GUÍA DE CONSULTA LEGAL PARA PROYECTOS DE TRANSFORMACIÓN DIGITAL

EN EL SECTOR DE AHORRO Y CRÉDITO POPULAR

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

implementada por:

Sparkassenstiftung Alemana
LATINOAMÉRICA Y EL CARIBE

ABRIL 2021

Guía de consulta legal para proyectos de transformación digital en el sector de ahorro y crédito popular.

Estudio encomendado por Sparkassenstiftung Alemana Latinoamérica y el Caribe (DSIK) y realizado por la firma Vite Abogados.

Eliseo Vite

Consultor Vite Abogados

Pablo Rueda

Consultor Vite Abogados

ÍNDICE GENERAL

Índice de gráficas y tablas

PRÓLOGO

Esta es la primera guía legal para proyectos de digitalización (Guía Legal) para el sector de ahorro y crédito popular que ha elaborado la Sparkassenstiftung Alemana para la Cooperación Internacional (DSIK), con la colaboración del despacho de abogados Vite Abogados (Asesor Legal). Este proyecto surge en el contexto de una fuerte necesidad del sector de ahorro y crédito popular mexicano (SACP) –y del sector financiero mexicano en general— de digitalizar procesos y servicios, ello tanto en el contexto de la pandemia ocasionada por el virus COVID-19 como por la creciente demanda de servicios no presenciales que requiere hacer más eficientes los procesos internos de las Entidades. Esta Guía Legal pretende ofrecer una orientación sobre los problemas que —desde el punto de vista normativo— el SACP enfrenta para llevar a cabo procesos de digitalización y está dirigida principalmente a las Sociedades Financieras Populares (SOFIPO), las Sociedades Cooperativas de Ahorro y Préstamo (SOCAP o Cajas de Ahorro), a las Sociedades Financieras Comunitarias (SOFINCO) y, finalmente, luego de considerar su importancia en el financiamiento de actividades productivas, y sin que ello tenga necesariamente una equivalencia legal, también se ha decidido incorporar para estos efectos a las Sociedades Financieras de Objeto Múltiple no Reguladas (SOFOM) para temas específicos de Prevención del Lavado de Dinero y Financiamiento al Terrorismo (PLD/FT). Además, presentamos algunos aspectos genéricos y experiencias comunes que pueden ser de utilidad a los lectores interesados en la regulación financiera del SACP.

La necesidad y tendencia hacia la digitalización no sólo tiene su origen en las circunstancias ya referidas, también existe un cambio de conducta del consumidor contemporáneo de servicios financieros. Un cliente que, con toda seguridad, cuenta con un teléfono celular, pero no necesariamente una cuenta de ahorro; una persona que tiene poco tiempo para acudir a una sucursal y pasa una buena parte de su día (por ocio, trabajo o ambos) frente a un dispositivo con acceso a Internet. Productos y servicios en la punta de los dedos. Inmediatez y comodidad. Todas las industrias han sido tocadas por este fenómeno: la prensa, las editoras de libros, las productoras musicales. Nuestras vidas se vuelven también digitales: reuniones de trabajo, interacciones interpersonales, compras, entre otros. Los servicios financieros no sólo no constituyen una excepción, sino que se colocan de manera central en esta nueva estructura. Una sociedad hiperconectada

demanda vinculación ágil con su dinero. Una sociedad que, a través de las Naciones Unidas, ha declarado que el acceso a Internet es un derecho humano[1].

Pensamos que el SACP mexicano, dadas las herramientas normativas con las que cuenta y la flexibilidad que tiene para incorporarse a esquemas de negocio novedosos que hasta hace poco eran impensables, tiene grandes posibilidades de lograr esta conversión digital y lograr cumplir, de manera más eficaz, con el propósito para el que fue creado: facilitar el acceso al crédito; apoyar el financiamiento de micro, pequeñas y medianas empresas y, en general, propiciar la solidaridad, la superación económica y social, así como el bienestar de sus miembros y de las comunidades en que operan, sobre bases educativas, formativas y del esfuerzo individual y colectivo.
Este sector, que comenzó a operar en México bajo la figura de las cajas rurales de préstamos y ahorros en 1910, se encuentra posicionado para enfrentar exitosamente al futuro.

El fenómeno de la digitalización es complejo, inmenso y requiere de muchas áreas de experiencia para una comprensión adecuada. En ese contexto, hay que señalar que este documento ha sido elaborado con el fin de orientar legalmente los procesos de digitalización de los servicios y procesos del SACP, lo cual nos planteó los siguientes retos al momento de comenzar el trabajo: (i) establecer una definición operativa de digitalización, (ii) circunscribir la normatividad relevante para el SACP con base en dicha definición y (iii) enfocar el análisis y el contenido a cierto tipo de Proyecto (como se definen en este documento) con base en su relevancia en el sector financiero (en general) y la viabilidad o necesidad de los mismos.

En cuanto al primer punto, hemos decidido definir "digitalización" como el uso de tecnologías informáticas (mismas que en la mayoría de los casos permiten o están relacionadas con el acceso a Internet) que posibilitan a una organización, en este caso las Entidades que forman parte del SACP, automatizar grandes ámbitos de su modelo de operación o del ofrecimiento de servicios para transitar a esquemas más eficientes (internos o externos) y/o de alcance mayor o masivo. Estas tecnologías pueden ser de tipos muy variados dependiendo de los requerimientos de cada Entidad: cómputo en la nube, análisis de datos de manera masivos (*big data*), uso del Internet como herramienta de comercio y publicidad, *blockchain*, inteligencia artificial, contratación a distancia y firma

[1] https://www.vice.com/en/article/3kxmm5/the-case-for-internet-access-as-a-human-right

electrónica, automatización de reportes regulatorios, entre muchas otras que se tratarán en este documento.

Si bien nuestra definición resulta amplia, consideramos que los otros dos elementos restantes fueron de gran ayuda para enfocar este trabajo. Las entidades del SACP están sometidas a una regulación extensa que incide directamente en su operativa, viabilidad y manera de ofrecer sus servicios. No toda digitalización, en nuestra opinión, tiene (necesariamente) relevancia legal y un impacto importante para el SACP, pero, sin duda, la transformación digital a un nivel profundo se entrelaza con la regulación financiera y requiere, en muchos casos, la intervención del regulador (ya sea para autorizar o incluso, como veremos posteriormente, para emitir una opinión informal o económica), de asesores externos y de proveedores de servicios (sobre todo tecnologías) especializados. No pretendemos que este documento sea una referencia absoluta o enciclopédica de todos los Proyectos de digitalización que pudieran llevarse a cabo en el SACP; sin embargo, hemos seleccionado a aquellos que consideramos más complejos y que requieren de un análisis legal cuidadoso para llegar a buen puerto.

Dada la diversidad de receptores y la difusión a la que aspira la Guía Legal, orientándonos por su carácter informativo hemos decidido dividir su contenido en dos secciones conceptuales. En las primeras secciones (Parte I y Parte II) hacemos una exposición sobre los propósitos y limitaciones de la Guía Legal y algunos conceptos generales. Posteriormente, hacemos un recorrido sobre temas legales de importancia central para implementar Proyectos de digitalización. Aunque existen múltiples reglas y, en muchos casos, excepciones de aplicación (sobre todo en temas de banca electrónica y prevención de lavado de dinero y financiamiento al terrorismo), creemos que cada sección presenta una introducción suficiente para poder manejar los temas que abordamos para cierto tipo de Proyectos en particular. El último trecho de esta Guía Legal (Parte III) contiene nuestro punto de vista sobre los aspectos prácticos de cada tipo de Proyecto, ofrece una metodología tentativa para su planificación e indica cuestiones prácticas que no suelen ser explícitas en la normativa. En este afán de convertir este texto en manual de consulta, tratamos de problematizar cada situación y ofrecer pasos tendientes a su resolución, aunque debido a la diversidad de situaciones que puede ofrecer la práctica no podemos decir que en modo alguno se trata de la última palabra sobre la materia. De manera tangencial también traemos a la mesa algunos aspectos extralegales que, si bien no son de la competencia del Asesor Legal, no pueden pasar desapercibidos debido al carácter pragmático de esta Guía Legal. En todo momento sugerimos acudir y consultar su alcance

contenido con especialistas financieros, fiscales u operativos que puedan clarificar su contenido.

Finalmente queremos agradecer a los participantes revisores de este Proyecto, quienes nos apoyaron con sus comentarios y puntos de vista para efecto de que el contenido sirviera a un interés práctico y orientado a una lectura fácil.

Esperamos que, si esta Guía se vuelve útil para las Entidades y demás público interesado en el SACP, la misma vea ediciones futuras que reflejen tanto los cambios normativos que naturalmente se verán con el paso del tiempo, así como las experiencias de aquellos que usaron este documento como referencia en la planeación y desarrollo de Proyectos concretos de digitalización.

Ciudad de México a 1 de agosto de 2021

PARTE I: ASPECTOS GENERALES DE LA GUÍA

SECCIÓN 1.- INTRODUCCIÓN.

Esta Guía Legal pretende ser un documento de consulta práctica sobre los aspectos legales involucrados en los tipos de Proyectos de digitalización que consideramos más relevantes. México es parte de una revolución en la forma de prestar servicios financieros; en el habla común esto se conoce como "Fintech", un término que en un sentido amplio se refiere a la prestación de servicios financieros mediante aplicaciones informáticas. En términos estrictamente legales, a partir de la publicación y entrada en vigor el 9 de marzo de 2018 de la Ley para Regular las Instituciones de Tecnología Financiera ("Ley Fintech"), esa palabra suele aplicarse a las Instituciones de Tecnología Financiera ("ITF") en alguna de sus modalidades: Instituciones de Fondos de Pago Electrónico ("IFPE") o Instituciones de Financiamiento Colectivo ("IFC"), e incluso, por asociación, a los modelos novedosos. Es por lo anterior que nos abstendremos de utilizar el término Fintech en referencia a los Proyectos de digitalización aplicados al Sector de Ahorro y Crédito Popular ("SACP") y evitar cualquier confusión al respecto.

Esta reforma legal ha intensificado la competencia en el sector de los servicios financieros y, a la vez, presenta nuevos incentivos y oportunidades para que las Entidades del SACP destaquen en esta etapa de transformación digital.

Desde luego, México y el SACP tienen particularidades que, por diversas razones, aún impiden una digitalización completa de los servicios financieros. Asimismo, existen costos que no deben ser ignorados. Sin embargo, la digitalización también es importante para facilitar la viabilidad de los modelos de negocio de las Entidades y propiciar su crecimiento, a veces, exponencial. A nivel internacional, uno de los ejemplos más notables de digitalización es el del DBS Bank de Singapur: esta institución comenzó un proceso de digitalización que tomó cerca de diez años[2], lo cual implicó[3] (i) cambiar su enfoque, es decir, no sólo verse como una entidad financiera sino una empresa tecnológica, (ii) crear medidas de valuación de la empresa que reflejaran sus ventajas sobre sus competidores

[2] A 7-year digital transformation for this Singapore bank enabled its survival success in the world's new normal (Internet). Consultado en: https://www.businessinsider.com/singaporean-banks-7-year-digital-transformation-enabled-its-survival-2020-9?r=MX&IR=T

[3] Becoming more than a bank: Digital transformation at DBS (Internet). Consultado en: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/becoming-more-than-a-bank-digital-transformation-at-dbs#

en un entorno competitivo, y (iii) transformar su cultura de trabajo (ir de lo tradicional a una cultura basada en lo digital). Este ejemplo exitoso de transformación "total" contiene elementos que, gradualmente y dependiendo del modelo de cada Entidad, podrían tomarse como ejemplo y principios generales de aplicación.

Es indispensable considerar el siguiente elemento central que presupone la transformación digital: el financiamiento. Cada Proyecto requiere de una evaluación de viabilidad financiera y su debida presupuestación. Si bien las métricas y condiciones de financiamiento vienen fijados por factores normativos y las circunstancias específicas de cada Entidad, hemos incluido en esta guía las alianzas estratégicas (*joint ventures*) como una de las maneras en que se pueden implementar Proyectos materia de este documento, de modo que exista una distribución de costos efectivo entre dos o más partes. Mientras que el sector Fintech (en sentido estricto), dado su carácter original como *startup*, tiene mayor familiaridad con ciertos aspectos relacionados con el financiamiento a través de rondas de capital y atracción de inversionistas, creemos que la capacidad del SACP para colaborar con él es muy grande.

Ahora bien, el enfoque de este documento se refiere a aspectos estrictamente legales. Esto significa que, en ocasiones, se requerirá de experiencia y enfoques distintos para efecto de poder implementar cada Proyecto y que la administración del mismo puede requerir de planificaciones paralelas (aunque no desconectadas) en varias áreas de experiencia; es decir, cada elemento involucrado en un Proyecto requiere de una asesoría experta y adaptada a su ámbito. Por ejemplo, la creación de un programa informático o la contratación con un proveedor de tecnología contiene factores técnicos que son esenciales para el éxito y conclusión del Proyecto y requieren de una planeación y administración que no se encontrará en las páginas de esta Guía Legal.

En todo caso, dependiendo de las características de cada Entidad, cada Proyecto debe considerar, al menos, las siguientes expectativas:

(i) La seguridad de la información y los activos o salvaguarda de la integridad del cliente final;

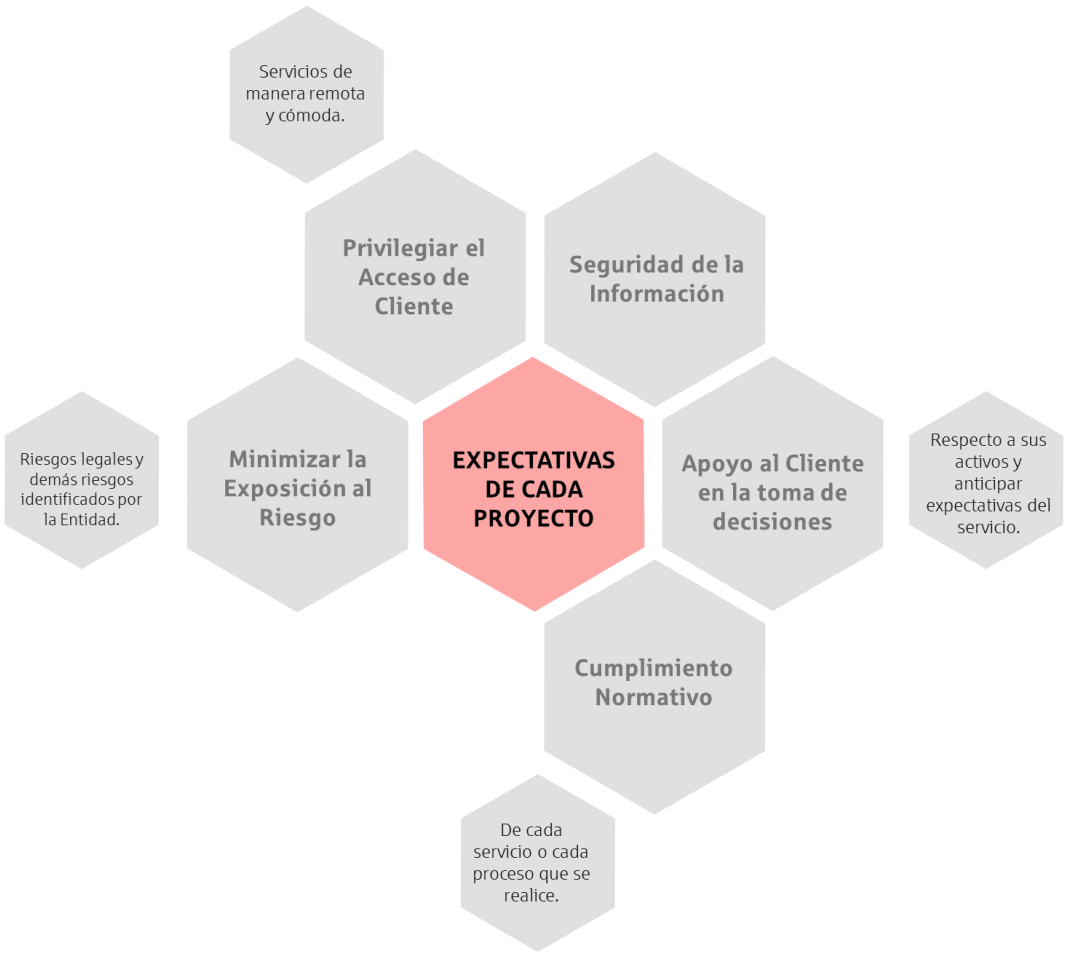
(ii) El cumplimiento normativo de cada servicio o proceso en todas sus etapas;

(iii) Minimizar la exposición a riesgos legales y demás riesgos identificados por la Entidad (operativos, financieros y tecnológicos principalmente);

(iv) Privilegiar el acceso del cliente a los servicios de manera remota y cómoda (tanto la contratación como el manejo del servicio); y

(v) En su caso, apoyar al cliente final a entender mejor las decisiones que puede tomar con los bienes o servicios tecnológicos puestos a su disposición, dependiendo de las características específicas de los mismos, y anticipar sus expectativas respecto al servicio. En aquellos Proyectos que sólo se refieren a la digitalización (en este caso propiamente se estaría hablando de "automatización"), el cliente no se refiere a un consumidor parte del público en general, sino al cliente interno, la persona que dentro de la Entidad estará a cargo de usar o beneficiarse del proceso automatizado.

Cuadro de expectativas de cada Proyecto



Gráfica 1. Cuadro de expectativas de cada Proyecto. Fuente: Vite Abogados

Por otra parte, metodológicamente hemos segmentado los Proyectos por secciones, lo cual permite al usuario de esta Guía Legal consultar directamente las que sean de su interés. También es posible que determinadas Entidades, de acuerdo con sus necesidades particulares, requieran una transformación digital profunda considerando varios frentes a la vez. Esto es llevar al máximo el potencial de digitalización y requeriría quizá de una aproximación distinta para integrar todos los procesos involucrados.

Comunicación, comunicación y más comunicación**.** En el Prólogo de esta Guía Legal hablamos de la necesidad de contar con canales de comunicación con los reguladores del SACP. Sabemos, empíricamente, que esa comunicación existe, es constante y su eficacia resulta útil para guiar procesos como los que son materia del presente documento. Sin embargo, no hay que perder de vista a los clientes, tanto internos como externos, de las Entidades. Los cambios pueden implicar disrupciones, transformaciones en rutinas, expectativas y contribuir a necesidades de nuevos comportamientos y actitudes. Recomendamos mantener canales abiertos para comunicar cualquier información relevante entre los interesados a fin de no afectar el trabajo ordinario de la Entidad o la relación con los clientes externos. Hay aspectos de los Proyectos que, por su naturaleza, deben permanecer confidenciales; sin embargo, recomendamos mantener siempre un intercambio abierto entre los involucrados para lograr una mejor asimilación de las transformaciones de la Entidad.

La presente Guía Legal se encuentra conformada por tres partes distintas. La parte I, conformada por esta Sección 1, plantea los aspectos generales de este documento: objetivos y limitaciones, la descripción del SACP, así como los reguladores de este sector. La parte II describe los antecedentes generales que las Entidades deben conocer para la administración adecuada de un Proyecto, tales como: partes responsables internas de una Entidad, aspectos de control interno y los manuales relevantes que una Entidad debe mantener actualizados, regulación en materia de transparencia y ordenamiento de los servicios financieros, regulación en materia de prevención de lavado de dinero y financiamiento al terrorismo (PLD/FT), aspectos relevantes en la prevención del fraude, aspectos generales sobre la seguridad, confidencialidad de la información y continuidad de la operación en las Entidades, así como regulación en materia de datos personales y secreto financiero. Por último, la parte III plantea distintas iniciativas de innovación financiera que las Entidades pueden considerar como los siguientes pasos para su actualización, tales como: banca electrónica y el uso de medios electrónicos, modernización del proceso crediticio y la digitalización del mismo, implementación de la

firma electrónica, apertura de cuentas vía remota, almacenamiento en la nube, aspectos relevantes en la contratación de proveedores y comisionistas, regulación para la contratación de prestadores de servicios operativos, uso de biométricos, medios de disposición, ingreso a los sistemas de pago, automatización de procesos, uso de Big Data, acercamiento a la banca abierta, creación de oportunidades de negocios en línea, alianzas con instituciones de tecnología financiera, proyectos para el manejo y conservación digital de la información, así como un acercamiento a la regulación de activos virtuales y a la tecnología *blockchain*.

1.1 Guía Legal: objetivos y limitaciones.

Utilidad es el principio rector del presente trabajo. Practicidad es su objetivo. Si bien este trabajo ha de abarcar los aspectos legales más relevantes de cada tipo de Proyecto, necesariamente hay limitaciones en cuanto a su alcance y consideraciones para cualquier usuario del mismo.

En cuanto a los objetivos que pretendemos alcanzar con la puesta a disposición de este documento al SACP y al público en general, nombraríamos los siguientes:

- Problematizar el universo normativo relevante respecto de Proyectos que tengan un impacto considerable en el SACP en el contexto de la digitalización de servicios y transmitir (i) la existencia de obstáculos legales detectados, (ii) la problemática práctica que, desde el punto de vista legal, enfrentan las Entidades del SACP, y (iii) proponer algunos enfoques que permitan solventar esos problemas.
- El impacto y la importancia de cada Proyecto seleccionado (y por lo tanto su posible inclusión en la Guía) se ha determinado con base en las siguientes prioridades: (i) relevancia del problema para un número considerable de receptores de la Guía Legal o mayor número de Entidades del SACP, (ii) viabilidad de una solución legalmente eficaz para la implementación de un Proyecto en la práctica, y (iii) accesibilidad del contenido técnico legal y precedentes en la materia.
- Comunicación clara de los conceptos legales a utilizarse, haciendo hincapié en las cuestiones de índole práctica para resolver cada tipo de problema planteado. Los conceptos que comiencen con letra mayúscula inicial o sea acrónimos o abreviaturas se encuentran en el Glosario del presente documento.
- Previsión e identificación de las variables que en la práctica pudieran afectar la implementación de cada solución propuesta.

