar como organismo encargado del cumplimiento, auditoría y evaluación de las medidas implementadas.

   Aspectos destacados clave para las instituciones financieras

   - **Medidas de seguridad:** El artículo 3 del decreto establece lo siguiente con respecto al desarrollo y a la implementación de medidas de seguridad. Específicamente, pide a los funcionarios de seguridad que "valoren la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y Sociedad de la Información y el Conocimiento". También pide procedimientos adecuados en cuanto a infracciones relacionadas con los datos para "minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados".

- **Privacidad por diseño:** El artículo 8 del decreto establece medidas técnicas y organizativas para ayudar a las compañías como las instituciones financieras a cumplir con las normas de protección de datos personales. Las siete medidas son:

  1. Técnicas de disociación, seudonimización y minimización de datos;
  2. Mecanismos para asegurar los derechos de los titulares;
  3. Documentación del consentimiento del titular para el procesamiento de datos;
  4. Documentación de conservación de datos;
  5. Adopción de planes de contingencia que incluyan medidas de seguridad de la información;
  6. Análisis funcionales y modelos de arquitectura de los datos;
  7. Otras medidas establecidas por la Unidad Reguladora y de Control de Datos Personales (URCDP).

2. Comunicación No. 2020/115 sobre Políticas de Prevención de Riesgos de Lavado de Activos y Financiamiento del Terrorismo: Modificación relacionada con «Conozca a su cliente»:

El 3 de julio de 2020, el Banco Central de Uruguay publicó una comunicación que modifica la normativa en materia de métodos de prevención del riesgo de lavado de dinero y financiamiento al terrorismo que opera bajo los principios de Conozca a su cliente (KYC, por sus siglas en inglés). Las reglas entraron en vigor de inmediato.

La comunicación describe tres nuevos mandatos para la "venta de artículos numismáticos":

1. Proporcionar el nombre completo de la persona física o jurídica, documento de identidad vigente para las personas físicas y número de Registro Único Tributario para las personas jurídicas.
2. Para compras superiores a $3 000 USD, o su equivalente en otras monedas, los clientes deben completar la "Ficha de Identificación de Cliente Ocasional" y presentar la documentación que se detalla en la misma.
3. Los usuarios, o clientes que realicen una serie de transacciones por un monto superior o igual a $15 000 USD, deberán completar la Ficha de Identificación de Cliente Habitual y presentar la documentación que se detalla en ella.

Políticas y Legislación

1. Plan de Gobierno Digital Uruguay 2020

En septiembre de 2019, la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento publicó el Plan de Gobierno Digital para el gobierno uruguayo. La agenda establece un marco de política digital nacional que se implementará a través de varias iniciativas, programas y proyectos. El gobierno quiere optimizar los servicios digitales para diferentes canales de distribución, incluidos los dispositivos celulares. El plan se divide en seis objetivos.

En general, el objetivo es crear un gobierno digital confiable, transparente y eficiente.

Aspectos destacados clave para las instituciones financieras

- **Marco regulatorio de transformación digital:** El plan del gobierno tiene los siguientes objetivos finales para la nueva estrategia digital:An integral regulatory framework to guides digital transformation regulation;

  1. Un marco normativo integral para guiar la regulación de la transformación digital;
  2. Un marco institucional consolidado para posibilitar la colaboración entre agencias y organizaciones externas;
  3. Una infraestructura tecnológica creada para una alta demanda de servicios que también implemente las medidas de seguridad necesarias para proteger los datos de los ciudadanos.

- **Avance del uso de la plataforma móvil:** En su plan, el gobierno afirma que impulsará "el uso intensivo de tecnologías como Internet, dispositivos móviles, plataformas compartidas y el aprovechamiento de los datos" como parte de su iniciativa de transformación digital.
- **Identificación digital universal:** Uno de los objetivos del plan es "universalizar" la identificación electrónica nacional para mejorar la seguridad de los servicios digitales. Se enumeran tres pasos para alcanzar este objetivo:

  1. "Promover un ecosistema de identificación electrónica consistente con los niveles de seguridad requeridos y los dispositivos existentes" mediante la implementación de RootCA y SSO en agencias estatales.
  2. Habilitación de servicios de identificación en la nube y en dispositivos móviles para facilitar el uso de la identidad digital por parte de los ciudadanos.
  3. "Extender el acceso a la identificación digital en los adultos mayores".

- **Modernizar el marco regulatorio:** El plan también exige la modernización del marco regulatorio para los servicios de gobierno digitales. Este objetivo presenta tres pasos para la implementación:

  1. Avanzar el marco legal nacional con referencia a nuevos estándares internacionales como RGPD.
  2. Fomentar una mayor conciencia de los derechos de protección de los datos personales.

3. Establecer la adopción de buenas prácticas de privacidad desde el diseño en todas las etapas de los desarrollos tecnológicos y promover su adopción tanto en el sector público como en el privado.