- Uso de la terminología técnica de manera sucinta y uso de lenguaje claro y sencillo, en lo posible.
- Orientación sobre posibles fuentes de información pública o materiales que podrían ser relevantes en el contexto de la Guía.
- Recibir en todo momento retroalimentación práctica y visualizar nuestra audiencia como un público amplio y no necesariamente familiarizado en cuestiones técnicas o legales.
- Por otra parte, el usuario de esta Guía Legal debe considerar que, como todo documento de esta naturaleza, la misma tiene las siguientes limitaciones que las Entidades del SACP y el usuario deben considerar:
- El Asesor Legal, autor del contenido legal, no cuenta con experiencia o conocimientos en ingeniería, informática o de aspectos de carácter financiero, entre otras materias especializadas, por lo que cualquier omisión o ausencia respecto de dichos temas debe entenderse como una limitación natural de este trabajo y no por ello como un aspecto poco relevante o que deba dejarse de lado. Como se verá más adelante, las cuestiones informáticas y financieras pueden dictar en muchos casos la manera de conceptualizar un Proyecto de digitalización e influir en su éxito.
- Ni el Asesor Legal ni SPK seremos responsables por el resultado de Proyecto alguno realizado con base en esta Guía Legal, ni de cualquier decisión que cualquier persona tome basándose en su contenido. No otorgamos garantía ni hacemos representación alguna en ese aspecto y el lector asume su responsabilidad al respecto.
- Este documento es informativo, por lo que el lector entiende que se trata de un documento auxiliar y que la asesoría legal, financiera, operativa, entre otras, para llevar a buen puerto un Proyecto de digitalización en una Entidad es vital para su ejecución.
- Aunque hemos sido cuidadosos en señalar el universo normativo que consideremos más relevante para los aspectos legales de los procesos de digitalización, la identificación de normas relevantes o esenciales para cada Proyecto debe ser evaluada caso por caso por un profesional especialista en derecho financiero y que tenga toda la información relevante sobre la Entidad previo a cualquier ejecución.

- El presente documento es un apoyo para los encargados de aplicar o revisar los aspectos legales de un Proyecto de digitalización que involucre a las Entidades y no substituye en ninguna circunstancia la asesoría de un profesional del derecho para evaluar las necesidades, alcances y resultados de un Proyecto de digitalización.
- Los ejemplos prácticos o propuestas de solución no son únicas y estamos conscientes de la diversidad de aproximaciones y puntos de vista que pueden surgir para implementar y concluir exitosamente un Proyecto (no sólo a nivel legal sino en las demás áreas de experiencia que pudieran ser relevantes).
- La presente Guía Legal se realiza considerando el derecho aplicable a esta fecha. El SACP es dinámico y la velocidad con la cual cambian, se abrogan leyes y regulaciones o se derogan aspectos parciales de las mismas, es constante. Por lo anterior, es posible que existan conceptos, consideraciones o fundamentos que gradualmente vayan quedando obsoletos, sean poco relevantes a medida que pase el tiempo o que incluso contravengan total o parcialmente lo que aquí se expone. Adicionalmente, los criterios de las autoridades encargadas de regular y supervisar el SACP pueden modificarse en el tiempo, por lo que la interpretación de ciertos conceptos o procesos puede estar sujeta a modificaciones periódicas.
- Este documento no ha sido consultado ni aprobado por ninguna autoridad gubernamental, por lo que los puntos de vista legales expresados en el mismo no han sido consensuados en modo alguno con los reguladores, quienes podrían tener puntos de vista diversos a los expuestos.
- Tratamos de dar un enfoque práctico y, sobre todo, cuidadoso a la manera de plantear la problemática aquí expuesta, apegándonos, cuando es necesario, a principios de interpretación legal muy estrictos; sin embargo, ni SPK ni el Asesor Legal asumen responsabilidad alguna respecto a cualquier interpretación punto de vista que pudiera diferir de lo expresado por las autoridades financieras.
- Consideramos que las Entidades, como entidades financieras reguladas, requieren de un acercamiento constante, serio y cordial con sus reguladores para efecto de implementar varios de los Proyectos o aplicar las normas aquí presentadas. Invitamos a las Entidades o a las personas responsables dentro de las mismas a acercarse con sus reguladores a través de los canales que las autoridades pongan a su disposición y, en los casos en que sea necesario, desarrollar con su punto de

vista cualesquiera aspectos que consideren convenientes, poco claros o que, por su importancia e impacto, tengan repercusiones en su situación legal, operativa o financiera.

- Por otra parte, no hemos incluido referencias a metodologías o herramientas informáticas de seguimiento de los Proyectos, puesto que, en algunos casos, ello depende de las partes técnicas que estén involucradas en los mismos. Nuestro enfoque pretende ser orientador para efecto de que el profesional del derecho a cargo pueda desarrollar un plan adecuado para verificar que se está cumpliendo con los aspectos legales de los Proyectos.

1.2 El Sector de Ahorro y Crédito Popular.

Como se mencionó al principio, para efectos de esta Guía Legal, las Entidades que conforman el SACP mexicano son las siguientes:

1.2.1 Sociedades Financieras Populares

Las SOFIPO o sociedades financieras populares, son sociedades anónimas constituidas conforme a la Ley General de Sociedades Mercantiles ("LGSM") y que operan conforme a la Ley de Ahorro y Crédito Popular ("LACP"). Para poder operar como SOFIPO se requiere el dictamen favorable de una Federación y la autorización discrecional de la CNBV. Dichas autorizaciones son intransmisibles.

Estas Entidades se conceptualizan en algunos documentos de política pública como Entidades de "microfinanzas"[4]. Sin embargo, conforme a la regulación, ello no es necesariamente cierto, pues su objeto es más amplio y pueden involucrarse, en la medida permitida por la ley, en actividades consideradas como tradicionalmente asociadas a la banca comercial. Entre los servicios que pueden prestar las SOFIPO se encuentran:

- Recibir depósitos del público.
- Recibir préstamos y créditos de bancos, fideicomisos públicos y organismos internacionales, afores aseguradoras y afianzadoras, entre otros.
- Expedir y operar tarjetas de débito y tarjetas recargables.

[4] Sociedades Financieras Populares (Internet) Consultado en: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Preguntas-Frecuentes/Paginas/Sociedades-Financieras-Populares.aspx

- Otorgar préstamos o créditos a sus clientes.
- Recibir o emitir órdenes de pago y transferencias.
- Recibir pagos de servicios por cuenta de terceros.
- Realizar la compraventa de divisas en ventanilla por cuenta de terceros o propia.
- Distribuir seguros, fianzas, así como recursos de programas gubernamentales.
- Pueden captar dinero de sus clientes y ofrecer a cambio rendimientos.

Las SOFIPO tienen como límite a las actividades que puedan realizar (i) lo señalado en la LACP en cuanto al Nivel de Operaciones que les es aplicable y (ii) sus estatutos sociales aprobados por la CNBV en el momento de otorgar la autorización correspondiente y, en su caso, cualquier modificación subsecuente a los mismos aprobada por dicho regulador.

Las SOFIPO tienen dos clasificaciones que son importantes tomar en cuenta para establecer cualquier actividad, línea de negocio o incluso uno de los proyectos que son parte de esta Guía Legal:

- Nivel de Capitalización: es un indicador que sirve para determinar si son necesarias medidas correctivas mínimas y especiales adicionales que, en caso necesario, deberán cumplir las SOFIPO para efecto de preservar su viabilidad como tal. Entre las medidas correctivas se encuentran la abstención de realizar ciertas actividades, informar a su Consejo de Administración ciertos asuntos, presentar planes de restauración de capital o incluso remover funcionarios.
- Nivel de Operación: se trata de una clasificación en cuatro niveles de las SOFIPO para efecto de determinar el tipo de operaciones que pueden realizar, así como las características de las mismas. El criterio se basa, en principio, en los montos de activos totales de cada Entidad, así como del cumplimiento de requisitos que la CNBV ha establecido en la regulación secundaria.

1.2.2 Cajas de Ahorro o SOCAP

Las SOCAP (también conocidas como Cajas de Ahorro) son sociedades cooperativas constituidas y organizadas conforme a la Ley General de Sociedades Cooperativas ("LGSC"), independientemente del nombre comercial, razón o denominación social que adopten, son entidades que tienen por objeto realizar operaciones de ahorro y préstamo

con sus Socios y quienes formen parte del sistema financiero mexicano con el carácter de integrantes del sector social, sin ánimo especulativo y sin fines de lucro.

Las SOCAP que tengan registrado un monto total de activos igual o superior al equivalente en moneda nacional a 2'500,000 UDIS requieren de la autorización de la CNBV para realizar o continuar realizando operaciones de ahorro y préstamo. Aquellas que tengan un monto menor de activos no requerirán de dicha autorización, pero deberán apegarse a ciertos requisitos legales para operar.

Asimismo, existen otros Niveles de Operación compuestas de cuatro categorías: de la I a la IV. Cada Nivel de Operación depende del monto de activos que tenga la Entidad y ello permite a las SOCAP realizar operaciones con diversas características.

Las Cajas de Ahorro con un nivel de operación básico deben estar registradas ante el Fideicomiso del Fondo de Supervisión Auxiliar de Sociedades Cooperativas de Ahorro y Préstamo y de Protección a sus Ahorradores ("FOCOOP").

Las Cajas de Ahorro están autorizadas para captar recursos monetarios de sus Socios de conformidad con la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo ("LRASCAP").

Los servicios que ofrecen las Cajas de Ahorro a sus Socios son los siguientes:

- Recibir depósitos de dinero a la vista, de ahorro, a plazo, retirables en días preestablecidos y retirables con previo aviso, de sus Socios.
- Cuentas de ahorro con menores de edad, en términos de la legislación común aplicable, siempre y cuando sus padres o tutores sean socios y hasta por 1,500 UDIS.
- Otorgar préstamos a sus socios.
- Transmisión de dinero entre sus Socios
- Recibir créditos de entidades financieras nacionales o extranjeras, organismos internacionales, así como instituciones integrantes de la administración pública y federal o estatal y fideicomisos públicos.
- Efectuar la distribución y pago de productos, servicios y programas gubernamentales.

1.2.3 Sociedades Financieras Comunitarias

Las SOFINCO (Sociedades Financieras Comunitarias) son las sociedades anónimas constituidas y que operen conforme a la LGSM y la LACP, cuyo objeto social es predominantemente apoyar el desarrollo de actividades productivas del sector rural, a favor de personas que residan en zonas rurales. Asimismo, su actuación se rige por los principios de territorialidad, acción gremial, solidaridad y ayuda mutua. También se encuentran clasificadas por Nivel de Operación y tienen normas de aplicación común con las SOFIPO.

Existe, en el momento de escribir la presente Guía Legal, sólo hay una SOFINCO autorizada.

1.2.4 Organismos Autorregulatorios

Los Organismos Autorregulatorios son entidades de carácter privado que tienen por objeto implementar estándares de conducta y operación entre sus agremiados, a fin de contribuir al sano desarrollo de las SOFIPO. Dichos organismos podrán ser de diverso tipo acorde con las actividades que realicen y deben ser reconocidos con tal carácter por la CNBV.

Entre las funciones de estos Organismos Autorregulatorios se encuentran las de emitir normas relativas a requisitos de ingreso, políticas de contratación de los agremiados con clientes, revelación de información al público, código de conducta, establecimiento de procesos para adopción de normas, entre otros temas. Dichas normas autorregulatorias no pueden contravenir ni exceptuar a lo establecido en las leyes y disposiciones aplicables.

Existen, al momento de publicación de la presente Guía Legal, dos organismos autorregulatorios relacionados con el SACP y con las Sociedades Financieras de Objeto Múltiple ("SOFOM"): (i) la Asociación Mexicana de Sociedades Financieras Populares, A.C.; y (ii) la Asociación de Sociedades Financieras Mexicanas de Objeto Múltiple, A.C.

1.2.5 Federaciones y Confederaciones

Las Federaciones son instituciones de interés público, con personalidad jurídica y patrimonio propios, sin fines lucrativos y autorizadas por la CNBV para ejercer de manera auxiliar la supervisión de las SOFIPO en los términos de la LACP. Su propósito es revisar, verificar, comprobar y evaluar los recursos, obligaciones y patrimonio, así como que las

operaciones, funcionamiento, sistemas de control y en general, todo lo que pudiera afectar la posición financiera y legal de las SOFIPO, conste o deba constar en los registros, a fin de que se ajusten al cumplimiento de las disposiciones que las rigen y a las sanas prácticas de la materia.

Las Federaciones se auxilian de un Comité de Supervisión, órgano que las apoya en el cumplimiento de sus objetivos.

Todas las SOFIPO, ya sea por asignación de CNBV o, como ocurre en la mayoría de los casos, por afiliación voluntaria, se encuentran agremiadas en Federaciones.

Las Cajas de Ahorro, como sociedades cooperativas, podrán agruparse libremente en federaciones, uniones o en cualquier otra figura asociativa con reconocimiento legal. Dichas instituciones serán instituciones de interés público, con personalidad jurídica y patrimonio propios. Estas entidades podrán proporcionar servicios de asesoría técnica, legal, financiera y de capacitación, así como promover homologación de manuales, por procedimientos, reglamentos y políticas, y, por último, sistemas contables e informáticos, entre sus organizaciones afiliadas.

Existen, al momento de escribir la presente Guía Legal, las siguientes Federaciones y Confederación en operación para SOFIPO:

1. Fine Servicios, S.C.
2. Federación Victoria Popular, S.C.
3. Federación Atlántico Pacífico del Sector de Ahorro y Crédito Popular, A.C.
4. Federación Fortaleza Social, A.C.
5. Federación de Instituciones y Organismos Financieros Rurales, A.C.
6. Confederación de Cooperativas de Ahorro y Préstamo de México, S.C. de R.L. de C.V.

Existen, al momento de escribir la presente Guía Legal, las siguientes Federaciones y Confederación en operación para SOCAP:

1. Federación de Instituciones y Organismos Financieros Rurales, A.C.
2. Federación de Cajas Populares Alianza, S.C. de R.L. de C.V.
3. Confederación de Cooperativas de Ahorro y Préstamo de México, S.C. de R.L. de C.V.

1.2.6 Sociedades Financieras de Objeto Múltiple

Las "SOFOM" no son parte del SACP en un sentido estricto y su propósito e historia no están necesariamente vinculadas con el sector; sin embargo, por su presencia en el mercado crediticio consideramos oportuno hacer referencia a ellas, así sea tangencialmente, dentro de la presente Guía Legal. Estas entidades financieras están constituidas como sociedades anónimas (o, en su caso, sociedades anónimas promotoras de inversión) para cuyo funcionamiento no es necesaria una autorización emitida por CNBV, pero deben contar con un registro vigente ante CONDUSEF. Su objeto social preponderante es la realización habitual y profesional de una o más de las actividades de otorgamiento de crédito, arrendamiento financiero o factoraje financiero.

El tipo de SOFOM al que haremos referencia en el presente documento será el de SOFOM no regulada, es decir, aquella que no se encuentra en el supuesto de (i) tener vínculos patrimoniales con ciertas entidades financieras conforme a la Ley de Organizaciones y Actividades Auxiliares del Crédito ("LGOAAC"), (ii) haber solicitado voluntariamente regularse como tal (previo el cumplimiento de ciertos requisitos), y (iii) aquellas que emitan valores de deuda a su cargo, inscritos en el Registro Nacional de Valores conforme a la Ley del Mercado de Valores ("LMV")[5].

[5] Conforme a la LGOAAC se considerarán sociedades financieras de objeto múltiple reguladas aquéllas que emitan valores de deuda a su cargo, inscritos en el Registro Nacional de Valores conforme a la Ley del Mercado de Valores, o bien, tratándose de títulos fiduciarios igualmente inscritos en el citado Registro, cuando el cumplimiento de las obligaciones en relación con los títulos que se emitan al amparo del fideicomiso dependan total o parcialmente de dicha sociedad, actuando como fideicomitente, cedente o administrador del patrimonio fideicomitido, o como garante o avalista de los referidos títulos.

Miembros del SACP y las SOFOM

Gráfica 2. Miembros del SACP y las SOFOM. Fuente: Vite Abogados

¿Qué tipo de Entidad necesito?

Para efectos de esta Guía Legal, hemos asumido que el Usuario sabe y conoce lo que hemos presentado anteriormente. Sin embargo, si el lector de este documento es una persona interesada en constituir y operar algunas de los tipos de Entidades descritos y mencionados anteriormente, tenemos las siguientes recomendaciones:

- Identificar Actividades Reguladas. Identificar las actividades o servicios financieros que requieren de una licencia o autorización. En específico establecer si requieren llevar a cabo "captación" o "intermediación bancaria" que consiste en la captación de recursos del público en el mercado nacional para su colocación en el público, mediante actos causantes de pasivo (obligaciones de pago) directo o contingente, quedando, el intermediario, obligado a cubrir el principal y, en su caso, los accesorios financieros de los recursos captados. Conforme al artículo 2 de la Ley de Instituciones de Crédito ("LIC"), se considera que existe captación de recursos del público cuando: a) se solicite, ofrezca o promueva la obtención de fondos o

recursos de persona indeterminada o mediante medios masivos de comunicación o b) se obtengan o soliciten fondos o recursos de forma habitual o profesional.

- Excluyendo a las SOFOM, las demás Entidades tratadas en esta Guía Legal pueden legalmente realizar la captación sujeta a ciertas condiciones y a su régimen aplicable.
- No obstante, el ofrecimiento habitual o profesional de operaciones de crédito por parte de sujetos distintos a las entidades financieras, no requiere de una licencia ni de una autorización gubernamental, aunque sujeta a las personas que la realizan a ciertas obligaciones frente a la SHCP, ya que se trata de lo que se conoce como una "actividad vulnerable". Las SOFOM no son la única manera de prestar servicios crediticios y, si bien son una entidad pensada con ese objeto (además de otorgar arrendamiento y factoraje financiero), la adopción de ese régimen debe obedecer a una planeación fiscal y legal cuidadosa.
- Asimismo, cualquier tema que involucre valores, recepción de fondos, pago de intereses o dar la apariencia de que se actúa como entidad financiera, generalmente va a requerir la autorización o registro ante algún Regulador.
- Revisar el Tipo de Entidad. Los asesores legales, por lo general, no se pronuncian sobre cuestiones relacionadas con la viabilidad financiera y los modelos de negocio de una sociedad de nueva creación; sin embargo, debe involucrárseles en el diseño de los productos y servicios para que pueda verificar qué tipo de entidad puede prestarlos y los requerimientos respectivos.
- Este punto es relevante, entre otras cosas, por lo siguiente: en el caso de ciertas Entidades, como las SOCAP, la regulación establece reglas distintas para adquirir los certificados de aportación social que no tienen valor nominal, además de que existen prohibiciones para su adquisición. Existen reglas especiales para representar a los socios de las SOCAP, por lo que a estas Entidades no le son aplicables las reglas normales de adquisición de participación y representación del capital social a que se refiere la LGSM.
- Modelo de Negocio. Una vez identificado el tipo societario o legal que conviene al plan de negocio y establecida la viabilidad legal de prestarlo a través de alguna Entidad en específico, es necesario preparar las proyecciones de viabilidad financiera. Para ello, el abogado o especialista a cargo deberá asesorar sobre la normatividad aplicable para cada tipo de servicio, sobre todo, aquellas que se

refieran a las reglas contables o financieras que pudieran aplicarle al tipo de Entidad seleccionado. Recordemos que las Entidades son sociedades altamente reguladas y que su contabilidad y reglas financieras están establecidas en la ley y las normas secundarias, por lo que cualquier proyección debe tomarlas en cuenta.

- Buscar Información. Como lo mencionamos, existen entidades y agrupaciones para cada tipo de Entidad, tales como las Federaciones o agrupaciones gremiales. Pese a que la tarea de estas entidades no es la de fungir como asesores de posibles Entidades en sentido estricto, sino fungir como organismos auxiliares en la supervisión de las Entidades, estas agrupaciones típicamente conocen las problemáticas prácticas del SACP y pueden orientar muchas decisiones futuras. Asimismo, su información y experiencia resultan ser muy valiosas para presupuestar un Proyecto o la creación de una nueva Entidad.

- Adquirir o Comprar. Un dilema frecuente el de constituir una Entidad o adquirir participación accionaria en Entidades ya constituidas y autorizadas para operar. No existe una respuesta unívoca, pero los factores que deben considerarse, al menos desde el punto de vista legal, son (i) la regulación en materia de transmisión de acciones de las Entidades que, en porcentajes importantes, implica la intervención o autorización de CNBV, (ii) la realización de auditorías fiscales, legales (corporativa, contractual y regulatoria), operativas, financieras y laborales y de seguridad social a la Entidad cuyas acciones se desee adquirir, (iii) el tiempo estimado para echar a andar el plan de negocio propuesto, pues, por regla general, la adquisición tiende a ahorrar tiempo, (iv) las negociaciones con los accionistas originales, y (v) la posibilidad de adquirir participación en las Entidades, ya que algunas de ellas, como las SOCAP, no admiten la adquisición o compraventa de su participación en un sentido estricto debido a su carácter de "cooperativa".

- Establecer un Plan de Trabajo. Tomada alguna decisión sobre el camino a seguir, será necesario establecer un plan de trabajo y un cronograma que ayude a trazar la ruta crítica para lograr operar como una Entidad. Estos documentos deben reflejar tiempos realistas para cada etapa y ser flexibles, pues aun cuando existen tiempos legales acotados para los procesos de adquisición-venta de acciones o constitución-operación de Entidades, en la práctica la preparación y aprobación por CNBV de los documentos puede tomar cierto tiempo, pues hay que considerar las revisiones económicas o internas de los documentos. Este plan de trabajo debe tomar en cuenta las guías que ha emitido CNBV respecto a las autorizaciones de

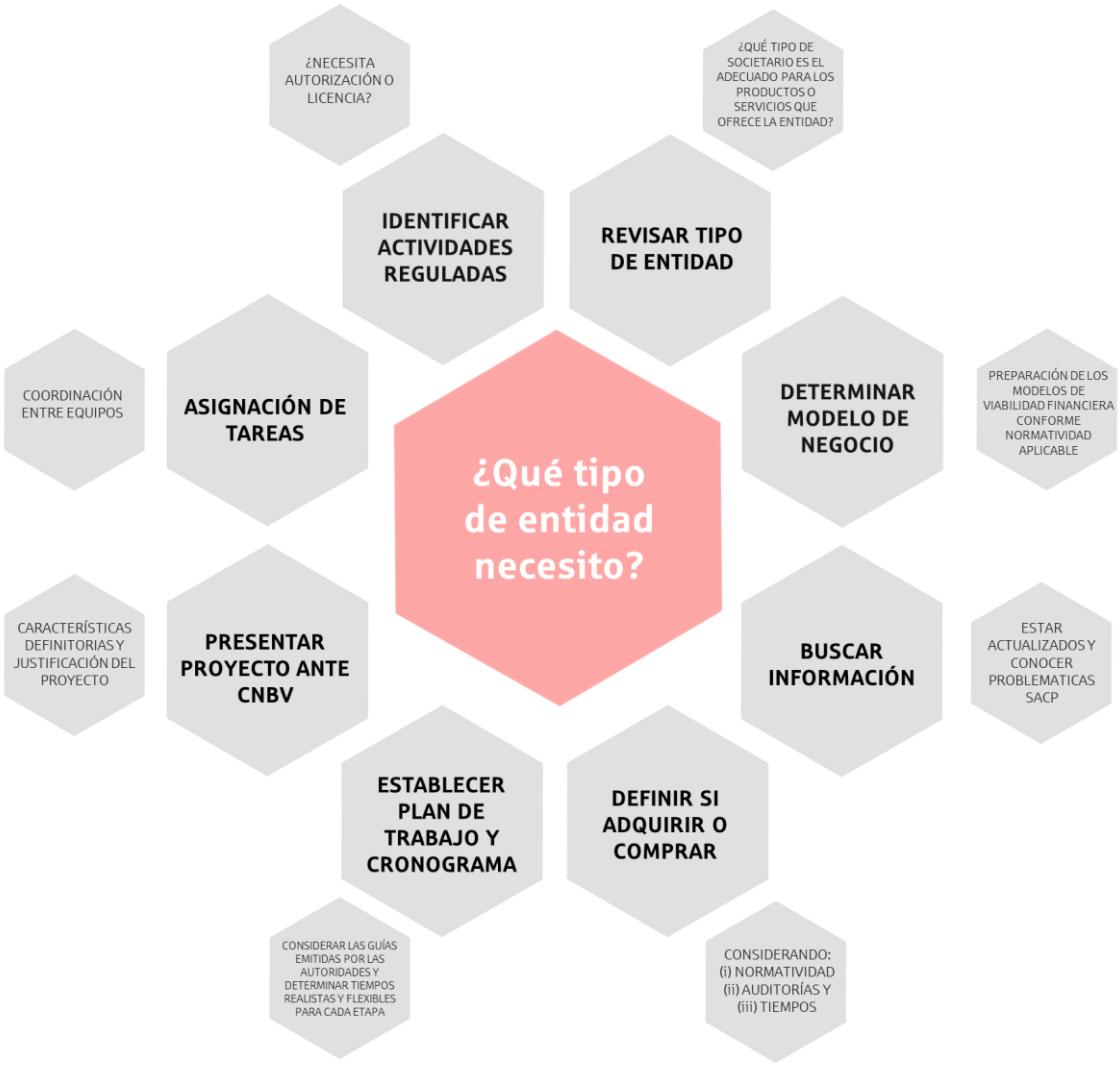
las Entidades y debe incluir la participación de los terceros relevantes para la tarea; por ejemplo, prestadores de servicios tecnológicos y accionistas, y directivos relevantes. Se trata de un documento consensuado y realista que, si bien se guía por los requerimientos legales, debe ser aprobado y comprendido por las demás áreas encargadas de llevar a término el proyecto.

- Presentación ante CNBV. La constitución y puesta en marcha de una Entidad es un proceso que involucra, sobre todo, a la CNBV, por lo que es necesario presentar el Proyecto ante dicho organismo para establecer una relación cordial con el regulador y conocer sus puntos de vista sobre el modelo de negocios. No existe una regla general sobre el momento en que debe ocurrir este acercamiento, pero recomendamos hacerlo cuando exista un avance importante sobre las características definitorias y la justificación del proyecto. Conforme a las guías de autorización, debe prepararse una presentación que incluya los puntos más relevantes de la nueva Entidad.

- Asignación de Responsabilidades. La administración de los Proyectos de creación de nuevas Entidades no es sencilla y requiere mucha coordinación entre los distintos equipos que estarán a cargo del proyecto. Sugerimos el uso de herramientas informáticas para administrar este tema y poder intercambiar de manera adecuada la información. El equipo principal generalmente se conforma de: (i) un encargado interno del proceso, que agrupa la información que se genera por la futura Entidad y los proveedores externos, y mantiene una comunicación abierta con los futuros accionistas y directivos; (ii) el asesor legal que debe ir guiando sobre los documentos necesarios, su alcance y, en su caso, algunos contenidos; (iii) una persona encargada de la implementación técnica-informática; y (iv) el creador y responsable de dar seguimiento al plan de negocios. Desde luego, estos roles se pueden traslapar, y es común que así sea, pero son aspectos que recomendamos tener muy en cuenta en este tipo de proyectos.

- Escoger la forma legal equivocada puede tener consecuencias adversas: los costos, los tiempos y las consecuencias sobre los accionistas y gente relacionada hace que esto sea una cuestión de primera importancia.

Evaluación del tipo de Entidad que necesito



Gráfica 3. Evaluación del tipo de Entidad que necesito. Fuente: Vite Abogados

1.3 Regulación y Reguladores del Sector de Ahorro y Crédito Popular.

Reguladores del SACP

Gráfica 4. Reguladores del SACP. Fuente: Vite Abogados

1.3.1 Comisión Nacional Bancaria y de Valores (CNBV)

La CNBV es un órgano desconcentrado de la SHCP, con facultades en materia de autorización, regulación, supervisión y sanción sobre los diversos sectores y entidades que integran el sistema financiero en México, así como sobre aquellas personas físicas y

morales que realicen actividades previstas en las leyes relativas al sistema financiero, incluyendo el SACP.

La CNBV se encarga, principalmente, de autorizar la operación de las Entidades[6], supervisar su operación así como declarar o intervenir en su liquidación o revocación. Adicionalmente, la CNBV tiene a su cargo emitir normas secundarias en relación con lo establecido en la LACP y la LRASCAP que incluyen temas de operación y funcionamiento, gobierno corporativo, operaciones entre partes relacionadas, reglas de reportes legales y contables. CNBV tiene la facultad de realizar visitas y ejercer funciones de inspección y vigilancia sobre las Entidades, autorizar la transmisión de acciones representativas del capital social de las Entidades y solicitarles información sobre sus actividades, supervisar y autorizar contrataciones con terceros que tengan ciertas características (tal como se explica posteriormente), entre otros temas. Muchos de las cuestiones mencionadas serán de relevancia para algunos de los proyectos que presentaremos en la presente Guía Legal.

1.3.2 Secretaría de Hacienda y Crédito Público (SHCP)

La SHCP es una dependencia de la Administración Pública Centralizada[7] que, para efectos de la presente Guía Legal, ejerce un papel relevante por lo que respecta a:

- La interpretación de las leyes financieras, de las cuales la LRASCAP y la LACP forman parte. Si bien corresponde a CNBV dar cumplimiento a muchos aspectos de las leyes financieras, en caso de oscuridad, silencio o falta de claridad, la única facultada para "interpretar para efectos administrativos" dichos ordenamientos es la SHCP, tal como lo establece el artículo 6 de la LRASCAP y el artículo 4 de la LACP.
- Emisión de normas en materia de prevención de lavado de dinero y financiamiento al terrorismo (PLD/FT), que son emitidas por SHCP y cuya administración y vigilancia comparte con CNBV.
- Dar su opinión en aquellos casos que la CNBV lo solicite o la ley lo determine.
- Intercambiar información sobre el SACP y las Entidades con otras entidades gubernamentales y coordinar esfuerzos con ellas.

[6] Salvo por lo que respecta a SOFOM y aquellos casos en que las Cajas de Ahorro no requieren de la misma.

[7] Que se conforma por la Oficina de la Presidencia de la República, las Secretarías de Estado, la Consejería Jurídica del Ejecutivo Federal y los Órganos Reguladores Coordinados integran la Administración Pública Centralizada.

- Hacer efectivas las multas que imponga la CNBV a las Entidades.
- Elaborar programas sectoriales respecto del SACP y promover la participación en el sector.
- Constituir el FOCOOP.

1.3.3 Banco de México

Banco de México o, como se le conoce comúnmente, "Banxico", es un organismo constitucionalmente autónomo que tiene como objetivo prioritario preservar el valor de la moneda nacional a lo largo del tiempo. Dentro de las funciones relevantes de esta autoridad dentro del sector financiero se encuentra la de regular ciertos aspectos que competen al SACP, por ejemplo: montos de pago mínimos aplicables a créditos, información que deben entregar a las sociedades de información crediticia (buró de créditos), pagos mínimos de tarjetas de crédito, Ganancia Anual Total, Costo Anual Total y cobro de intereses por adelantado, así como reglas de los sistemas de pagos, entre otros.

1.3.4 Condusef

Condusef es un organismo público descentralizado que depende de SHCP. Tiene dos líneas de actuación definidas: las preventivas y las correctivas. Dentro de las primeras está la promoción de la educación y orientación financiera al público en general y dentro de la segunda se encuentra la atención y resolución de quejas de usuarios de servicios financieros.

Desde el punto de vista normativo, Condusef es relevante para el SACP en atención a que está encargada de administrar y aplicar una parte importante de las disposiciones de transparencia y ordenamiento de los servicios financieros, así como emitir la reglamentación correspondiente para temas como contratos de adhesión, publicidad de los servicios financieros, publicidad de comisiones y servicios financieros, despachos de cobranza, entre otros. Las Entidades están obligadas, de manera periódica, a realizar validaciones y entregar información a los diversos registros que administra CONDUSEF (SIPRES, RECO, REDECO, REUNE), así como a realizar su publicidad conforme a la normatividad emitida por ese organismo.

1.3.5 INAI

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo constitucional autónomo garante del acceso a la información pública y el de protección de datos personales.

Para efectos de esta Guía Legal, garantizar el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información, son aspectos que deben cuidarse en cada Proyecto.

En ese sentido, el INAI, aunque no es una autoridad financiera como las mencionadas anteriormente, tiene la facultad de verificar y vigilar el cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares ("LFPDPPP"), interpretarla, emitir criterios y recomendaciones en materia de datos personales y resolver procedimientos de protección de datos, entre muchos otros, lo cual atañe directamente a las Entidades en virtud de que sus Usuarios suelen ser personas físicas en su mayoría.

PARTE II. ANTECEDENTES GENERALES.

SECCIÓN 2.- ASPECTOS GENERALES DE LA ADMINISTRACIÓN DE UN PROYECTO LEGAL.

Existen casos donde es necesario que los asesores legales tengan el papel central dentro de un Proyecto.

Un Proyecto es "un esfuerzo temporal emprendido para crear un producto, servicio o resultado único"[8]. Por regla general, todos los proyectos comparten tres características:

- Punto de inicio y punto final definidos.
- Temporalidad.
- Son novedosos o buscan innovar.

Los Proyectos de digitalización expuestos en esta Guía Legal comparten esas características. No debe confundírseles con “procesos”, como lo serían, por ejemplo, la serie de pasos que se siguen en la implementación de un proyecto cualquiera: en ese aspecto, el Proyecto, una vez implementado, suele estar compuesto de una serie de procesos que se vuelven parte de la rutina y se incorporan al día a día de las Entidades.

El *Institute of Legal Project Management* proporciona un enfoque estructurado para la administración de proyectos de carácter legal[9],

A. Definición del proyecto.
B. Planificación del Proyecto.
C. Entrega del Proyecto.
D. Cierre del Proyecto.

Se trata, sin duda, de principios básicos de administración de proyectos de carácter legal. El reto tanto del Administrador del Proyecto como de las partes involucradas, es concretarlo sin perder de vista que existe un componente tecnológico que debe tomarse en cuenta en todo momento.

[8] Project Management Institute (Internet) Consultado en: https://valorganado.com/es/content/468-proyecto
[9] Applied Legal Project Management (Internet) Consultado en: https://legalprojectmanagementelearning.com

A continuación, describimos cada una de las etapas y nuestra sugerencia sobre la manera de adaptarlas a las necesidades de cada Proyecto.

A. Definición del Proyecto

Si el Proyecto y su alcance legal no se definen adecuadamente, cualquier intento posterior de planificarlos y gestionarlos podría generar contingencias o efectos no deseados en las Entidades. La administración exitosa de proyectos tiene que ver con la estructura, pues la necesidad de contar con cierta flexibilidad y no perder de vista los factores reales de cada Entidad es de suma importancia, en especial, el factor humano, que incide de manera importante en los tiempos y resultados de cada tarea.

La definición del proyecto debe partir de lo siguiente:

- Tipo de Proyecto e identificación de la normatividad aplicable.
- Partes involucradas (áreas técnicas, financieras, tecnológicas, áreas internas o proveedores, etcétera).
- Identificación de requisitos internos conforme a la normatividad aplicable.
- Establecimiento del alcance del Proyecto, contemplando: áreas impactadas, cliente interno y externo, procesos a implementar o relacionados con la finalidad del Proyecto.
- Objetivos que cumplan con las siguientes características[10]:
  - Específicos: que se circunscriba a un aspecto, tarea o acción determinada.
  - Medibles: a través de una metodología de análisis que posibilite saber en qué medida se alcanzan los objetivos.
  - Alcanzables: que las circunstancias permitan que sean perfectamente realizables dentro de los tiempos programados para finalizar el Proyecto.

[10] KNÖL, Esteban. Objetivos SMART: qué son y cómo utilizarlos. (Internet) Consultado en: https://www.titular.com/blog/objetivos-smart-que-son-y-como-utilizarlos.

- Relevante: definir objetivos que se relacionen y sean subsidiarios al objetivo general de la Entidad.
- Temporales: que se encuentran limitados por un lapso de tiempo determinado.

- Establecer las limitaciones del Proyecto para eliminar cuestiones adicionales o posteriores y que no inciden directamente en el logro del objetivo final.

Desde luego, estos son puntos de partida para la investigación inicial, de modo que el Administrador del Proyecto y las áreas involucradas identifiquen, discutan y definan el alcance del Proyecto.

En esta etapa se recomienda la generación de formatos o matrices donde se plasme la estructura seleccionada y que se denominará "Esquema de Proyecto". Esto ayudará en la etapa de planeación y, también, a guiar las discusiones preliminares. Asimismo, será una herramienta indispensable para encauzar mejor los esfuerzos y ser más eficientes con el tiempo en las juntas o conferencias.

Los campos que recomendamos incluir en este documento son los siguientes:

- Nombre de la Entidad.
- Nombre del Proyecto.
- Tipo de proyecto (por ejemplo "Automatización de Procesos Crediticios").
- Partes responsables incluyendo: nombre, organización, correo electrónico y un teléfono para localizarlos (sobre todo si se involucran personas externas).
- Hechos relevantes: antecedentes, datos de competidores, datos de regulación aplicable, cambios en el organigrama de la Entidad, nueva asignación de funciones, identificación de Proyectos semejantes en otras Entidades, entre otros.
- Aspectos legales, financieros y operativos relacionados con el proyecto.
- Objetivos del Proyecto: se sugiere se redacten por el área que estará a cargo de implementarlo.

- Supuestos: estos son eventos o circunstancias que espera que ocurran durante el desarrollo del Proyecto y que de no ser ciertos o exactos podrían impactar negativamente el análisis de la viabilidad del mismo y su resultado final.
- Restricciones: problemas que probablemente afecten la actividad del equipo responsable del Proyecto, ya sean de carácter humano, operativo o financiero.
- Exclusiones: aspectos que no serán cubiertos como parte de este Proyecto.
- Listado de requisitos. Esto solo necesita expresarse a un alto nivel en esta etapa, pero debe explicar lo que se requiere para lograr los objetivos del cliente. En este caso generalmente se derivan de la normatividad aplicable.
- Declaración del alcance. Esto explica el trabajo que será necesario realizar para cumplir con los requisitos, que a su vez deben estar orientados a intentar alcanzar los objetivos proyectados.
- Entregables. Estos deben incluir fechas de entrega ajustadas a los objetivos.
- Evaluación de riesgos. Aquí se enumeran los principales riesgos que podrían afectar negativamente al proyecto. En esta parte también se deben especificar los aspectos más importantes para mitigar los riesgos identificados.
- Plan de información. Aquí se enumeran las partes responsables y se menciona la información que deben obtener o que debe proporcionárseles, la manera en que se comunicará la información y la frecuencia con la cual se llevará a cabo el seguimiento y supervisión de cada etapa.
- Responsabilidades de los miembros del equipo a cargo del Proyecto, alineadas con los objetivos y etapas del mismo.
- Resultados. Establecer expectativas realistas y medibles de lo que se espera del Proyecto.
- Presupuesto. En este punto habrá que hacer ajustes relativos al tema. De cualquier forma, la Entidad debe comenzar a solicitar información sobre los costos que estarán involucrados en cada Proyecto. A pesar de que el enfoque final que se le dé al Proyecto tendrá un impacto decisivo en esta parte, por lo menos este tema debe quedar plasmado de manera preliminar y aceptable para la Entidad y sus accionistas o Socios.

B. Planificación del Proyecto.

El Esquema de Proyecto no es el único documento que debe guiarnos durante el Proyecto. En ciertos casos, es recomendable contar con documentos secundarios donde se detallen las tareas pendientes, por ejemplo, documentos donde se asignen tareas y objetivos específicos a las Partes Responsables y un cronograma donde se detallen los tiempos y las etapas que deberán irse cumpliendo para alcanzar los objetivos.

Las Entidades son sociedades complejas, lo cual implica que cualquier cambio en su organización, ya sea por un proyecto de digitalización o cualquier otro, tiene consecuencias en su manera de operar y en la continuidad de sus procesos. En ese sentido, es necesario que la planificación tome en cuenta también los procesos operativos y que se involucre en todo momento a las áreas que podrían verse afectadas.

C. Entrega de proyectos

En esta etapa es donde se compara el trabajo realmente completado con el trabajo que se planificó. En términos generales, hay ciertos elementos en este proceso de seguimiento que deben ir de acuerdo con el cronograma:

- Pruebas de la realización de las tareas asignadas.
- Calidad de lo entregado.
- Entrega dentro de los plazos acordados.
- Evaluación del costo y beneficio de lo entregado.
- Evaluación de la gestión del Proyecto.

Si un Proyecto no se está entregado dentro de las fechas que corresponden, entonces ello debe declararse en el informe de actualización regular del Proyecto o en los reportes de seguimiento que se realicen de tiempo en tiempo. El Administrador del Proyecto debe tomar las medidas necesarias para efecto de asegurarse que no existan nuevos retrasos, o bien, en caso de haberlos, identificar las causas y aplicar las medidas de mitigación que sean necesarias.

Es importante que el Administrador del Proyecto (AP) cuente con el apoyo del Director General o del Consejo de Administración para efecto de tomar las medidas que considere adecuadas. A menudo es posible que, por existir poca claridad en cuanto la función del AP, éste no tiene la autoridad para tomar medidas adecuadas tendientes a corregir el rumbo del Proyecto. Es común que existan muchos factores que no se hayan podido prever a lo largo de un Proyecto: entregas a destiempo de proveedores, consultas con reguladores o terceros que sufren algunos retrasos, etc., cuestiones que implican la reelaboración, en alguna medida, de los documentos originales de planeación del proyecto. Desde luego, esta autoridad del Administrador del Proyecto debe consensuarse con las demás Partes Responsables, para efecto de que sus acciones sean viables y no existan fricciones o se generen circunstancias que hagan inviable la reconducción del Proyecto.

Es importante que todas las Partes Responsables puedan verificar el avance del proyecto. Esto evitará malentendidos y permitirá ahorrar tiempo en reuniones innecesarias. Idealmente, debe existir una lista de documentos (*checklist*) que recomendamos tenga las siguientes características:

- Descripción de entregables.
- Fecha de entrega.
- Parte Responsable a cargo de cada documento (en algunos casos puede tratarse de corresponsables).
- Estado del documento.

La forma final de la lista de documentos dependerá de las características del Proyecto. De cualquier forma, su distribución y actualización continua es una herramienta que permite medir el avance y ahorrar tiempo.