- **Mejora de la ciberseguridad:** El objetivo de ciberseguridad de los planes pide la mejora de las medidas mediante tres acciones:

  1. Crear un Centro Nacional de Operación de Ciberseguridad con un modelo de participación público-privada.
  2. Promover niveles adecuados de ciberseguridad en los sistemas informáticos en el sector privado.
  3. Crear un Laboratorio de Investigación y Análisis del cibercrimen.

- **Consulta pública de la Estrategia de Inteligencia Artificial del Gobierno Digital:** El gobierno de Uruguay lanzó una consulta pública en 2019 solicitando comentarios sobre una estrategia de Inteligencia Artificial (IA) para los servicios digitales de gobierno. Tras llevar a cabo un análisis de las propuestas y tras una segunda etapa de consulta pública, el documento final se publicó en septiembre de 2019. El documento final describe los riesgos y beneficios del uso de tecnologías de IA en el marco del gobierno digital de Uruguay. Sin embargo, los objetivos descritos en el reporte también identifican la necesidad de que haya participación por parte del sector privado en el desarrollo de un marco regulatorio de IA y otras iniciativas relacionadas con la inteligencia artificial.

2. Hoja de ruta del sistema de pagos en Uruguay 2020-2022

En marzo de 2020, el Banco Central de Uruguay publicó su agenda y hoja de ruta del sistema de pagos para el periodo de 2020 a 2022. El documento presenta líneas de acción que tienen como objetivo modernizar el sistema de pagos del país y a la vez proteger a los consumidores, fomentar la competición y prevenir el lavado de activos y el financiamiento al terrorismo. La hoja de ruta presenta tres líneas de acción principales para lograr los objetivos del banco.

La hoja de ruta no proporciona un calendario para una agenda de trabajos anuales, pero establece que se ofrecerá una a los usuarios y agentes "con la debida antelación". Sin embargo, las "medidas y productos concretos" tendrán sus propios cronogramas de desarrollo.

Aspectos destacados clave para las instituciones financieras

- **Innovación e integración de nuevas tecnologías:** El primer objetivo pide promover la competencia en los mercados financieros. El Banco alineará los objetivos de cumplimiento con los estándares internacionales para fomentar la adopción de buenas prácticas a nivel del sistema de pago. También analizará y monitoreará los costos operativos del sistema de pago para promover la competencia y el acceso.

  En cuanto a los consumidores, el Banco está promoviendo "los cambios legales y reglamentarios necesarios para el funcionamiento de los cheques electrónicos, así como la digitalización de cheques", y la portabilidad de datos entre instituciones financieras.

- **Regulaciones y seguridad:** La hoja de ruta también exige que el Banco cree las condiciones para el desarrollo e integración de nuevos productos de tecnologías mediante la agilización del proceso regulatorio. El objetivo es adoptar nuevas tecnologías y productos para su uso en el mercado de manera más rápida y eficiente.

  Además, la hoja de ruta pide que el gobierno se esfuerce por mejorar la seguridad cibernética y la protección de datos dentro del sistema de pago nacional.

---

1 Mencia, Isabelle. "Fintech in Brazil: No Signs of Slowing Down." Colibri Content, March 12, 2020. Bit.ly/2I5LpmD.

2 Gadioli, Camila Spinelli, and Leonardo Rodrigues Tavares Meirinho. "'Banco Maré': Brazilian Cryptocurrency Targeting Social Impact." Lexology. Motta Fernandes Advogados/Terralex, September 30, 2019. Bit.ly/361cv6E.

3 Brown, Allan. "Why Chile May Become LatAm's No. 1 Fintech Hub." BNamericas, April 30, 2020. Bit.ly/386oCBY.

4 "FinTech Regulation in Colombia." Timbi. Timbi Blog, May 29, 2020. Bit.ly/3mTHZSY.

5 Aldaya, Francisco Miguel. "COVID Catalyzes Financial Inclusion in Colombia." S&P Global Market Intelligence. S&P Global, June 23, 2020. Bit.ly/3kYPrLY.

6 Daza, Maria-Leticia Ossa, Matthew Vitorla, and Gabriela Montoya Jurado. "Colombia Launches Regulatory Sandbox for Fintechs." Willkie.com. Latinvex, October 14, 2020. Bit.ly/2GtvaPJ.

7 "Superfinanciera Promotes Security Standards in Transactions and a Better Customer Experience in the Digital Ecosystem." ColombiaFintech.com. Superintendencia Financiera de Colombia, December 17, 2019. Bit.ly/3esYFh5.

8 Cardona, Diego, and Andres Meza. "External Circular 008 of August 18, 2020, through Which the Superintendency of Industry and Commerce Issues Instructions for the Adequate Collection and Processing of Personal Data within the Framework of the Implementation of Biosafety Protocols Ordered by the Ministry of Health and Social Protection." Philippi Prietocarrizosa Ferrero DU & Uría, August 20, 2020. Bit.ly/386Bw2S.

9 Daza, Maria-Leticia Ossa, Matthew Vitorla, and Gabriela Montoya Jurado. "Colombia Launches Regulatory Sandbox for Fintechs." Willkie.com. Latinvex, October 14, 2020. Bit.ly/2GtvaPJ.