En algunos casos, si se cuenta con herramientas informáticas para administrar un proyecto (un tema que trataremos más adelante), incluso existe la posibilidad de verificar y distribuir alertas basadas en hitos o metas que deben cumplirse en distintas fechas, y que permiten a todos consultar el estado del Proyecto, al igual que verificar si existe un retraso importante o sensible. Estas alertas también ahorran mucho tiempo, pues permiten visualizar un problema de manera inmediata y así tomar medidas correctivas rápidamente.

D. Cierre del Proyecto

La terminación o cierre del Proyecto variará dependiendo de su naturaleza: en algunos casos, su terminación estará marcada por la emisión de una autorización, oficio o registro emitido por los Reguladores. En otros casos, por la implementación efectiva a nivel operativo y tecnológico. Es importante que las Partes Responsables aprueben el resultado obtenido y tengan como completado el proyecto de conformidad con sus objetivos; un formulario de aceptación, un acta de entrega o un documento relacionado es suficiente para hacerlo. En algunos casos, dependiendo de la relevancia del proyecto, se sugiere incluso presentar la terminación al Consejo de Administración, sobre todo en aquellos casos que, ya sea por regulación o por su relevancia, deben ser monitoreados por ese órgano.

Asimismo, el cierre implica también la revisión de los resultados del Proyecto. Esto implica revisar, a través del Administrador del Proyecto y de un tercero no relacionado con éste, evaluar la documentación realizada y, en su caso, verificar que los procesos informáticos ya se encuentren funcionando y operativos. Asimismo, se tienen que comparar los objetivos con los resultados a la vista, esto en algunos casos puede tomar tiempo. Algunos parámetros de evaluación comunes son los siguientes:

- Verificar si se cumplieron los objetivos del Proyecto.
- Consultar a las Partes Responsables sobre la calidad de entregables, en cuanto a tiempo de entrega y alcance.
- Hacer un recuento de los problemas del Proyecto y evaluar si los mismos pudieron ser superados adecuadamente.
- Identificar las estrategias que resultaron más ventajosas y funcionales.
- Identificar las cuestiones que deben realizarse de manera diferente en Proyectos futuros similares.

En algunos casos será necesario proponer e implementar un tiempo de transición, por ejemplo, si se remplaza un sistema automatizado en materia PLD/FT, la transición puede tomar tiempo. En ocasiones es menester realizar un plan por separado para finalizar esta implementación y no realizar la disrupción en las actividades de cada área de la entidad.

» *Proyectos que necesitan proyectos*

En alguna ocasión, el Asesor Legal estuvo a cargo de coordinar los procesos de remediación en materia de PLD/FT de una institución de banca múltiple que, por motivos de confidencialidad, llamaremos "Banco Zeta". Banco Zeta, una entidad especializada en créditos corporativos, llamó al Asesor Legal para pedirle que llevara a cabo las siguientes tareas:

- Revisión de los expedientes de "conocimiento del cliente" o Know your Customer ("KYC" por sus siglas en inglés) de todos los acreditados de Banco Zeta.
- Determinación de los elementos que faltaban en cada uno de los expedientes KYC conforme a las políticas del banco y la regulación aplicable.
- Apoyar a Banco Zeta en la preparación de cartas dirigidas a sus clientes solicitando los elementos faltantes.
- Alimentar el sistema automatizado PLD/FT de Banco Zeta con el fin de actualizar la base de datos y, en su caso, subir la nueva información enviada por los clientes que atendieran la solicitud realizada por Banco Zeta.
- Coordinar los esfuerzos para certificar la suficiencia de los expedientes que fueran regularizados.

El Proyecto se concluyó de manera satisfactoria y dentro de los tiempos acordados; sin embargo, existieron diversos elementos que no fueron planeados ni atendidos por Banco Zeta que complicaron el desarrollo de lo planeado:

- Las plantillas de llenado de información (donde se establecía el tipo de información y documentos que habría que buscar en cada Expediente KYC dependiendo del tipo de cliente) fueron realizadas por el Asesor Legal, a pesar de que ello no se encontraba en la descripción de sus actividades. No existía un diagnóstico adecuado de lo que debía buscarse en cada expediente y, en ese sentido, el Asesor Legal tuvo que desviarse de los objetivos iniciales para poder atender este tema.
- Los expedientes no se encontraban digitalizados en su totalidad, por lo que en muchos casos el manejo de los mismos tenía que hacerse de manera física, lo cual

resultaba inconveniente por varias razones: (i) falta de practicidad para ubicar la sección donde debía encontrase la información del Expediente KYC, (ii) el tráfico de documentación sensible que, en algunos casos, podía incluir pagarés u originales que podían dañarse o perderse durante los trayectos de entrega (la mayoría estaba almacenado en una bodega), y (iii) el tiempo que consumía revisar expedientes físicos afectaba de manera importante las métricas de cumplimiento (número de expedientes revisados, tiempo de entrega, entre otros).

- El Sistema Automatizado de Banco Zeta estaba conectado, de algún modo, con otros sistemas de esa entidad y el acceso que se tuvo al mismo, en ocasiones, dificultaba el cumplimiento de otros procesos de Banco Zeta por los cambios que tenía que realizar el equipo del Asesor Legal a las bases de datos.
- No se había nombrado a un Director General en Banco Zeta, por lo que la responsabilidad en la toma de decisiones se tornaba difusa y no existía un control adecuado para ello. Por ejemplo, no había una dirección clara sobre la manera en que habría que buscar a los clientes para que entregaran información faltante o el establecer un sistema de seguimiento adecuado que no afectara las funciones informales de las áreas de venta (que fueron asignadas para enviar las cartas).

En ese sentido, el objetivo parecía muy claro: identificar faltantes de Expedientes KYC, alimentar la base de datos de Banco Zeta para actualizarla y solicitar la información. Sin embargo, consideramos que dicho Proyecto, a pesar de haberse concluido con éxito, requería las siguientes consideraciones adicionales:

- Un diagnóstico adecuado de la situación de los sistemas de Banco Zeta y de cómo un proceso de remediación podría afectar las actividades ordinarias del banco.
- La falta de un enlace efectivo entre el Asesor Legal y la dirección de Banco Zeta, lo cual retrasaba la toma de decisiones significativamente.
- La falta de una métrica adecuada sobre los tiempos que tomaba a cada persona contratada por Banco Zeta la revisión de cada Expediente y el llenado de la base de datos.
- La falta de herramientas informáticas (en este caso una plantilla que pudiera servir para reportar faltantes y generar automáticamente la carta de seguimiento) para poder facilitar las tareas.

En resumen: previo a realizar un proyecto como el referido, Banco Zeta debió completar varios pasos anteriores para evitar dilaciones y, sobre todo, hacerlo más eficiente desde el punto de vista del tiempo y los recursos asignados para su conclusión.

2.1 Identificación de Aspectos Esenciales.

En la sección anterior de esta Guía Legal, identificamos la estructura general de la administración de proyectos, incluyendo las etapas y los temas que deben abordarse para llevarlo a buen término. Dado que los Proyectos de digitalización contienen elementos técnicos, es importante establecer en qué momento se requerirá la implementación de estos, y si ello es paralelo a un proceso legal. Por ejemplo, una solicitud para operar con cierto proveedor tecnológico (que cumpla ciertas características como veremos más adelante) puede requerir primero de una notificación ante CNBV, así como la entrega de un expediente técnico, entre otros temas. Lo anterior, sin embargo, no implica (necesariamente) que toda la implementación tecnológica se encuentre completamente desarrollada para su uso en la fecha en que entre en vigor el contrato. Es decir, si bien los objetivos y metas legales y a nivel tecnológico forman parte de un solo proyecto, estos se deben identificar y esclarecer por cuerdas separadas.

Área de Sistemas.

Debe existir una comunicación adecuada y continua entre el asesor legal a cargo de conducir el proyecto (que recomendamos funja también como Administrador del Proyecto) y el Área de Sistemas. Sobre todo, para efecto de que el abogado pueda transmitirle (de preferencia por escrito y mediante memorándums o tarjetas informativas) lo siguiente:

- Requerimientos legales mínimos e indispensables que deben satisfacerse para cumplir con la normatividad aplicable, algunos de ellos de carácter técnico, y asesorar sobre la manera en que se deberán elaborar los documentos para su presentación a los Reguladores, en su caso.
- Señalamiento de los temas que deben ajustarse dependiendo de las características del servicio o proceso a implementarse.

- Indicar los aspectos que no son claros o que requieren de una asesoría externa o ante el Regulador, y evaluación de su importancia en la implementación del Proyecto.
- Proveer de formatos base para que puedan redactar, descargar y ordenar la información que, en su caso, tenga que entregarse al Regulador o ajustarse conforme a los Manuales de la Entidad y que faciliten la documentación del Proyecto.
- Verificar que la tecnología a implementarse cumpla con los estándares de seguridad de la información aplicables a la Entidad y/o aquellos que se encuentren plasmados en sus Manuales. Asimismo, verificar si es obligatorio o conveniente realizar una auditoría en la materia durante el proyecto.
- Ilustrar a los equipos de tecnología sobre antecedentes o ejemplos análogos al Proyecto que se trata de implementar en la medida de lo posible. En nuestra experiencia, los equipos técnicos pueden o no llegar a cierto grado de detalle al describir una funcionalidad, pero dicha especificidad debe ser indicada por el Administrador del Proyecto o el abogado responsable, quien tienen la experiencia sobre la manera en que el Regulador revisará esa información. Las Áreas de Sistemas, en principio, son ejecutivas y la labor descriptiva debe ser apoyada por el Área Legal para efecto de que la misma pueda ser inteligible a cualquier tercero; en especial frente al Regulador.
- El Área de Sistemas debe probar y realizar comprobaciones (testing) de los elementos informáticos involucrados en los Proyectos para efecto de establecer que los procesos de implementación van avanzando adecuadamente.

Aspectos Financieros

La presupuestación del Proyecto es otro de los aspectos que debe trabajarse de manera temprana y que implica al Director General y, en su caso, al Consejo de Administración. Es común, en nuestra experiencia, que ciertos Proyectos no puedan concluirse debido a que no son viables desde el punto de vista financiero. Nuestras recomendaciones al respecto serían:

- Revisar el presupuesto en la fase exploratoria y revisarlo nuevamente cuando ya se tenga establecida la estructura definitiva del Proyecto. No se recomienda quedarse con estimaciones iniciales: los requerimientos legales, las necesidades de integración, la necesidad de contratar programas adicionales o simplemente una cotización hecha por un tercero especialista en informática sobre supuestos distintos a los que finalmente guiarán el Proyecto, pueden afectar la precisión del presupuesto.
- El presupuesto debe estar basado en la información que proporcione: en primer lugar, el Área de Sistemas, pues ellos son los que pueden establecer las necesidades realistas, apoyar con cotizaciones exactas de proveedores y establecer si lo presupuestado será suficiente. Se recomienda hacer varios presupuestos tentativos considerando diversos supuestos y proveedores y que el abogado a cargo del proyecto asesore sobre los límites mínimos regulatorios y legales que deben cumplirse para que el Proyecto sea legalmente viable.
- Subdividir el presupuesto en caso de que sea necesario para manejarlo por Proyectos más pequeños. Las transformaciones digitales no ocurren en un día, por lo que el tamaño del Proyecto debe ser manejable para la Entidad.
- Las cantidades presupuestadas deben ser realistas y contemplar la posibilidad de retrasos en el cumplimiento de las fechas estimadas, contrataciones adicionales o atender supuestos o contingencias no contempladas originalmente en el Proyecto. Sobre todo, tener presente que la participación de agentes externos a la Entidad siempre conlleva riesgos potenciales o puede implicar en ciertos casos la generación de costos adicionales.
- Establecer herramientas que permitan la verificación y rastreo del gasto asignado a cada Proyecto.
- Establecer un plan de contingencia: nos hemos enfrentado a casos de proveedores que, por una u otra razón, no pueden satisfacer las expectativas o cumplir con sus contratos. Siempre existe la posibilidad de que situaciones fuera del control de la Entidad o de las Partes Responsables, como la mencionada, requieran gastos adicionales (así como ajustes a la planeación del Proyecto).

Al tratarse de una Guía Legal, hemos expuesto hasta este punto los aspectos que desde nuestra óptica deben desarrollarse para instrumentar un Proyecto desde el punto de vista jurídico. En ese sentido, es posible que el Área de Sistemas o lectores de este documento con una formación tecnológica observen otros aspectos de la administración de proyectos que son estándares en el sector informático y que no se revisarán en el presente documento. Entre dichos aspectos destacaríamos los siguientes:

- Herramientas de seguimiento. En el mercado existen muchas aplicaciones que sirven para realizar el seguimiento de proyectos. Algunas tienen planes gratuitos con la opción de ampliar los mismos para el caso de que se requieran administrar muchos Proyectos o se requieran particularidades adicionales.

- Metodologías. La metodología expuesta en la sección anterior de esta Guía Legal se refiere a una estructura común basada en estándares internacionales para la administración de proyectos legales y en la experiencia del Asesor Legal. No obstante, en el caso que se requiera desarrollo interno de software o incluso la contratación de un desarrollo por un tercero, éste utilizará algunas de las metodologías concretas que se han implementado actualmente (*agile, scrum, waterfall*). Dicho desarrollo debe ser integrado dentro del gran esquema del Proyecto, respetando los criterios del Área de Sistemas o del Asesor Externo al respecto.

» *Probando los Conceptos.*

La implementación de algunos Proyectos puede ser complicada e intensiva en recursos. Incluso las mejores planeaciones deben rendirse ante situaciones inesperadas y sufrir contratiempos. Así como en la ciencia se realizan experimentos controlados y en situaciones que, idealmente, no pueden dañar a nadie, bajo ciertas condiciones (y previa consulta de un experto legal) es posible que las Entidades realicen "pruebas de concepto" de algunos productos o procesos de digitalización. Una prueba de concepto ("POC", por sus siglas en inglés) es un ejercicio para probar una idea, diseño o, en el caso de las Entidades, productos o servicios de manera limitada. El propósito principal de desarrollar una prueba de concepto es demostrar la funcionalidad y viabilidad de una idea. Esta

implementación permite visualizar cómo funcionará el producto, da una idea del diseño, funcionalidades y límites.

Ahora bien, esta figura no existe como tal en la ley, y el presente no debe interpretarse como la existencia de una autorización limitada para probar nuevos temas en una Entidad, sin que ello carezca de consecuencias legales (para eso existe la figura del "modelo novedoso" en la Ley Fintech). A reserva de que cada Entidad realice un análisis legal interno de los supuestos de alguna prueba de concepto, consideramos que debería realizarse dentro de los siguientes parámetros:

- Si es un producto o servicio nuevo, en ninguna circunstancia involucrar al público en general o a clientes existentes de la Entidad. Esto genera consecuencias en varios niveles legales y operativos y una mala implementación, aunque sea temporal, podría generar una contingencia legal.
- Utilizarse a nivel de laboratorio, entre personas autorizadas por la Entidad sin que ello implique un cambio interno o en los Manuales de la Entidad y de modo que funjan como "sujetos de prueba" con montos simbólicos.
- No utilizar datos personales o información de clientes que no hayan autorizado su uso para esos fines.
- Establecer quiénes serán las partes involucradas y asegurarse de que la realización limitada de esa actividad o proceso no contraviene ninguna norma legal.
- Tomar las medidas adecuadas para que no se afecte a terceros, sobre todo a los clientes de las Entidades, en la realización de dichas actividades.
- Abstenerse de publicitar la POC o de realizar algún tipo de anuncio que pudiera inducir al público a confusión respecto de la aplicabilidad.
- Establecer parámetros de seguridad operativa e informático mínimos que garanticen que la POC no será un foco de contingencias en esos ámbitos.

En cualquier caso, dependiendo del caso concreto, sugerimos que la Entidad que busque probar un concepto consulte de forma previa a cualquier implementación a un asesor legal y, en su caso, al Regulador.

Clientes

En paralelo o como parte de la preparación y estructuración del Proyecto lo primero que hay que analizar es la figura del "Cliente", comprendida como:

- Cliente Interno: la persona o áreas de la Entidad que serán las encargadas de implementar o utilizar en su día a día el resultado del Proyecto que se va a implementar. Esta identificación tiene consecuencias a nivel de: (i) identificación de una Parte Responsable de esa área para efecto de participar de manera (activa o supervisora) del Proyecto, y (ii) obtener su retroalimentación sobre las implicaciones de cada Proyecto.

- Cliente Externo: en el caso de nuevos productos o servicios (en este caso digitales), sugerimos establecer la segmentación del mercado a la cual se quiere acudir con ellos. Esto es importante para establecer la viabilidad del nuevo producto, establecer necesidades de diseño, ajustar los temas relacionados con PLD/FT y evaluar los temas legales que deben incorporarse en el Proyecto (por ejemplo, los temas de transparencia y ordenamiento de los servicios financieros que mencionamos más adelante).

Canales

El establecimiento del canal a través del cual se ofrecerá un producto o un servicio es uno de los aspectos centrales para efectos de planear un Proyecto. Por canal debe entenderse cualquier medio que se usará por la Entidad para presentar el resultado de un producto o servicio al Cliente Interno o al Cliente Externo de la Entidad. Algunos ejemplos de canales son los corresponsales, el Internet y los cajeros automáticos, entre otros, los cuales deben satisfacer requerimientos legales específicos.

Productos y Servicios.

De manera breve expusimos los productos y servicios que pueden ofrecer las Entidades en la Sección 1 del presente documento. Sin embargo, para efectos de la presente Guía Legal, hemos preferido un enfoque más genérico y centrado en aspectos conceptuales. Por ejemplo, en esta Guía Legal no nos hemos concentrado en describir cómo implementar un producto de captación concreto y con características que pueden variar dependiendo

del plan de negocio de cada Entidad. Sin embargo, hemos seleccionado procesos que consideramos genéricos y que pueden aplicar a una variedad de productos y servicios como apertura de cuentas remotas, implementación de firmas electrónica, almacenamiento en la nube, entre otros procesos.

Los Proyectos pueden traslaparse y mezclarse con otros. Aquellos que presentamos y describimos a continuación pueden ser implementados en paralelo dependiendo de las necesidades concretas de cada Entidad.

Procesos

En términos generales, el sector financiero se está moviendo hacia una manera de administrar los servicios que toma en cuenta cada una de las fases que deben existir previo a la entrega de un servicio o producto. Sin embargo, sugerimos que en los diseños de Proyectos se tenga en cuenta no sólo el producto o servicio final para el Cliente, sino todos los pasos intermedios, así como todas las áreas relacionadas: desarrollo de negocios, marketing, desarrolladores, seguridad informática, control interno. Es decir, usar un enfoque sistémico de todo lo que tiene que suceder antes de que se ofrezca un producto o un servicio al público en general. Si no se tiene identificada la cadena de servicio y procesos para un producto, especialmente cuando este implique un Cliente externo, será difícil que el Proyecto llegue a buen término.

Tecnologías

Esta Guía Legal no pretende ser una guía tecnológica, sino que se dirige esencialmente a presentar una manera de administrar e implementar Proyectos legales con un componente digital, si bien relevancia de algunas tecnologías fue tomada en cuenta para efecto de preparar este documento. Entre los temas que, de acuerdo con varios reportes públicos y nuestra experiencia, serán más relevantes para el futuro de los servicios financieros, pensamos que son de interés para el lector:

- El cómputo en la nube para el almacenamiento y procesamiento de operaciones.
- Las Aplicaciones Informáticas Estandarizadas o “APIs” que permiten el acceso a la banca abierta.
- Automatización de procesos.

- Big Data.
- Tecnologías de pagos.
- Inteligencia Artificial.
- Blockchain.
- Ciberseguridad.

No se trata de una lista exhaustiva, y no es el objetivo de la Guía Legal exponer los componentes y la manera en que las mismas impactarán a los servicios financieros. Se trata de una muestra que ha sido seleccionada y, en lo aplicable, desarrollada en el presente documento.

Organización

Este tema ya se ha tratado anteriormente en la Sección 1 al referirnos a la organización de los Proyectos. Por otra parte, en la Sección 3 hacemos referencia a las partes responsables internas, así como a las funciones y órganos que participan en las decisiones de una Entidad y que tienen relevancia para el Proyecto.

Ubicaciones

Cada Proyecto implica planificar, presupuestar, ejecutar y medir ciertos aspectos con base en sus objetivos. Aunque no es común contemplar necesariamente la ubicación física para las Partes Responsables debido a la posibilidad de trabajar en línea y a la naturaleza digital de los Proyectos, es posible que en ocasiones se requiera asignar, por parte de las Entidades, un espacio específico para tener reuniones, revisar documentos que no están digitalizados o que, por su confidencialidad no pueden dejar las oficinas de las Entidades, o incluso para hacer más inmediata la interacción con otras Partes Responsables internas de cada Entidad. Dependerá de cada Proyecto el atender este tema.

SECCIÓN 3.- PARTES RESPONSABLES INTERNAS.

En la sección 2 se habló de las Partes Responsables del Proyecto. Dada la importancia de este aspecto, a continuación, se describen las responsabilidades que pueden tener órganos y funcionarios internos de las Entidades en un Proyecto.

Hemos excluido a la asamblea de accionistas (o se Socios) debido a que, en principio, los Proyectos se refieren a cuestiones de administración que competen tanto al Consejo de Administración como al Director General, sin embargo, es necesario analizar si la planeación de un Proyecto debe ser aprobada por dicho órgano mediante la aplicación de las siguientes preguntas:

- ¿Los estatutos establecen montos específicos como umbral para que la asamblea de accionistas apruebe ciertos Proyectos?
- ¿Existen acuerdos entre accionistas que establezcan disposiciones relacionadas con el plan de negocios de la Entidad y que se relacionen con el Proyecto?
- ¿El Proyecto implica que la Entidad preste algún servicio que no estaba originalmente autorizada para prestar?
- ¿Existe la posibilidad de que el Proyecto exponga a la Entidad a nuevos riesgos o riesgos adicionales a los tolerados comúnmente por ella?
- ¿La adopción del Proyecto implica cambios sustanciales a algún plan de negocio, resolución o documento emitido por la asamblea de accionistas?
- ¿Las disposiciones especiales en materia de LD/FT o cualesquier obstaculizan el Proyecto?
- ¿El presupuesto excede significativamente los parámetros ordinarios de gastos en tecnología o proyectos especiales?

En todo caso se recomienda consultar con el área legal responsable de la Entidad los aspectos generales de cada Proyecto para efecto de determinar si el involucramiento de este órgano será necesario.

3.1 El Órgano de Administración.

Las Entidades cuentan con un Consejo de Administración y con un Director General o gerente general (Director General) para efecto de llevar a cabo la administración de sus asuntos. Dependiendo del tipo de Entidad, los requisitos de integración y funcionamiento varían un poco, pero son similares a los de las Entidades mercantiles en general.

El Consejo de Administración puede jugar varios roles en relación con un Proyecto dependiendo de su magnitud y características, pues este órgano tiene a cargo la responsabilidad de supervisar el control interno, aprobar la estructura orgánica de la Entidad y aprobar los Manuales (por ejemplo, el Manual de Crédito), muchos de los cuales se relacionan con los Proyectos. Dichas funciones pueden variar dependiendo del Nivel de Operación de la misma cuando sea aplicable. Al respecto, ponemos a su disposición resoluciones ejemplificativas para aprobar los Manuales por primera vez o, en su caso, para aprobar modificaciones a los mismos en el Anexo III del presente documento.

Asimismo, el Consejo de Administración, en el caso de prestadores de servicios para cuya contratación se requiera autorización de CNBV, deberá aprobar esa contratación y asegurarse de lo siguiente[11]:

- Que al contratar los servicios o comisiones no se ponga en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Entidad.
- Que las prácticas de negocio del tercero o comisionista sean consistentes con las de operación de la Entidad.
- Que no habría impacto en la estabilidad financiera o continuidad operativa de la Entidad con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizará en la prestación del servicio.

[11] Sección II de la Guía para la Autorización de Contratación de Servicios o Comisiones dirigida a las SOCAP ("Guía para la Contratación de Servicios") y Sección II de la Guía para la Autorización de Contratación de Comisionistas dirigida a las SOFIPO y SOFINCO ("Guía para la Contratación Comisionistas")

- Establecer los criterios que permitan a las Entidad, a través de su Director General, evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones que realice la Entidad.

Asimismo, dependiendo de la importancia de los servicios a contratarse, el Consejo de Administración tendrá facultades para evaluar el desempeño de esos terceros.

Lo anterior tiene varias implicaciones prácticas:

- Ciertos Proyectos, específicamente los que implican procesos operativos o administrativos o la contratación de comisionistas, deben contar con una evaluación de riesgos y ajustarse a las políticas aprobadas por el Consejo de Administración para su contratación y seguimiento de su desempeño.
- En los casos donde el Proyecto requiere de un presupuesto o erogación extraordinaria es recomendable llevar el asunto hacia dicho órgano para su aprobación.
- Las aprobaciones del Consejo de Administración requieren presentarse de manera adecuada, incluyendo la inserción del asunto en el orden del día. Se sugiere preparar materiales explicativos del Proyecto para efecto de ilustrar a los consejeros sobre el Proyecto y facilitar la toma de una decisión informada.

3.2 Comités.

Las Entidades cuentan con algunos órganos colegiados que auxilian al Consejo de Administración en el desempeño de sus funciones. Algunos de ellos son optativos, mientras que otros son obligatorios. Entre estos comités se encuentran:

- Comité de Auditoría.
- Comité de Crédito.
- Comité de Comunicación y Control.
- Comité de Riesgos.

- Comité de Remuneración

No todas las Entidades deben contar con los mismos comités y su obligatoriedad puede variar dependiendo del tipo de Entidad.

Conforme se definan las características del Proyecto, será necesario involucrar a dichos Comités, sobre todo los cuatro primeros y, en los casos en los que se requiera, obtener su autorización correspondiente para poner en marcha algunos de los Proyectos.

3.3 El Director General.

La Dirección General de las Entidades es el órgano que, junto con el Consejo de Administración, legalmente comparte la responsabilidad de administrar las Entidades por lo cual se requiere la acreditación de ciertos requisitos para efecto de ocupar esta posición.

Entre sus facultades y responsabilidad están la de proponer o elaborar políticas relacionadas con las actividades de las Entidades, así como proporcionar datos e informes precisos para auxiliar al Consejo de Administración en la adecuada toma de decisiones. También tiene incidencia (ya sea por la facultad de nombrar o de participar) en los Comités.

El Director General tiene un papel central en los Proyectos debido a que: (i) tiene a su cargo la ejecución y supervisión de las operaciones de las Entidades, por lo que, en principio, todos los Proyectos deben ser aprobados y supervisados por él o ella; (ii) en caso de ciertos contratos celebrados con terceros y en ciertos supuestos de acreditación de suficiencia tecnológica (que describimos más adelante) él o ella tiene la responsabilidad de firmar y asegurar al Regulador que los requisitos correspondientes se cumplen; (iii) la preservación y continuidad del control interno está esencialmente en sus manos; (iv) es el encargado de proponer el nombramiento de funcionarios relevantes de la Entidad, por ejemplo, la persona encargada de la administración de riesgos; (v) tiene a su cargo revisar y proponer cambios a los Manuales de la Entidad; (vi) es el responsable de la implementación y evaluación de estrategias crediticias, y (vii) tiene a su cargo la responsabilidad de proponer y recomendar al Consejo de Administración ciertas medidas relacionadas con la operación continua de la Entidad, entre otros temas.

3.4 Director Jurídico o Área de Cumplimiento.

La Dirección Jurídica o su equivalente, se encuentra comúnmente en la mayoría de las Entidades. No se trata de una posición prevista en los ordenamientos legales, sino una función que existe en muchas Entidades debido a su régimen y las numerosas obligaciones que el SACP tiene que cumplir bajo las leyes aplicables. En algunos casos, este papel se realiza por un asesor externo y, en otros, por áreas que también cuentan con otras funciones. Hay entidades que incluso cuentan con varias personas con esta denominación debido a que su volumen de trabajo o de operaciones les permite contar con personal especializado.

Su involucramiento en el caso de los Proyectos es necesario en la mayoría de los casos, aunque el grado de intervención puede variar conforme a la manera en que se estructure el Proyecto.

3.5 Oficial de Cumplimiento.

El Oficial de Cumplimiento es el funcionario de las Entidades encargado de supervisar y vigilar el cumplimiento de las disposiciones en materia de PLD/FT. Dependiendo de si la Entidad cuenta o no con un Comité de Comunicación y Control[12], sus funciones pueden ser extensas en la materia o compartidas con dicho órgano. Los procesos de identificación de los clientes de las Entidades, así como el manejo y uso del Sistema Automatizado son su responsabilidad, por lo que su intervención es indispensable en Proyectos que involucren dichos aspectos.

3.6 Director de Operaciones.

No se trata de una posición que esté expresamente descrita en la ley. Como el Director Jurídico, sus funciones pueden estar traslapadas con las de otros funcionarios o incluso ser ejercidas directamente por el Director General. La tendencia en las entidades financieras, inclusive a nivel mundial, es contar con este funcionario, pues permite atender

[12] Conforme a las Disposiciones Generales SOFIPO y conforme a las Disposiciones Generales SOFIPO las Entidades deberán constituir y mantener un Comité de Comunicación y Control cuando cuenten con más de 25 personas a su servicio, ya sea que realicen funciones para la misma de manera directa o indirecta a través de servicios complementarios.

de manera directa aspectos prácticos e inmediatos de la marcha de la Entidad, apoyando así al Director General. Asimismo, este funcionario asegura que la Entidad pueda cumplir con su estrategia y objetivos de manera más eficiente. En todo caso, este funcionario o su equivalente deben estar involucrados en los Proyectos para efecto de garantizar que la planeación sea efectiva.

3.7 Auditoría Interna.

Las Entidades deben contar con un área de auditoría interna independiente de las áreas de negocios, administrativas y de contraloría, cuyo responsable o responsables, serán designados por el Consejo de Administración. Su responsabilidad es, entre otros aspectos, verificar el funcionamiento adecuado del sistema de control interno, para lo cual debe evaluar la adecuada implementación y cumplimiento de las políticas y procedimientos en materia de control interno establecidos por el Consejo de Administración. Para cumplir con sus objetivos, la regulación le otorga diversas facultades, por ejemplo, la de llevar a cabo pruebas sustantivas de los procedimientos operativos, auditar el cumplimiento de políticas internas, revisar que los sistemas informáticos cumplan sus objetivos, entre otras.

En el caso de las Cajas de Ahorro, la función de la Auditoría Interna tiene una descripción un poco más específica orientada a la evaluación de riesgos de manera particular.

En todo caso, la participación de la Auditoría Interna en un Proyecto es importante desde su planeación para efecto de:

- Asegurar que el Proyecto se apegará a los lineamientos de riesgo (tecnológico o de otra especie que contemple la Entidad en sus políticas internas).
- Establecer la manera en que el Proyecto podrá ser evaluado y establecer dichos procedimientos, incluso antes de la etapa de cierre.
- Comunicarse constantemente con esta área para informar de avances o consultar aspectos esenciales del Proyecto que tengan que ver con exposición al riesgo o la seguridad de la información.

3.8 Asesoría Externa.

La asesoría externa para cada Proyecto debe ser uno de los aspectos iniciales en su preparación. Para efecto de determinar si la asesoría externa es requerida y la naturaleza de la misma, es necesario que la Entidad, a través de las personas a cargo de implementar el Proyecto, se haga las siguientes preguntas:

1. ¿El Proyecto es completamente nuevo u obedece a la ampliación de aspectos o áreas que ya existen dentro de la organización? ¿Existe alguien dentro de la Entidad que tenga experiencia similar?

2. ¿La información que se requiere para llevar a cabo el Proyecto es técnica o requiere experiencias sobre temas que no se encuentran dentro de las tareas rutinarias de la Entidad?

3. ¿Se cuenta con los recursos humanos suficientes para llevar a cabo el Proyecto a nivel interno?

En todo caso, se recomienda realizar un diagnóstico interno sobre la información con que se cuenta en relación con un Proyecto, así como la investigación el mismo en fuentes públicas.

Dependiendo de las respuestas a esas preguntas deben agruparse las áreas de experiencia requeridas para el Proyecto, las cuales, como se ha mencionado anteriormente, generalmente se encuentran dentro de las siguientes áreas de experiencia:

- Legal.
- Prevención de lavado de dinero y financiamiento al terrorismo.
- Tecnológica.
- Financiera.
- Operativa y/o continuidad de negocios.

La selección de cada uno de los expertos o asesores externos tradicionalmente se realiza mediante recomendaciones de funcionarios internos de la Entidad con base en experiencias de otras Entidades. No obstante que dicho camino asegura que existan referencias claras sobre las credenciales de los asesores externos, sugerimos tomar en cuenta los siguientes aspectos:

- Solicitar detalles de la experiencia de cada uno de los empleados o prestadores de servicios que potencialmente estarían involucrados en el Proyecto.
- Realizar una serie de entrevistas previas al equipo del asesor externo para realizar preguntas concretas sobre el Proyecto: puntos de vista sobre su viabilidad, evaluación previa sobre la necesidad de involucrar otras áreas, aspectos que considera problemáticos, tiempos estimados de terminación con base en experiencias pasadas, entre otros temas.
- Solicitar un listado del equipo que apoyará al Asesor Externo en la realización de las tareas e involucrarlos en el proceso de entrevistas.

El alcance de los servicios debe constar por escrito en un contrato de prestación de servicios que contenga por lo menos:

- Alcance de los servicios. Existen ocasiones en que, debido a que el Asesor Externo será quien determinará gran parte del alcance del Proyecto, no será posible determinar en un primer momento el alcance total de sus servicios. Bajo estas circunstancias, puede dejarse abierta la posibilidad de ampliar el contrato o, en su caso, celebrar uno nuevo en cuanto el alcance quede determinado.
- Establecer cláusulas de confidencialidad estrictas. Esto debe hacerse, en especial, si el Asesor Externo tendrá acceso a sistemas o documentos con información sensible o de clientes de las Entidades. En todo caso, es necesario verificar si es necesario obtener algún permiso adicional o realizar algún acto previo para permitir el acceso a dicha información.
- Clausulado de salida. Es común que los contratos confundan los términos “recisión” con “terminación”. El primero se refiere a la potestad que tiene la parte afectada por un incumplimiento de solicitar la terminación de un contrato, así como, a su elección, requerir el pago de daños y perjuicios o el cumplimiento forzoso. La

terminación, por su parte, no conlleva necesariamente la recisión ni implica un incumplimiento. Esta confusión entre ambos conlleva a que, en ocasiones, los contratos no cuenten con un mecanismo claro para salir del contrato sin responsabilidad para las partes en caso de que ello simplemente deje de ser conveniente. Desde luego, en casos donde se ha avanzado en el cumplimiento del contrato, debe cuidarse que los derechos de las partes, por ejemplo, a recibir una contraprestación por lo ya trabajado se liquide previo a cualquier opción de terminación o que dicha terminación no sea riesgosa o cause daño a las Entidades.

- Estándares de servicios. En el caso de Asesores Externos legales, no es común establecer algún estándar de calidad, cosa que, por su parte, sí es común en el caso de los Asesores Externos con experiencia tecnológica u operativa. En todo caso, se sugiere insertar un clausulado que haga hincapié en los principios de profesionalismo y dedicación suficiente a la prestación de los servicios, con especial énfasis en el resultado esperado de la colaboración en el Proyecto.

3.9 Reguladores.

El involucramiento de los Reguladores es un aspecto importante y delicado: existe una normativa que señala lo que se puede o no se puede hacer en la mayoría de los casos. Sin embargo, debido a la complejidad y la amplitud de la normatividad aplicable, existen zonas grises (sobre todo en proyectos tecnológicos) que pueden requerir una consulta. La naturaleza de la consulta, formal o informal, dependerá de la naturaleza del supuesto. Pensamos que la interacción con el Regulador puede ser productiva si se toma en cuenta lo siguiente:

- Las consultas deben hacerse en términos concretos y una vez que se ha explorado la idea de manera suficiente para formularlas adecuadamente.
- En la medida que sea necesario, preparar materiales de apoyo que sinteticen la información relevante y que permitan conducir una reunión informativa.
- Apoyar al Regulador con puntos de vista y con argumentaciones estructuradas sobre la viabilidad del Proyecto propuesto. El Regulador no es un asesor legal ni de ninguna especie, sus funciones son la supervisión y vigilancia (principalmente), por lo que ellos no están obligados a dar una solución para la implementación del Proyecto. Sin duda en aquellos Proyectos que sean comunes al SACP tendrán

puntos de vista y criterios consensuados, pero en el caso de Proyectos novedosos será necesario llegar con conocimiento profundo previo y una estructuración potencial concreta.

- La interacción con el Regulador debe incluir a las personas que conozcan del Proyecto y que puedan proporcionar información útil.

3.10 Proveedores Externos.

El Asesor Externo, por definición, es quien presta un servicio intangible consistente basado en su experiencia y pericia en cierta área. Se trata de una consultoría cuyo entregable es, en primer lugar, guía e información sobre ciertos aspectos del Proyecto. Su entregable, si bien puede traducirse en documentos o acciones concretas, es la asesoría y adaptación de su experiencia al caso concreto. Por su parte, un proveedor externo generalmente tiene entregables concretos y definidos: lo que adquiere la Entidad son productos ya estructurados y estandarizados (si bien pueden adaptarse a ciertas necesidades prácticas específicas), por ejemplo, en el caso de sistemas de administración de nómina o incluso proveedores de artículos de papelería. Por lo que respecta al Proyecto, nos centraremos en proveedores de tecnología.

Las Entidades, en sus políticas de contratación de servicios o comisiones que se encuentran en ciertos supuestos relevantes (y que por su importancia están sometidos al cumplimiento de cierta regulación específica tal como se describe más adelante), deben contemplar medidas de evaluación que, entre otros temas, establezcan:

(i) La capacidad de los terceros o comisionistas para implementar medidas o planes que permitan mantener la continuidad del servicio con niveles adecuados de desempeño, confiabilidad, capacidad y seguridad.

(ii) La integridad, precisión, seguridad, confidencialidad, resguardo, oportunidad y confiabilidad en el manejo de la información generada o transmitida por la Entidad con motivo de la prestación de los servicios o comisiones, así como el acceso a dicha información, a fin de que sólo puedan tener acceso a ella las personas que deban conocerla.

(iii) Los métodos con que cuenta la Entidad para evaluar el cumplimiento al contrato correspondiente, o bien, la adecuada prestación de los servicios o comisiones.

(iv) Los criterios y procedimientos para calificar periódicamente la calidad del servicio.

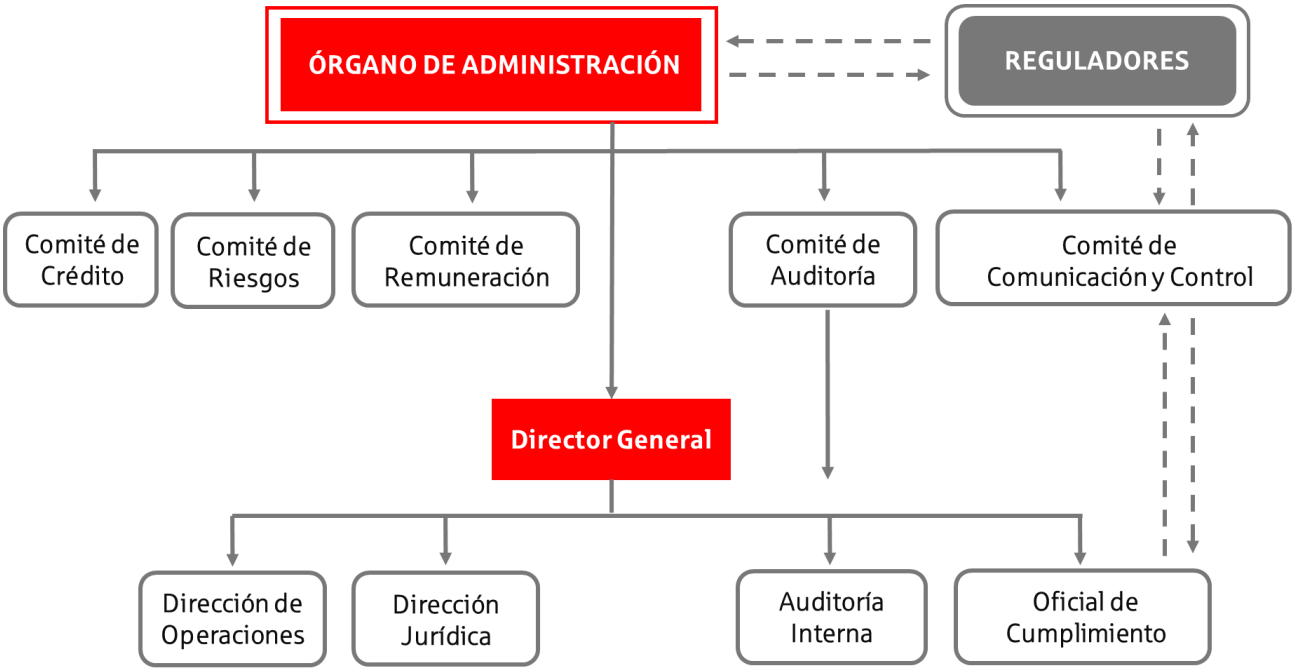
(v) La capacidad de las Entidades de mantener la continuidad en la prestación de los servicios o comisiones que se hubieren contratado, o bien, las opciones externas con que se cuenta, en cualquier caso, a fin de disminuir la vulnerabilidad operativa de la Entidad.

(vi) La capacidad de las Entidades para orientar la administración integral de riesgos e identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos que puedan derivarse de la prestación de los servicios o comisiones relevantes.

(vii) La capacidad del sistema de control interno para cumplir con las políticas y procedimientos que regulen y controlen la prestación de los servicios o comisiones relevantes.

Lo anterior son aspectos que deben revisarse a la luz de las políticas específicas de cada entidad, lo cual requiere el involucramiento de distintas áreas para la preparación del Proyecto.

Organigrama ejemplificativo de las Entidades



Gráfica 5. Organigrama ejemplificativo de las Entidades. Fuente: Vite Abogados

SECCIÓN 4.- CONTROL INTERNO Y MANUALES.

4.1 Importancia del Control Interno.

Las Entidades, conforme a la normatividad aplicable, deben contar con un "Sistema de Control Interno" con el propósito de: supervisar los riesgos del negocio, delimitar funcionalidades y responsabilidades de cada área, establecer esquemas de operación y control, acceso de sistemas y medidas que garanticen la integridad y confidencialidad de la información contenida en las bases de datos y aplicaciones implementadas para la realización de operaciones, incorporar medios de respaldo para asegurar la continuidad del negocio, establecer políticas antifraude y contingencias similares.