10 "OECD Highlights Costa Rica's Progress in Digital Transformation." BNamericas. The Costa Rica News, October 14, 2020. Bit.ly/2I4G6nn.

11 Barquero, Randall, Alejandro Vasquez, Monica Arias, and Ana Carolina Alvarez. "Fintech 2020: Costa Rica." PracticeGuides.Chambers.com. Chambers & Partners, March 2, 2020. Bit.ly/3IbSuAJ.

12 “Why Is Opening a Bank Account in Costa Rica so Difficult?” CostaRicaLaw.com, December 17, 2019. Bit.ly/2JuKfS4.

13 “Digital Banking on the Rise in El Salvador.” Temenos.com. Temenos, November 19, 2019. Bit.ly/2TQmKoC.

14 “The World Bank in Guatemala.” WorldBank.org. World Bank, September 4, 2020. Bit.ly/34XU97i.

15 Cardoso, Cauam, and Jonars Spielberg. “Assessment of Potential Opportunities for Use of Digital Payments for Smallholder Farmers in Guatemala’s Western Highlands.” D-Lab.MIT.edu. MIT Digital Lab/MIT, May 2, 2020. Bit.ly/34ZEPqJ.

16 “Honduras - Banking Systems.” PrivacyShield.Gov. U.S. Dept. of Commerce. Accessed November 3, 2020. Bit.ly/2JFUPGd.

17 “Enhanced Stability in Honduras’ Financial Sector.” World Bank, June 24, 2014. Bit.ly/38bnjS5.

18 “Fintech: Innovations You May Not Know Were from Latin America and the Caribbean .” IADB.org. IDB/Finnovista, 2017. Bit.ly/3kTAhaN.

19 Appleby, Peter. “Banks on Edge as COVID-19 Marks First Bankruptcy.” MexicoBusiness.news. Mexico Business, June 29, 2020. Bit.ly/3mXe9wV.

20 Campero, Mariana, and Linnea Sandin. “The Covid-19 Pandemic Threatens Mexico’s Economy.” CSIS.org. Center for Strategic and International Studies (CSIS), May 27, 2020. Bit.ly/2I22gqb.

21 Reynaga, Eduardo Ortiz, and Maelis Carraro. “Fintech in Mexico: Why Many Low-Income People Stay Excluded.” BFA Global. BFA Global, June 12, 2020. Bit.ly/368NDK0.

22 “CoDi Platform Statistics.” Estadísticas de la plataforma CoDi®, February 11, 2020. Bit.ly/3jXhE4o.

23 Cardoni, Juan Manuel Gustale. “Shifting Winds in Latin America: Tackling Financial Inclusion in Paraguay: Banks with Souls and the Role of Public Financial Institutions as a Means to Reach the Underserved.” Latin America Policy Journal Seventh Edition 2018 (2018). Bit.ly/3ep8NYf.

24 “The World Bank in Paraguay.” WorldBank.org. World Bank, April 20, 2020. Bit.ly/2TS26nQ.

25 “Paysafecard Continues Expansion in South America with Launch in Paraguay.” BNamericas.com. Paysafecard, April 27, 2020. Bit.ly/38aB9Ev.

26 Gunning, Gavin. “Global Banking Country-By-Country Outlook 2020: The Calm Before The Turn?” SPGlobal.com. S&P Global Ratings, November 18, 2019. Bit.ly/3k56T0c.

27 “The Economic Context of Uruguay.” Nordeatrade.com. Nordea, October 2020. Bit.ly/2TTxxyj.

28 Van Oost, Marcel. “FinTech in Uruguay: The Silicon Valley of South America.” LinkedIn. LinkedIn, June 13, 2020. Bit.ly/38c8SNV.

29 “Two pro-Cash Petitions Protesting Uruguay’s Cashless Law: ‘Ley De Inclusión Financiera’.” CashMatters.org. Cash Matters, May 28, 2019. Bit.ly/32gM5g6.

OneSpan

OneSpan ayuda a proteger al mundo del fraude digital creando confianza en las identidades de las personas, los dispositivos que usan y las transacciones que realizan. Hacemos esto asegurando que la banca digital sea accesible, segura, fácil y útil. La plataforma Trusted Identity (Identidad de confianza) y las soluciones de seguridad de OneSpan ya reducen el fraude de manera significativa en las transacciones digitales y aseguran el cumplimiento con las normas para más de 10 000 clientes, incluidos más de la mitad de los 100 bancos mundiales más importantes. Ya sea mediante la automatización de acuerdos, la detección de fraudes o la protección de transacciones financieras, OneSpan ayuda a reducir costos y a acelerar la adquisición de clientes a la vez que mejora la experiencia para los usuarios. Obtenga más información en **OneSpan.com**.

DESCARGUE AQUÍ EL INFORME COMPLETA EN INGLÉS SOBRE EL REGLAMENTO FINANCIERO GLOBAL DE ONESPAN PARA ESTAR AL DÍA DE LOS ÚLTIMOS CAMBIOS NORMATIVOS Y LEGISLATIVOS EN TODO EL MUNDO.