En las Entidades esto tiene un componente escrito: los Manuales. En ellos se desarrollan los puntos anteriores y, por otra parte, el funcionamiento concreto de cada uno de los procesos internos. Si bien los Manuales son documentos detallados de los temas mencionados, gran parte de su puesta en práctica corresponde a procesos y actividades que pueden no estar reflejadas del todo en los documentos. Por lo tanto, la consulta con las personas que tienen a su cargo la implementación del control interno es uno de los pasos necesarios para estructurar un Proyecto y poder establecer lo siguiente:

- Si el proyecto es viable y compatible en el contexto de los Manuales donde se refleja el Sistema de Control Interno.
- Las responsabilidades dentro del Proyecto de las personas que tengan a su cargo dicho control interno.
- Los cambios que sería necesario implementar tanto a los Manuales como a los procesos que en la práctica deben llevarse a cabo.
- La necesidad de involucrar al Regulador para efecto de realizar cambios o transformaciones dentro del control interno.

4.2 Evaluación de Proveedores.

El Consejo de Administración está a cargo de designar un responsable, que podrá ser el Auditor Interno o el Comité de Auditoría, para que dé seguimiento, evalúe y reporte periódicamente a dicho Consejo de Administración, el desempeño de los prestadores de servicios o comisionistas relevantes (ver Sección 15. Contratación de Proveedores y Comisionistas), así como el cumplimiento de las normas aplicables relacionadas con los servicios o las operaciones correspondientes.

El Consejo de Administración debe revisar, cuando menos, una vez al año las políticas de selección de los terceros o comisionistas y aprobar las modificaciones que sean necesarias con base en los resultados de las evaluaciones realizadas por el responsable de dar seguimiento y evaluar el desempeño de aquellos.

4.3 Manuales Relevantes.

Para efecto de obtener la autorización para organizase y operar, las Entidades deben contar, por lo menos, con los siguientes Manuales:

- Manual de Control Interno, cuyo objeto es establecer el funcionamiento de control interno de la Entidad, en el cual se fundarán: (i) los objetivos, políticas y procedimientos de control interno; (ii) la estructura organizacional, especificando las responsabilidades y los responsables de llevar a cabo las funciones dentro de la Entidad; (iii) los sistemas de información dentro de la Entidad; (iv) la descripción de la normatividad interna de la Entidad[13]. Es decir, en este Manual se deben establecer las directrices y lineamientos generales de control que le son aplicables a todo el personal dentro de su quehacer y responsabilidades diarias, como parte de los procesos operativos, administrativos y de registro de operaciones, orientados a dar una mayor certidumbre a la toma de decisiones y conducir a la Entidad con una seguridad razonable al logro de sus objetivos y metas dentro de un ambiente ético, de calidad, mejora continua, eficiencia y de cumplimiento de la ley.

[13] Artículo 33 de las Disposiciones Generales SOCAP y artículo 54 de las Disposiciones Generales SOFIPO.

- Manual de Crédito. Dicho manual debe contener las políticas y los procedimientos de crédito, mismo que deberá de contener los siguientes lineamientos mínimos[14] para:

  (i) La promoción y otorgamiento de crédito, estableciendo los métodos de aprobación y otorgamiento de crédito.

  (ii) Integración de expedientes de crédito contemplando las políticas y procedimientos para la integración de un expediente único por cada acreditado.

  (iii) Evaluación y seguimiento de cada uno de los créditos de la cartera.

  (iv) Recuperación de cartera crediticia.

- Manual de Captación. Es un instrumento básico para la adecuada estandarización de criterios y procesos operativos y administrativos utilizados por la Entidad para atender la demanda de operaciones pasivas, así como estructurar la organización interna específica para llevar a cabo dichas operaciones y contar con una herramienta de orientación de todo el personal involucrado en este proceso de la Entidad.
- Manual de Administración Integral de Riesgos. En él se deben desarrollar los objetivos, políticas y procedimientos para la administración de riesgos de crédito y otros riesgos a los que se encuentra expuesta la Entidad, la designación de la persona responsable de la administración de riesgos, así como el desarrollo de las metodologías, modelos y parámetros para identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos a que se encuentra expuesta la Entidad.[15]
  El manual de administración integral de riesgos deberá contener, al menos, los siguientes aspectos[16]:

  (i) Los objetivos sobre la exposición al riesgo de crédito, de mercado y de liquidez;

[14] Artículo 33 de las Disposiciones SOCAP y artículo 54 de las Disposiciones SOFIPO.

[15] Artículos 75, 76, 112 *in fine* de las Disposiciones Generales SOFIPO y artículos 59, 60 y 100 *in fine* de las Disposiciones Generales SOCAP.

[16] Artículo 114 de las Disposiciones Generales SOFIPO y artículo 112 de las Disposiciones Generales SOCAP.

(ii) Una estructura organizacional diseñada para llevar a cabo la administración de riesgos. Dicha estructura deberá establecerse de manera que exista independencia entre la persona responsable de la administración de riesgos respecto de las unidades de negocio;

(iii) La determinación o procedimiento para calcular los límites de los riesgos;

(iv) El tipo de reportes que elaborarán, así como la forma y periodicidad con la que deberá informarse al Consejo de Administración, al Director General y a las unidades de negocio, sobre la exposición al riesgo de la Entidad;

(v) Las medidas de control interno, al igual que las correspondientes para corregir las desviaciones que se observen sobre los límites de exposición al riesgo;

(vi) El proceso para la aprobación de propuestas de nuevas operaciones, servicios y líneas de negocios, como también de estrategias o iniciativas de administración de riesgos;

(vii) Los planes de acción en caso de contingencias por caso fortuito o fuerza mayor, y

(viii) Los mecanismos de corrección en caso de que se excedan los límites de riesgo autorizados.

- Manual de Tecnologías de Información, cuando la Entidad utilice equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados, y que previamente pacten las Entidades con sus Socios o clientes para la celebración de sus operaciones y la prestación de sus servicios ("Medios Electrónicos"), deberá contar con un manual de tecnologías de la información en el cual se desarrollen las operaciones y servicios que proporcionará a través de ellos, así como los

mecanismos y procedimientos de seguridad en la transmisión, almacenamiento y procesamiento de la información a través de los Medios Electrónicos.[17]

- Manual PLD/FT, en los cuales se deberán establecer los criterios, medidas y procedimientos establecidos en las Disposiciones PLD/FT[18] que las Entidades están obligadas a observar para prevenir y detectar actos, omisiones y operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión del delito previsto en el artículo 139 Quáter del Código Penal Federal o que pudiesen ubicarse en los supuestos del artículo 400 Bis del mismo Código Penal Federal.

  En este Manual, las Entidades deben desarrollar las políticas de identificación y conocimiento del Cliente, así como los criterios, medidas y procedimientos internos que la Entidad adoptará para dar cumplimiento a las Disposiciones PLD/FT. Asimismo, el mencionado manual deberá incluir los criterios, medidas, procedimientos y demás información relacionada con:

  (i) Política de identificación del Cliente, que permita determinar, entre otros, el tipo de persona que es el potencial Cliente (persona física de nacionalidad mexicana, extranjera con residencia temporal o permanente, extranjera residente en el extranjero; persona moral extranjera; dependencias y entidades públicas federales, estatales, municipales, fideicomisos, etc.), carácter con el que acude (titular, tercero autorizado, apoderado, proveedor de recursos, propietario real, beneficiario), entre otros, etc.

  (ii) Política de conocimiento del Cliente que incluya, por lo menos, procedimientos para que la Entidad dé seguimiento a las operaciones realizadas por los Clientes, procedimientos para el debido conocimiento del perfil transaccional de cada uno de los Clientes; supuestos en que las operaciones se aparten del perfil transaccional de cada uno de sus Clientes; medidas para la identificación de posibles Operaciones

[17] Artículo 171 Bis 21 de las Disposiciones Generales SOCAP y artículo 265 Bis 21 Disposiciones Generales SOFIPO.

[18] Disposiciones PLD/FT, significan las Disposiciones de Carácter General a que se refieren los artículos 71 y 72 de la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo; las Disposiciones de Carácter General a que se refiere el artículo 124 de la Ley de Ahorro y Crédito Popular; y las Disposiciones de Carácter General a que se refieren los artículos 115 de la Ley De Instituciones De Crédito en relación con el 87-D de la Ley General de Organizaciones y Actividades Auxiliares del Crédito y 95-Bis de este último ordenamiento, aplicables a las Sociedades Financieras De Objeto Múltiple.

Inusuales; y, en caso de ser necesario, consideraciones para modificar el grado de Riesgo previamente determinado para un Cliente (ver Sección 8 Seguridad y Confidencialidad de la Información y Continuidad de la Operación).

(iii) Prohibiciones para la realización de operaciones en efectivo con dólares de los Estados Unidos de América ("EUA") conforme a lo establecido en las Disposiciones PLD/FT.

(iv) Reportes de operaciones: relevantes, inusuales, internas preocupantes, realizadas en dólares de los EUA y transferencias internacionales de fondos.

(v) Estructuras internas, contemplando la estructura del Comité de Comunicación y Control, al oficial de Cumplimiento, así como sus funciones y obligaciones.

(vi) Programas de capacitación y difusión.

(vii) Sistemas automatizados (ver Sección 6 Prevención de Lavado de Dinero y Financiamiento al Terrorismo).

(viii) Reserva y confidencialidad.

(ix) Otras obligaciones en la materia.

Dichos Manuales se refieren a aspectos particulares de la Operación que deben considerase en el momento de planear un Proyecto. Una vez que el mismo se encuentre debidamente estructurado, será necesario que una de las Partes Responsables realice una revisión preliminar de los Manuales, establezca qué aspectos de los mismos serán relevantes para el Proyecto y, finalmente, contacte a las áreas encargadas de su implementación. En su caso, el mapa del Proyecto deberá realizarse considerando los Manuales e incluir las correspondientes modificaciones a los mismos.

Para el desarrollo de los Manuales señalados, se hacen las siguientes recomendaciones a las Entidades:

- Antes de la redacción de los Manuales, se deben tener presentes los objetivos que se busca cumplir con el Proyecto y reflejar en los mismos la estrategia de elaboración e implementación de los procedimientos que seguirá la Entidad para alcanzarlos.

- Consultar los Manuales ejemplificativos elaborados por las autoridades reguladoras que, si bien no existen ejemplos de todos los Manuales, es fundamental consultar los que sí están disponibles a través de Internet, ya que pueden orientar a la Entidad para identificar qué es lo que buscan dichas autoridades. En el supuesto en que exista un Manual ejemplificativo para el caso concreto, se recomienda a la Entidad apegarse al mismo en la medida de lo posible, ya que estos, generalmente19, contendrán todos los elementos legales establecidos en la normatividad.
- La Entidad debe identificar los requerimientos mínimos legales que se deben incluir, así como los elementos y la estructura que tendrá el manual que se va a redactar.

Los elementos extralegales que se deben considerar son[20]:

(i) Objetivo. Se deberá describir el propósito que se busca obtener con la implementación del Manual.

(ii) Alcance. Se deberán establecer los límites de aplicación del Manual dentro de la Entidad, incluyendo los aspectos del negocio que estarán regulados por el manual en cuestión y los procesos respectivos.

(iii) Participantes, es decir, el personal responsable de las actividades y procedimientos descritos en el Manual.

(iv) Diagramas en los que se muestran los procedimientos en forma gráfica.

(v) Actividades, que son las tareas a realizar como parte del procedimiento descrito, mismas que deben contener: descripción, responsable, reglas.

[19] La especificidad del proyecto puede provocar que ciertos aspectos del mismo no estén plasmados en los manuales ejemplificativos. En ese sentido, es importante considerar que los manuales ejemplificativos no son ni tienen el objetivo de sustituir la elaboración de manuales preparados especialmente para las Entidades.

[20] ¿Qué es y cómo hacer un manual de procedimientos? (Internet) Consultado en: https://softgrade.mx/manual-de-procedimientos/

Se recomienda que dentro de la estructura del Manual se le otorgue un apartado especial a cada requisito legal que establezca la normatividad aplicable. Lo anterior garantiza que cada uno de los requisitos se haya atendido y, en caso de que los manuales tengan que ser autorizados o sean revisados por los reguladores, sea fácil para ellos identificar cada uno de los mencionados requisitos.

A modo de ejemplo, las Disposiciones Generales SOCAP disponen que el manual de crédito *"Deberá contener las políticas y los procedimientos de crédito, y como mínimo los lineamientos siguientes: (…)*

> *b) Integración de expedientes de crédito: Las políticas y procedimientos para la integración de un expediente único por cada acreditado, en el cual se contenga cuando menos la documentación e información siguiente:*
>
> *1. Identificación del solicitante.*[21]"

De lo anterior, se recomienda que el apartado se titule "Integración de expedientes de crédito" y que contenga un subapartado que se titule "identificación del solicitante" y así respectivamente.

- Definir de manera clara las funciones y las responsabilidades de las áreas de la Entidad para tener mayor control y organización interna. Se recomienda ilustrar la estructura de la Entidad a través de un organigrama.
- Establecer el criterio u objetivo específico que se busca cumplir en el apartado del Manual y, posteriormente, describir los procesos y procedimientos para que se tenga claro qué es lo que se busca con el procedimiento.
- Contar con un mecanismo de evaluación y control interno para asegurar un estudio efectivo y la máxima protección posible contra errores, fraude y corrupción.

[21] Artículo 33 Disposiciones Generales SOCAP.

- Desarrollar un sistema presupuestario que establezca un procedimiento de control de las operaciones futuras, asegurando, de este modo, la gestión proyectada y los objetivos futuros[22].
- Disponer de controles válidos, de tal forma que se estimulen la responsabilidad y desarrollo de las cualidades de los empleados y el pleno reconocimiento de su ejercicio evitando la necesidad de controles superfluos, así como la extensión de los necesarios.

4.4 Evaluación de Riesgos.

Los Manuales de Riesgos se refieren a la asignación de funciones a distintas áreas en materia de administración de riesgos, riesgos de capitalización y demás riesgos que deben reconocer y prevenir las Entidades en sus operaciones como riesgos de crédito, de mercado, de liquidez y operativos, principalmente. Cada tipo de riesgo debe tener asignada una metodología para efecto de realizar la medición de éstos con base en parámetros que, si bien en algunos casos se encuentran predeterminados por la regulación, deben adaptarse a la realidad de cada Entidad. En ese sentido, en algunas Entidades, el riesgo informático o riesgos de ciberseguridad no se encuentran identificados o no cuentan con un desarrollo adecuado.

En la planeación de un Proyecto sugerimos, en el contexto de la evaluación de riesgos, llevar a cabo el siguiente ejercicio:

- Establecer por área o áreas responsables un modelo que permita establecer a qué tipo de riesgos quedaría expuesta la Entidad con base en las características del Proyecto.
- Realizar un modelo de riesgos que considere todas las características del Proyecto y aplique la metodología contenida en los Manuales de la Entidad.
- Analizar si es necesario realizar evaluaciones adicionales o de riesgos no contemplados expresamente en los Manuales de la Entidad debido al carácter novedoso de los Proyectos.

[22] *Gómez Giovanny. (Internet).* Manual de procedimientos: qué es, objetivos, estructura y su justificación frente al control interno. *Consultado en* https://www.gestiopolis.com/manuales-procedimientos-uso-control-interno/

Es posible que incluso el Regulador, en aquellos Proyectos donde sea necesaria su intervención, solicite la evaluación de riesgo bajo ciertos criterios específicos y adaptados a la naturaleza de lo que se desea implementar.

La evaluación de riesgos es la actividad fundamental para detectar las posibles amenazas a las que se encuentra expuesta la Entidad y le permite no sólo entender de manera cuantitativa y cualitativa la exposición a las mismas como resultado del Proyecto, sino a establecer estrategias de mitigación y, en su caso, ajustar las operaciones e infraestructura de la Entidad y términos concretos del Proyecto conforme a los resultados de esta evaluación.

SECCIÓN 5.- TRANSPARENCIA Y ORDENAMIENTO DE LOS SERVICIOS FINANCIEROS.

5.1 Conceptos Generales de Transparencia.

La Ley para la Transparencia y Ordenamiento de los Servicios Financieros ("LTOSF") es uno de los ordenamientos centrales en materia financiera, sobre todo en lo que concierne la relación entre Entidades y sus clientes externos finales. La revisión de este ordenamiento es esencial en los Proyectos que impliquen un nuevo producto debido a que:

- Establece reglas específicas para el otorgamiento de créditos y la realización de operaciones de las Entidades (e.g. cobro de intereses, uso de tarjetas).
- Establecer reglas sobre transparencia y cobro de comisiones por parte de las Entidades.
- Indica las bases para la fórmula del cálculo del Costo Anual Total ("CAT") y de la Ganancia Anual Total Neta ("GAT"). En ese sentido, es necesario revisar las disposiciones de Banxico al respecto, pues no a todo contrato emitido por las Entidades les son aplicables estos cálculos y las disposiciones que las acompañan. A manera de ejemplo, las Entidades no estarán obligadas a calcular el CAT de los créditos de arrendamiento financiero, factoraje financiero, descuento mercantil, créditos empresariales o corporativos, por cualquier monto, entre otros, de acuerdo con la disposición 3 de la Circular 21/2009 emitida por Banxico.
- Especifica las reglas de contratación frente al público en general (contratos de adhesión).
- Regula el contacto entre las Entidades y sus clientes en aspectos como cobranza y publicidad.
- Regula la divulgación de información sobre productos y servicios por parte de las Entidades.
- Fija las características de los estados de cuenta.
- Indica parámetros determinados para prácticas comerciales que no son aceptables (e.g. prohibición de "ventas atadas").

Condusef es el Regulador que ha emitido las disposiciones secundarias sobre la mayoría de los puntos anteriores, salvo por lo relacionado con el CAT, el GAT y los medios de disposición (tarjetas) que corresponde regular a Banxico.

En ese sentido el diseño de un nuevo producto o servicio por parte de una Entidad debe tomar en cuenta los aspectos anteriores. Para ello, sugerimos evaluar los Proyectos que tengan como objeto implementar un nuevo producto o servicio dirigido al público, según sea aplicable, conforme a los siguientes lineamientos:

- Ubicar si el tipo de producto o servicio materia del Proyecto (de ser el caso) va dirigido al público en general o si se trata de una operación única o poco frecuente que pretende llevar a cabo la Entidad (por ejemplo, celebración de un servicio que pudiera considerarse como no relevante para efectos regulatorios).
- Establecer los supuestos económicos del nuevo producto: costos, cobros, comisiones, tasas de interés, entre otras. Todas las comisiones deben hacerse públicas y registrarse en el Registro de Comisiones Vigentes ("RECO") administrado por Condusef; sin embargo, las mismas deben corresponder al catálogo que al respecto ha emitido dicho regulador. Asimismo, comisiones consideradas como fuera de mercado o abusivas podrían ser consideradas ilegales o incobrables.
- En el caso de productos, el Proyecto podría estar sujeto a las reglas de cobro de interés establecidas en la LTOSF (por ejemplo, la prohibición de cobrar intereses por adelantado, entre otras).
- En caso de que un área distinta a la legal elabore el Contrato de Adhesión materia del Proyecto, por la naturaleza especializada de los mismos, sugerimos solicitar el visto bueno de la Dirección Jurídica o el área equivalente para efecto de aprobar el formato respectivo y asegurarse que el mismo cumpla en el fondo y en la forma con lo establecido en la regulación. En algunos casos hemos observado que el área de crédito es la encargada de crear los contratos de las Entidades (ya que los contratos se preparan previamente) y el área legal se encarga de revisar que no existan cláusulas abusivas, impedimentos legales, condiciones contrarias a la legislación aplicable, entre otras cosas.
- Asegurarse que los documentos adicionales al producto o servicio sean válidos y sean cobrables conforme a las disposiciones en comento. Por ejemplo, en el caso

de pagarés, verificar que los mismos cumplan con los requisitos legales que permitirán su admisión en un juicio executivo mercantil.

- Consensuar entre las áreas legales y de marketing o publicidad que la información dirigida al público cumpla con las disposiciones de Condusef y que la información correspondiente esté disponible para el público.

Además de lo ya mencionado, es importante que las Entidades conozcan otros dos conceptos relacionados a la materia de transparencia que no se desarrollan en la LTOSF. Estos conceptos son el CAT y el GAT.

1. Costo Anual Total (CAT)

a) Es una medida del costo de un financiamiento. Es expresado en términos porcentuales anuales que, para fines informativos y de comparación, incorpora la totalidad de los costos y gastos inherentes a los créditos. Por ser un porcentaje anual, permite efectuar comparaciones directas entre las diferentes condiciones ofrecidas en el mercado por proveedores de créditos similares. El CAT es el indicador más importante para comparar el costo de los créditos.

b) El CAT incluye:

- Periodicidad de los pagos.
- Amortizaciones del principal.
- Intereses ordinarios.
- Comisiones, cargos y primas de seguros requeridas para el otorgamiento del crédito.
- Diferencia entre el precio del bien si se adquiere a crédito y su precio al contado.
- Bonificaciones y descuentos pactados en el contrato.

c) Uso de la tasa de interés del CAT: Se tiene que distinguir entre (i) publicidad; (ii) contrato; y (iii) estado de cuenta.

- Publicidad y propaganda: cuando se trate de productos de crédito que sean ofrecidos en el primer año de comercialización, la entidad deberá dar a conocer el CAT que resulte del cómputo de la estimación de las características del producto de crédito que dicha entidad pretenda establecer para cada producto. Cuando se trate de productos que hayan sido comercializados por más de un año, el CAT se calculará con base en la tasa de interés promedio de producto.
- Contratos: se utilizará la tasa de interés específica del producto y el cliente particular. En caso de que se ofrezcan créditos revolventes, la circular 21/2009 contempla características específicas.
- Estados de cuenta: se utilizará la tasa de interés personalizada del cliente.

2. Ganancia Total Anual (GAT)

a) Definición: Es el indicador del rendimiento de una operación de ahorro o inversión con el cual es posible comparar entre productos de acuerdo al beneficio o rendimiento total que ofrecen. Se trata de una herramienta de información y de comparación que permite al público conocer de manera sencilla el rendimiento total que podrían tener sus recursos, lo que promueve la competencia entre intermediarios y la transparencia en favor de los usuarios.

b) Elementos del GAT: Dado que se refiere a la "ganancia total" de una inversión o ahorro, se deben incorporar todos los elementos que inciden en su rendimiento efectivo, como son la tasa de interés, el monto del depósito, comisiones y otras características como la periodicidad.

c) ¿En qué operaciones pasivas debe de calcularse el GAT?

- Depósitos retirables con previo aviso, retirables en días preestablecidos, de ahorro, a plazo fijo; así como préstamos documentados en pagarés con rendimiento liquidable al vencimiento;
- Cualquier operación pasiva que en su nombre, publicidad o propaganda incluya las palabras "ahorro" o "inversión", o se induzca al público a suponer que se trata de un producto de ahorro o inversión; y

- Operaciones pasivas cuyos productos se dirijan a menores de edad.

d) Obligaciones de las Entidades: Conforme a las disposiciones aplicables, las entidades que deban incluir el GAT en los contratos, publicidad y propaganda tienen que:

- Anteponer las palabras “GAT nominal” y “GAT real” al valor correspondiente a cada una;
- Expresar la GAT nominal y la GAT real en términos porcentuales redondeada a dos decimales;
- Mostrar un solo valor para la GAT nominal y un solo valor para la GAT real, por lo que no deberán referirse máximos ni mínimos; e
- Incluir las leyendas “Antes de impuestos” y “La GAT real es el rendimiento que obtendría después de descontar la inflación estimada” en la misma página o pantalla en la que se muestren la GAT nominal y la GAT real.

5.2 Contratos de Adhesión.

Un “Contrato de Adhesión” es un documento elaborado unilateralmente por las Entidades para establecer en formatos uniformes los términos y condiciones aplicables a la celebración de una o más operaciones pasivas, activas o de servicios que lleven a cabo dichas entidades con los Usuarios de sus servicios, en el entendido de que estos últimos no podrán negociar dichos términos y condiciones.

En principio, se debe elaborar un Contrato de Adhesión por cada uno de los productos o servicios que la Entidad ofrezca. En términos generales será necesario elaborar un contrato nuevo conforme la Entidad ofrezca un nuevo producto y/o servicio.

Los Contratos de Adhesión que utilicen las Entidades Financieras para documentar operaciones con el público deberán cumplir con los requisitos que mediante disposiciones de carácter general ha establecido Condusef, entre los que se encuentran:

- Incluir una descripción detallada de la operación o servicio, características, términos, condiciones, así como los derechos y obligaciones que adquieren cada

una de las partes y la mención de los medios de disposición vinculados a la operación o servicio contratado;

- Mencionar la fecha de corte tratándose de créditos en cuenta corriente y las fechas para el cálculo de intereses en los demás productos o servicios financieros o el lugar en el cual podrán ser consultadas por el usuario;
- Indiciar la denominación, domicilio y dirección de internet de la Entidad, en su caso;
- Agregar el nombre completo del Usuario;
- Expresar las comisiones y tasas de interés;
- Mencionar la vigencia, modificaciones y terminación del Contrato de Adhesión;
- Servicios de atención al usuario;

La LTOSF establece que los Contratos de Adhesión pueden celebrarse con los clientes siempre que conste su consentimiento expreso por los medios electrónicos que al efecto se hayan pactado. De acuerdo con lo establecido en el artículo 11, párrafo octavo de la LTOSF los Contratos de Adhesión se pueden celebrar con la firma autógrafa de los clientes, mediante su huella digital, o bien, otorgando su consentimiento expreso por los medios electrónicos que se hayan pactado. Asimismo, los Usuarios pueden solicitar a través de medios electrónicos, ópticos o de cualquier otra tecnología, previamente pactados por las partes, la terminación anticipada de los Contratos de Adhesión. Las Entidades podrán utilizar un mecanismo de verificación de identidad para dichos efectos.

Los Contratos de Adhesión deben ser registrados por las Entidades en el Registro de Contrato de Adhesión de la Condusef ("RECA") para que los clientes de las Entidades puedan consultarlos. Las Entidades deben crear un registro por cada Contrato de Adhesión que maneje la Entidad, en el cual deben proporcionar información sobre (i) tipo de operación; (ii) producto o servicio que se oferta; y (iii) documentos que integren el contrato.

Relacionado con lo anterior, los estados de cuenta a través de los cuales las Entidades informan a los clientes de las operaciones o servicios deben emitirse de forma gratuita y mensual (o con la periodicidad pactada, siempre que no sea mayor a 6 meses) y contener los requisitos mínimos que establecen las disposiciones de la Condusef.

5.3 Publicidad.

Las Entidades deben ajustar su publicidad (incluyendo la que se realice a través de medios electrónicos) a los siguientes principios, entre otros:

- Veracidad y precisión de la información relacionada con los productos o servicios ofrecidos;
- Concordancia con el Contrato de Adhesión;
- Inclusión del CAT vigente, siempre que sea necesario que se incorpore;
- Abstenerse de incluir elementos de competencia desleal;
- Transparencia en las características y, en su caso, riesgos inherentes al producto o servicio;
- Transparencia en los requisitos para el otorgamiento de créditos con tasas preferenciales o determinados límites de crédito (en su caso); y
- Publicidad de las comisiones que cobran.

Las Entidades, en su página de Internet, deben incluir toda la información de los productos o servicios financieros que ofrezcan al público en general cumpliendo con los requisitos que establecen las disposiciones emitidas por Condusef. Asimismo, dicha página de Internet debe incluir otros aspectos relacionados con el régimen de las Entidades, incluyendo montos protegidos por el Fondo de Protección, así como un listado de los productos que ofrezcan y que sean garantizados por ese fondo, identificándolos por su nombre comercial. También, deben incluir la tasa de interés, rendimiento o descuento, y calcular el esquema de financiamiento y de pago, acorde con las características de la operación o servicio de que se trate incluyendo la tabla de amortización.

Las Entidades deben dar a conocer al público la existencia del Buró de Entidades Financieras en sus sucursales y página de internet, además de publicar de forma permanente en su página de internet el logotipo con el que se identifica al Buró, la descripción y alcances de éste y la indicación de que la información publicada corresponde únicamente a la Entidad y que para conocer toda la información deberá acudir al sitio oficial.

Además de la información que las Entidades deben poner a disposición del público en su página de internet y en la sucursal, estas deben proporcionar al Buró de Entidades Financieras la siguiente información para que sus clientes puedan consultarla en el sitio oficial de éste:

- Tipo de producto o servicio que se ofrece y características del mismo;
- Nombre comercial de la Entidad;
- Requisitos de contratación con la Entidad;
- Limitación del producto o servicio;
- Alcance del producto;
- Exclusiones o restricciones;
- Costos de contratación; y
- Dirección electrónica específica en que se encuentran sus programas.

5.4 Contraprestaciones.

En el momento de determinar la viabilidad de una comisión es preciso tener en mente las siguientes reglas.

- Las Entidades únicamente podrán cobrar comisiones que se vinculen con un servicio prestado al cliente, o bien por una operación realizada por él.
- Las Entidades no podrán cobrar más de una Comisión por un mismo acto, hecho o evento. Este mismo principio aplicará cuando así lo determine el Banco de México tratándose de actos, hechos o eventos en los que intervengan más de una Entidad.
- Las Entidades no podrán cobrar comisiones que inhiban la movilidad o migración de los clientes a otra entidad financiera.
- Las comisiones que las Entidades determinen deberán ser claras y transparentes.

En los créditos, préstamos o financiamientos que las Entidades otorguen, el pago de los intereses no podrá ser exigido por adelantado, sino únicamente por períodos vencidos.

Asimismo, conforme al artículo 9 de la LTOSF, las tasas de interés ordinarias y moratorias que aparezcan en los documentos que instrumenten los créditos, préstamos y financiamientos que otorguen las Entidades, así como las que se mencionen en los estados de cuenta, deberán expresarse en términos anuales y resaltarse en caracteres distintivos de manera clara, notoria e indubitable.

Es importante resaltar que las comisiones que se cobren a los clientes de las Entidades, al igual que los Contratos de Adhesión, deben inscribirse en el registro que la Condusef denominado Registro de Comisiones Vigentes ("RECO"). Para inscribir las comisiones, se deben cumplir con los requisitos mínimos que se establecen en las disposiciones especiales de la Condusef, tales como: (i) utilizar lenguaje sencillo y comprensible; (ii) identificar de manera clara el hecho, acto o evento que genera la comisión; (iii) no ubicarse dentro de las comisiones prohibidas de cobrar; etc.

5.5 Unidad Especializada de Atención a Usuarios.

Además de lo anterior, todas las Entidades y, en general, las entidades financieras, deberán contar con una Unidad Especializada de Atención a usuarios ("UNE"), quien será la encargada de atender cualquier consulta, reclamación y/o aclaración respecto a los productos y servicios de las Entidades. Esta obligación conlleva la de registrarse en el Registro de Unidades Especializadas de Atención a usuarios ("REUNE") al momento en que la Entidad se registra como entidad financiera ante el SIPRES y proporcionar la siguiente información en relación con la UNE:

- Nombre y datos de localización del titular de la UNE, así como de, en su caso, el o los encargados regionales.
- Entidades federativas en las que tengan sucursales u oficinas de atención al público.
- Modelo de aviso de datos de la UNE, con las especificaciones que establecen las disposiciones aplicables.

Aspectos característicos de la contratación electrónica.

En resumen, las LTOSF y las disposiciones secundarias emitidas por Condusef permiten la contratación electrónica, establecen reglas sobre la publicidad realizada por Internet y permiten el envío y generación de comprobantes de operación y estados de cuenta a través de medios electrónicos.

Este tema debe verse de manera complementaria con lo relacionado a Banca Electrónica que se menciona en la Sección 9 de la presente Guía Legal.

SECCIÓN 6.- PREVENCIÓN DE LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO.

Las Entidades se encuentran sujetas a Disposiciones PLD/FT para efecto de que las mismas no sean utilizadas, principalmente, para la realización de dos delitos (con todas sus variedades y excepciones): (i) el lavado de dinero, que consiste en una serie de pasos que tiene como fin realizar operaciones económicas o financieras que tienen por objeto dar una apariencia legal a cantidades o recursos que proceden de otros delitos, y (ii) el financiamiento al terrorismo, es decir, fondear y proveer recursos a organizaciones que tienen como fin usar el terror como medio de presión para alcanzar ciertos fines. Desde luego esta es una definición informativa, para ver la tipología completa sugerimos revisar los artículos 400 Bis, 400 Bis 1, 139, 139 Bis y 139 Ter, 139 Quáter y 139 Quinqui del Código Penal Federal.

Las Disposiciones PLD/FT tienen aspectos que inciden de manera directa en la manera de operar los servicios financieros de la Entidades. En este caso corresponde tanto al Oficial de Cumplimiento y, de haberlo, al Comité de Comunicación y Control, asegurar y vigilar la aplicación de dichas reglas.

6.1 Conceptos Generales en materia de PLD/FT.

Entre los conceptos más importantes para efecto de contextualizar la importancia de las Disposiciones PLD/FT en los Proyectos, se encuentran los siguientes:

- Identificación de Clientes. Se refiere a la implementación de lineamientos por parte de las Entidades que les permita recolectar, verificar y actualizar datos pertenecientes a sus clientes (no únicamente de ellos, sino personas que también podrían estar relacionadas con ellos en el contexto del servicio a contratarse). Esto es lo que en la jerga internacional se conoce como el know your customer (KYC).
- Reportes. Las Entidades están obligadas a entregar a CNBV una serie de reportes relacionados con los aspectos PLD/FT, por ejemplo, un “Reporte de Operaciones Inusuales”, “Reporte de Operaciones Relevantes”, “Reportes de Operaciones en Efectivo con Dólares de los Estados Unidos de América”, “Reporte de Operaciones Internas Preocupantes”, entre otros y cuyo detalle no es materia de la presente Guía Legal. Dichos reportes tienen como objeto proveer de información a CNBV y a

SHCP sobre las operaciones de la Entidad y, en su caso, alertar sobre conductas que pudieran favorecer conductas ilícitas.

- Enfoque basado en riesgos. Las Entidades deberán diseñar e implementar una metodología para llevar a cabo una evaluación de Riesgos a los que se encuentran expuestas derivado de sus productos, servicios, clientes, países o áreas geográficas, transacciones y canales de envío o distribución con los que operan. Esta metodología deberá establecer y describir todos los procesos que se llevarán a cabo para la identificación, medición y mitigación de los Riesgos para lo cual deberán tomar en cuenta tanto los factores de Riesgo que para tal efecto hayan identificado como la información que resulte aplicable dado el contexto de cada Entidad contenida en la evaluación nacional de riesgos de lavado de dinero y financiamiento al terrorismo ("Evaluación Nacional de Riesgos")[23] y sus actualizaciones. Estos reportes también implican que las Entidades deban realizar monitoreos periódicos de dichos riesgos.

- Monitoreo. Los Reguladores ponen a disposición de las Entidades una serie de listas que estas deben verificar para efecto de determinar (i) si le es posible celebrar operaciones con entidades domiciliadas o con presencia en jurisdicciones donde no se aplican de manera suficiente medidas PLD/FT, (ii) si alguno de sus clientes o usuarios se encuentre dentro de la "Lista de Personas Bloqueadas[24]", incluyendo a cualquier tercero que actúe en nombre o por cuenta de los mismos, y (iii) si una persona debe ser considerada como "Persona Políticamente Expuesta[25]".

[23] Es un ejercicio de autoevaluación que permite a los países redefinir su política en la materia, orientando los recursos hacia la prevención y mitigación de aquellos factores que representan un mayor riesgo de lavado de dinero, financiamiento al terrorismo y financiamiento a la proliferación de armas de destrucción masiva.

La Evaluación Nacional de Riesgos tiene como objetivo lograr, mediante un esfuerzo organizado, sistemático y plural la identificación, análisis, evaluación y comprensión de los riesgos que implican el lavado de dinero, financiamiento al terrorismo y financiamiento a la proliferación de armas de destrucción masiva en el país a efecto de implementar y desarrollar un régimen eficiente, eficaz, coordinado y de calidad en la materia.

Unidad de Inteligencia Financiera. Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo en México 2019-2020. (Internet) Consultado en: https://www.uif.gob.mx/work/models/uif/comunicados/imp/ENR2019-2020/

[24] Es la lista que contiene los nombres de las personas que han sido identificadas por realizar actividades con recursos de procedencia ilícita conforme a los parámetros internacionales y nacionales.

[25] Aquel individuo que desempeña o ha desempeñado funciones públicas destacadas en un país extranjero o en territorio nacional, considerando entre otros, a los jefes de estado o de gobierno, líderes políticos, funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales o funcionarios o miembros importantes de partidos políticos.

- Sistema Automatizado. Las Entidades están obligadas a contar con un "Sistema Automatizado" como parte de su Infraestructura Tecnológica, que desarrolle diversas funcionalidades. El sistema está definido con base en finalidades o atribuciones que debe desarrollar de manera informática, no tanto a un tipo de tecnología específica. La regulación no establece estándares técnicos como tales sino funcionalidades que deben cumplirse por dicho sistema, por lo que en la práctica existen sistemas sencillos (Entidades con baja operación o de creación reciente) y otros que, debido al volumen de datos, requieren de automatizaciones más complejas.

6.2 Clasificación de Clientes por Grado de Riesgo.

Las Entidades deberán clasificar a sus Clientes por grado de riesgo y establecer, como mínimo, dos clasificaciones: (i) alto riesgo y (ii) bajo riesgo. Las Entidades podrán establecer niveles intermedios de Riesgo adicionales a las clasificaciones antes señaladas.

Con la finalidad de determinar el grado de riesgo en que deba ubicarse a los Clientes al inicio de la relación comercial, las Entidades deberán considerar la información que les sea proporcionada por estos al momento de la apertura de la cuenta o celebración del contrato respectivo. Adicionalmente, las Entidades deberán llevar a cabo, al menos, dos evaluaciones por año calendario, a fin de determinar si resulta necesario o no modificar el perfil transaccional y/o clasificar a estos en un grado de riesgo diferente al inicialmente considerado. Las evaluaciones se realizarán sobre aquellos Clientes cuya apertura de cuenta o celebración de contrato se hubiere realizado al menos con seis meses de anticipación a la evaluación correspondiente.

Para determinar el grado de riesgo en el que deban ubicarse los Clientes, cada Entidad establecerá en sus políticas, criterios, medidas y procedimientos internos los criterios conducentes para determinar el grado de riesgo, tomando en cuenta, entre otros aspectos, los siguientes:

Se asimilan a las Personas Políticamente Expuestas, el cónyuge, la concubina, el concubinario y las personas con las que mantengan parentesco por consanguinidad o afinidad hasta el segundo grado, así como las personas morales con las que la Persona Políticamente Expuesta mantenga vínculos patrimoniales.

- Los antecedentes del Cliente.
- Profesión, actividad o giro del negocio del Cliente.
- Origen y destino de los recursos del Cliente.
- Lugar de residencia del Cliente.
- Demás circunstancias que determine la Entidad.

Las Entidades clasificarán a sus Clientes en función al grado de riesgo de éstos en los términos de los mecanismos establecidos en el Manual PLD/FT (ver Sección 4 Control Interno y Manuales).

Tratándose de Personas Políticamente Expuestas de nacionalidad mexicana, las Entidades determinarán si el comportamiento transaccional corresponde razonablemente con las funciones, nivel y responsabilidad de dichas personas, de acuerdo con el conocimiento e información de que dispongan las Entidades.

6.2.1 Alto Riesgo

Previamente a la apertura de cuentas o celebración de contratos de Clientes que, por sus características, pudiesen generar un alto Riesgo para la Entidad al menos un directivo o su equivalente que cuente con facultades específicas para aprobar la aportación de capital, apertura o celebración de dichas cuentas o contratos, según corresponda, deberá otorgar, por escrito o en forma electrónica, la aprobación respectiva. Asimismo, la Entidad deberá prever en el Manual PLD/FT los procedimientos para hacer del conocimiento al Comité de Comunicación y Control o al Oficial de Cumplimiento sobre la celebración de aquellas cuentas o contratos que puedan generar un alto Riesgo, y para coordinar las actividades de seguimiento de dichas operaciones para dictaminarlas, en su caso, como operaciones inusuales o internas preocupantes.

La aprobación anterior se debe realizar de igual forma en los casos en que con posterioridad al inicio de la relación comercial, la Entidad detecte que un Cliente reúne los requisitos para ser considerado Persona Políticamente Expuesta y, además, como de alto riesgo.

Las Entidades aplicarán a los Clientes que hayan sido catalogados de alto riesgo, así como a los Clientes nuevos que reúnan tal carácter, cuestionarios de identificación que permitan obtener más información sobre el origen y destino de los recursos y las actividades y operaciones que realizan o que pretendan llevar a cabo. Es importante que las Entidades consideren que, conforme a las Disposiciones PLD/FT siempre serán considerados como Clientes de alto riesgo las Personas Políticamente Expuestas extranjeras.

En las operaciones que realicen los Clientes que hayan sido clasificados de alto Riesgo, las Entidades adoptarán medidas y procedimientos razonables para conocer el origen de los recursos y procurarán obtener los siguientes datos adicionales de identificación:

- Tratándose de Clientes personas físicas: datos que permitan identificar al cónyuge y dependientes económicos del Cliente, así como las personas morales con las que puede mantener vínculos patrimoniales.
- Tratándose de Clientes personas morales mercantiles: datos que permitan conocer su estructura corporativa y los accionistas o socios que ejerzan el control sobre ellas, requiriendo información relativa a la denominación, nacionalidad, domicilio, objeto social y capital social de las personas morales que conforman el grupo empresarial o, en su caso, los grupos empresariales que integran al consorcio del que forme parte el Cliente.
- Tratándose de Clientes personas morales con carácter de sociedades o asociaciones civiles: datos que permitan identificar a la persona o personas que tengan control sobre tales sociedades o asociaciones.

Además de lo anterior, las Entidades deberán verificar, cuando menos una vez al año, que los expedientes de identificación de los Clientes clasificados como de alto Riesgo cuenten con todos los datos y documentos actualizados.

6.2.2 Bajo Riesgo

Son consideradas como cuentas de bajo riesgo las cuentas de depósito a la vista en moneda nacional que ofrezcan las Entidades y se trate de Clientes que sean personas físicas cuya operación se encuentre limitada a abonos iguales al equivalente en moneda

nacional a mil Unidades de Inversión por Cliente ("UDI"), en el transcurso de un mes calendario.

A los Clientes clasificados con grado de bajo riesgo se les podrán aplicar las medidas simplificadas contempladas en las Disposiciones PLD/FT, consistentes en integrar los expedientes de identificación de dichos Clientes únicamente con los datos relativos al nombre completo, sin abreviaturas, fecha de nacimiento y domicilio de estos. En este caso, los datos relativos al nombre y fecha de nacimiento del Cliente deberán ser obtenidos de su identificación oficial.

La Entidades podrán establecer en su Manual PLD/FT, o bien, en algún otro documento o manual elaborado por la misma, criterios y elementos de análisis con base en los cuales se considerarán productos y servicios distintos a las cuentas de depósito a la vista en moneda nacional como de bajo Riesgo, incluyendo, los criterios y elementos de análisis con base en los cuales considere a tales productos y servicios como de bajo riesgo, incluyendo, entre otros, el monto máximo de los niveles transaccionales permitidos para efectos de seguir considerando a dichos productos dentro de la categoría de riesgo señalada.

En el supuesto de que el nivel transaccional de cualquiera de los productos o servicios sobrepase el monto máximo establecido por la Entidad para que sean considerados como de bajo Riesgo, la Entidad deberá proceder a integrar el expediente de identificación del Cliente respectivo con la totalidad de la información y documentación que corresponda, en términos de las Disposiciones PLD y Manual PLD/FT.

Las Entidades no podrán aplicar a sus Clientes las medidas simplificadas cuando tengan sospecha fundada o indicios de que los recursos, bienes o valores que sus Clientes pretendan usar para realizar una Operación, pudieran estar relacionados con los actos o conductas a que se refieren los artículos 139 Quáter o 400 Bis del Código Penal Federal.

6.3 Sistema Automatizado.

Cada Entidad, como parte de su Infraestructura Tecnológica, deberá contar con sistemas automatizados que desarrollen, entre otras, las siguientes funciones:

(i) Conservar, actualizar y permitir la consulta de los datos relativos a los registros de la información que obre en el respectivo expediente de identificación de cada Cliente;

(ii) Generar y transmitir de forma segura a la SHCP por conducto de la CNBV, la información relativa a los reportes que debe generar la Entidad, así como aquella que deba comunicar a dichos Reguladores,

(iii) Clasificar los tipos de Operaciones o productos financieros que ofrezcan las Entidades a fin de detectar posibles Operaciones Inusuales;

(iv) Detectar y monitorear las Operaciones realizadas en una misma cuenta o por un mismo cliente;

(v) Ejecutar el sistema de alertas que permita detectar cambios en el perfil transaccional del cliente;

(vi) Contribuir a la detección, seguimiento y análisis de la información que sea relevante en el contexto de los reportes que deben entregar a SHCP a través de CNBV, la información que haya sido proporcionada por el cliente al inicio de la relación comercial, los registros históricos de las Operaciones realizadas por este, el comportamiento transaccional, los saldos promedio y cualquier otro parámetro que pueda aportar mayores elementos para el análisis de este tipo de Operaciones;

(vii) Agrupar en una base consolidada las diferentes cuentas y contratos de un mismo Cliente, a efecto de controlar y dar seguimiento integral a sus saldos y Operaciones;

(viii) Conservar registros históricos de Operaciones materia de reportes;

(ix) Servir de medio para que el personal de las Entidades reporte a las áreas internas que las mismas determinen, de forma segura, confidencial y auditable, las posibles Operaciones Inusuales u Operaciones Internas Preocupantes;

(x) Mantener esquemas de seguridad de la información procesada que garanticen la integridad, disponibilidad, auditabilidad y confidencialidad de la misma;

(xi) Proveer la información que las Entidades incluirán en la metodología de evaluación de Riesgos;

(xii) Ejecutar un sistema de alertas respecto de aquellas Operaciones que se pretendan llevar a cabo con personas que se encuentren dentro de las listas que deben consultar las Entidades, y

(xiii) Facilitar la verificación de los datos y documentos proporcionados de forma remota por el Cliente.

Como se mencionó, el Sistema Automatizado puede beneficiarse de una serie de tecnologías y aplicaciones para efecto de cumplir con sus objetivos. Al respecto, ver Sección 20 Automatización de Procesos.

6.4 Identificación a Distancia.

La identificación del Cliente debe realizarse de acuerdo con el tipo de persona de que se trate (e.g. física, moral, nacional o extranjera). Asimismo, el nivel de identificación o de información y datos que se deberá solicitar de cada cliente puede variar de acuerdo a su clasificación: si determina que el Cliente cae en cierta categoría (es decir, que por sus características existe la posibilidad más o menos actual de que pueda utilizar la Entidad para actividades ilícitas), entonces la Entidad debe solicitar información adicional (*enhanced due diligence*) o abstenerse de realizar la contratación respectiva, según sea el caso.

La regla general es que las Entidades deben integrar y conservar, previamente, un expediente de identificación de cada uno de sus Clientes cuando estos, de manera presencial, realicen aportaciones al capital social de las mismas, abran una cuenta o celebren un contrato para realizar operaciones de cualquier tipo.

Hay que tomar en cuenta que cuando la apertura de una cuenta o la celebración de un contrato se lleve a cabo a través de comisionistas facultados para celebrar Operaciones a nombre y por cuenta de las Entidades, el expediente de identificación puede ser integrado y conservado por dichos comisionistas. Para tales efectos, la Entidad deberá convenir

contractualmente con el comisionista de que se trate la obligación de este de mantener dicho expediente a disposición de aquella para su consulta, así como proporcionarlo a la propia Entidad para que pueda presentarlo a la SHCP o a la CNBV, según se requiera. Esto es relevante para la contratación de comisionistas, tal como se menciona en la Sección 15 del presente documento, en donde se habla sobre la Contratación de Proveedores y Comisionistas.

Adicionalmente, las Entidades deben convenir contractualmente con los comisionistas la obligación de estos de:

(i) Obtener, previo a la apertura de cuentas o celebración de contratos, la información y documentación para la integración del expediente de identificación respectivo.

(ii) Mantener los expedientes a disposición de CNBV y SHCP.

(iii) Contar con mecanismos para que las propias Entidades puedan verificar que los expedientes se encuentren integrados correctamente.

Las Entidades pueden llevar a cabo el proceso de identificación no presencial de clientes (o potenciales clientes) personas físicas de nacionalidad mexicana para la apertura de cuentas de depósito.

Las Entidades, para efectos de la identificación de sus clientes o potenciales Clientes que sean personas físicas de nacionalidad mexicana, en la celebración no presencial de contratos para la apertura de cuentas de depósito, siempre que se pacte en los contratos respectivos que la suma de los abonos en el transcurso de un mes calendario no exceda del equivalente en moneda nacional a 30,000 UDIs, así como de créditos comerciales que se otorguen a personas físicas con actividad empresarial y créditos al consumo, en ambos casos por montos menores al equivalente en moneda nacional a 60,000 UDIs, podrán ser objeto de identificación no presencial, siempre que[26]:

[26] Ver Anexo 2 de las Disposiciones PLD/FT

- Obtengan la previa aprobación de CNBV.
- Requiera a la persona física de que se trate el envío de un formulario a través del medio electrónico establecido por la propia Entidad en el cual se debe incluir cierta información necesaria para su identificación, así como el producto o servicio que se pretende contratar.
- El cliente envíe en formato digital los documentos necesarios para identificarlos y se requiera que dicho solicitante se tome una fotografía.
- La Entidad debe verificar si dicho solicitante ya tiene la calidad de cliente y, en su caso, verificar que los datos coincidan con los registros de la Entidad, así como confirmar ciertos datos proporcionados por el solicitante (CURP, INE) a través de mecanismos oficiales, por ejemplo, la página oficial del Registro Nacional de Población en que se puede consultar el CURP.
- Informar al solicitante del procedimiento para desarrollar la comunicación en tiempo real y entregar un código de un solo uso para requerirlo previo al inicio de la comunicación.
- Llevar a cabo la comunicación mediante guías de diálogo y ser conservada sin ediciones y en su totalidad, así como observar ciertos requisitos tendientes a su verificación y fidelidad, incluyendo toma de imágenes. Para este requisito se exige que la tecnología permita lograr una identificación fehaciente del entrevistado con un nivel de fiabilidad aceptable conforme a la normatividad.
- Suspender el proceso de contratación en caso de que la calidad o imágenes no permitan realizar la plena identificación, no se presenten las identificaciones requeridas, la información de los documentos no coincida con los registros de entidades públicas, el código de un solo uso no sea confirmado, entre otros supuestos.

La tecnología utilizada para estos procedimientos deberá ser aprobada por el responsable de riesgos o su equivalente o, en caso de no contar con este, por el Comité de Auditoría o el órgano de administración de la Entidad

Las Entidades que abran una cuenta o celebren un contrato a través de Dispositivos[27] de forma no presencial a Clientes, conforme a las Disposiciones PLD/FT, además de los datos de identificación ordinarios, deberán requerir y obtener de sus Clientes, con previo consentimiento de estos, la "Geolocalización del Dispositivo" desde el cual estos abran la cuenta o celebren el contrato, así como: (a) Clave de elector, en su caso, (b) consentimiento expreso, (c) correo electrónico o teléfono celular, entre otros requerimientos. Las Entidades no deberán llevar a cabo la apertura de la cuenta o la celebración del contrato de forma no presencial con los Clientes personas físicas de nacionalidad mexicana o extranjera, cuando no recaben el dato relativo a la Geolocalización. El consentimiento podrá obtenerse mediante la Firma Electrónica, Firma Electrónica Avanzada (ver Sección 12 Implementación de Firma Electrónica), o bien, conforme a los demás supuestos que establezcan las Disposiciones PLD/FT.

Las Entidades pueden recabar las versiones digitales de la documentación de identificación de los clientes de forma no presencial y a través de medios ópticos o de cualquier otra tecnología. Las versiones digitales que las Entidades recaben para efectos de identificación deberán permitir su verificación en términos de las Disposiciones PLD/FT.

Las Entidades, salvo algunas excepciones, están obligadas por regla general a realizar una entrevista previa a la celebración de un contrato con los Clientes. No obstante, en el caso de las cuentas que las Entidades clasifiquen como bajo riesgo, las Entidades pueden llevar a cabo la recepción o captura de los datos de forma remota en sustitución a la entrevista antes mencionada (Ver Sección 13 Apertura de Cuentas Remotas). Los resultados de la entrevista deben asentarse de forma escrita o electrónica. La entrevista se puede realizar de manera remota.

En lo relativo a las cuentas de bajo riesgo, las Entidades podrán llevar a cabo la recepción o captura de los datos de forma remota, siempre y cuando la Entidad de que se trate verifique la autenticidad de los datos del Cliente mediante un procedimiento de validación remota de datos y documentos proporcionados por los Clientes.

[27] Dispositivo, significa el equipo que permite acceder a la red mundial denominada Internet, el cual puede ser utilizado para realizar aperturas de cuenta o celebrar contratos, así como realizar operaciones.

6.5 Enfoque basado en Riesgos.

La metodología de evaluación de Riesgos, para su diseño debe considerar lo siguiente:

- Identificación de indicadores asociados a cada uno de los Riesgos a los que pudiera estar expuesta la Entidad, incluyendo sin limitar aquellos que se relacionan con los productos y servicios ofrecidos, clientes y usuarios, países y áreas geográficas, así como transacciones y canales de envío.
- Emplear una metodología de medición de Riesgos que relacione los indicadores y elementos mencionados anteriormente, asignando un peso a cada uno de ellos de manera consistente y conforme a su importancia.
- Identificar los Mitigantes que la Entidad tiene implementados al momento de diseñar la metodología.

La metodología diseñada debe aplicarse para efecto de conocer los Riesgos a los que está expuesta cada Entidad y, en su caso, tomar las medidas correspondientes. Todo esto debe revisarse de manera constante para mantener protegida a la Entidad de Riesgos nuevos o potenciales.

En la implementación de un Proyecto, la metodología del enfoque basado en riesgo es relevante pues puede ocurrir que:

- Derivado de la naturaleza del Proyecto, la exposición al Riesgo de la Entidad sea tan alta que el Proyecto deba modificarse o, en algunos casos, considerarse totalmente inviable en caso de que los Mitigantes no sean suficientes para prevenir el riesgo de posibles conductas ilícitas.
- En caso de nuevos productos o servicios que requieran canales no contemplados anteriormente por la Entidad, debe evaluarse la posibilidad de modificar el enfoque basado en Riesgo de la Entidad para establecer nuevos indicadores e incluso ajustar la medición de Riesgos e incorporar las Mitigantes correspondientes.
- Vigilar que el Proyecto no presente inconsistencias entre el Manual de Cumplimiento y la metodología del enfoque basado en Riesgos.

6.6 Digitalización y PLD/FT.

La automatización de procesos y funciones (por ejemplo: RPA, por sus siglas en inglés) es una de las últimas tendencias en materia PLD/FT, las cuales consisten en el uso de programas informáticos para realizar tareas repetitivas y que son poco atractivas para los humanos o, en la mayoría de los casos, requieren un uso intensivo de recursos humanos provocando ineficiencias en costos.

Hay dos términos que deben ser entendidos de manera separada con base en sus objetivos:

- Los procesos de automatización de funciones consisten en el uso de software para automatizar sistemas mediante la replicación de las acciones de una persona real al interactuar con dichos sistemas. En otras palabras, se realizan estos procesos a través de bots que interactúan con la Infraestructura Tecnológica ya existente de las Entidades para realizar la entrada de datos, procesar transacciones o responder consultas. Por ejemplo, los chatbots, que son ampliamente utilizados en muchos sitios web, son representantes de RPA.
- Inteligencia Artificial ("IA"), consiste en la simulación de procesos de inteligencia humana mediante sistemas informáticos. Estos procesos incluyen el aprendizaje mediante la adquisición de información para el uso y transformación de datos, el uso del contexto y las reglas para llegar a conclusiones y adquirir "experiencia" en el desarrollo de sus tareas. Estos ámbitos incluyen el reconocimiento de imágenes, visión artificial, reconocimiento de voz, generación de lenguaje natural y análisis de sentimientos.

No se trata de términos excluyentes. La automatización de funciones se beneficia normalmente de los adelantos de la IA. Ambas se refieren a la automatización, solo que la IA se orienta más al procesamiento de los datos (por ejemplo, analizar patrones de Operaciones u orientar decisiones con base en información) y la automatización de funciones a los procesos (reproducción de información de un archivo) que necesitan en gran medida del apoyo humano para realizarse. Algunas aplicaciones eficaces, por ejemplo, la identificación de operaciones fraudulentas en los casos de grandes volúmenes transaccionales puede beneficiarse de ambas tecnologías.

Para efecto de que una Entidad valore si la automatización de funciones es algo adecuado para ellos, deben realizar un plan de automatización hacia dentro de la Entidad que define los aspectos que deben someterse al mismo, empezando por lo siguiente:

- Considerar los costos y los proveedores adecuados para ello. Si bien aún estamos en una etapa donde un número pequeño de empresas (no digamos Entidades) aún no han adoptado estas tecnologías, su presencia en la vida cotidiana está muy presente: por ejemplo, en las sugerencias de compras de sitios como Amazon.
- Determinar si existe la capacitación necesaria dentro de la Entidad para efecto de poder operar de manera continua las tecnologías.
- Identificar y categorizar procesos con el apoyo del Oficial de Cumplimiento y de las áreas de negocio que manejan información relevante en materia PLD/FT. En caso de las Entidades, los procesos más relevantes en materia de PLD son, por normativa: (i) identificación de Clientes; (ii) monitoreo de operaciones y de clientes (screening); y (iii) análisis de parámetros para determinar el envío de ciertos reportes. Sin embargo, cada Entidad debe reconocer cuáles generan más información o tienen posibilidad de automatizarse para ahorrar recursos a la organización y dejar libre al personal para realizar tareas de más alto nivel.
- Mapear cada uno de los procesos indicados anteriormente: (i) identificar a las personas involucradas (en este caso el Oficial de Cumplimiento y el Director General son las personas con responsabilidades centrales en materia de PLD/FT), (ii) evaluar si las oportunidades de automatización son realistas (presupuestaria y normativamente), (iii) evaluar e identificar a los proveedores, y (iv) estructuración del Proyecto conforme a lo establecido en la **Sección 2.**
- Identificar ineficiencias en la administración de los datos de la Entidad. Es común que algunos Sistemas Automatizados utilicen aún para algunos procesos hojas de cálculo en Excel que agotan su utilidad rápidamente cuando es necesario manejar volúmenes amplios de datos o si es precioso vincularlos a otros procesos, o cuando es preciso extraer lecciones valiosas de ellos (mala integración de los datos).
- Hacer una encuesta o requerir la opinión de los encargados de los procesos relevantes de PLD/FT sobre su experiencia en el manejo de tecnologías y en su actitud hacia la misma. La cultura corporativa es un factor importante para efecto de alcanzar el éxito de una nueva tecnología.

- Explorar la posibilidad de aplicar una prueba de concepto antes de comenzar el Proceso (ver Sección 2 Aspectos Generales de la Administración de un Proyecto Legal).
- Asegurarse de que los servicios secundarios que permitirán la automatización son accesibles y viables (operativa y financieramente). En muchos casos la necesidad de contratar servicios en la nube para el procesamiento de información o servicio similares suele ser necesaria (e.g. Google, Amazon, Microsoft).
- Involucrar a las personas encargadas de ciberseguridad en el Proyecto.
- A partir del año 2019, se estableció el requerimiento de identificar la "Geolocalización" del dispositivo a través del cual se realiza la contratación digital. Este dato se refiere a las coordenadas geográficas de latitud y longitud en que se encuentre el dispositivo. De acuerdo con las Disposiciones PLD, las Entidades tendrán prohibido realizar la apertura de cuentas o la celebración de contratos no presenciales con personas físicas cuando no sea posible o no se recabe la Geolocalización del dispositivo del que se trata.

Cabe mencionar que, aunque las Disposiciones PLD explícitamente permiten a las Entidades llevar a cabo procesos de contratación remota con sus potenciales clientes, este elemento puede estar sujeto a criterios de la CNBV al respecto. En relación con lo anterior, sugerimos consultar a la CNBV previo a cualquier inversión o ejecución de un proyecto de contratación remota.

Puntos clave de la automatización de procesos y funciones

Gráfica 6. Puntos clave de la automatización de procesos y funciones. Fuente: Vite Abogados

» *Límites de la digitalización*

La digitalización de los procesos (tanto de PLD/FT), como de cualquier otra índole, deben ser a la medida del plan de negocios de cada Entidad. En el mercado existe mucha expectación y ruido por temas como los que acabamos de mencionar (IA en especial). De cualquier forma, existe gran cantidad de información emitida por proveedores de servicios de dichas tecnologías. Esto es positivo, pues la adopción de nuevas ideas y su discusión lleva al deseo de innovar en las empresas de todos los sectores. Sin embargo, un proceso de implementación de IA debe ser cuidadoso y depende en gran medida de la identificación de necesidades concretas, de la existencia de deficiencias o retrasos en procesos repetitivos, o en planes de expansión que requieran cambios sustanciales en la cantidad de datos a ser manejados por las Entidades. Igualmente, está sujeto al presupuesto que las Entidades tengan destinado a la digitalización de la Entidad y las

capacidades financieras propias (desarrolladas de forma más extensa en la parte III de la presente Guía Legal). En todo caso, no todo proceso de digitalización debe implicar el cambio de procesos de la noche a la mañana: existen tareas tan simples (y requeridas por la regulación) que es tedioso y complicado hacerlas manualmente, como es el tema de los formularios o el vaciado de información de clientes a base de datos (y su posterior consulta).

Las Entidades, por regulación, deben contar un Sistema Automatizado con las características descritas en el numeral 6.3 anterior. Es una obligación contar con una herramienta informática y, sobre ella (y sus funcionalidades básicas), es recomendable construir las bases para procesos de transformación que, aun cuando no son idealmente eficientes, al ser continuos, pueden tener un impacto importante en el largo plazo.

SECCIÓN 7.- PREVENCIÓN DE FRAUDE.

El sector financiero habitualmente enfrenta riesgos importantes en algunas materias, por ejemplo, en materia de operaciones con recursos de procedencia ilícita y fraude. Previendo lo anterior, la CNBV ha establecido lineamientos y políticas mínimas que deben cumplir las Entidades para prevenir el fraude y mitigar los riesgos vinculados con lo anterior. Estas políticas y procedimientos normalmente se documentan en un Manual que debe entregarse junto con la solicitud de autorización para organizarse y operar que presenten las entidades; sin embargo, a medida que las Entidades desarrollan nuevas líneas de negocios y modifican la forma en la que ofrecen sus productos y servicios, los riesgos también cambian y, de no contar con políticas y lineamientos para prevenir el fraude que atiendan esos nuevos riesgos específicos, las Entidades pueden quedar expuestas y ser el objeto de fraude o ser utilizados como vehículos para cometer fraude.

7.1 Consideraciones regulatorias.

La prevención de fraude en las Entidades implica considerar los siguientes aspectos regulatorios para una estrategia adecuada:

- Modificaciones a los Manuales internos de las Entidades o, en su caso, creación de políticas adicionales, ya que las políticas y mecanismos de prevención de fraude deben documentarse para que sean efectivas y contar con definición clara que afecta temas de control interno y PLD/FT. Las Entidades, al vincular este tema al control interno de la Entidad y el Manual PLD/FT, deben considerar las modificaciones y presentarlas ante la CNBV antes de plasmarlas en el mencionado documento (Ver Sección 4 Control Interno y Manuales)
- Modificaciones a los controles internos de las Entidades. Estas modificaciones pueden comprender reestructuras a nivel organizacional, elaboración de nuevos documentos de control, contratación de especialistas en materia de prevención de fraudes o capacitación de personal existente para que conozca de la materia. Cuando exista una modificación importante, sobre todo a los temas PLD/FT al interior de las Entidades, debe entregarse a CNBV una copia de dichas modificaciones.

- Disposiciones de contratación de proveedores para contratar un proveedor en materia de prevención de fraudes. Típicamente, las Entidades optan por contratar a un proveedor especialista en la materia para que provea de sistemas y experiencia. Dependiendo del grado del proveedor, las Entidades pueden tener que observar los requisitos para la contratación de proveedores que establece la CNBV (Ver Sección 15 Contratación de Proveedores y Comisionistas).

7.2 Marco general de prevención de fraude.

La creación de un marco general de prevención de fraudes debe considerar diversos elementos para asegurar su efectividad. En primer lugar, el marco general de prevención de fraude debe considerar los requisitos legales y regulatorios mencionados previamente. A modo de ejemplo, el Comité de Organizaciones Patrocinadoras de la Comisión *Treadway* (o COSO, por sus siglas en inglés)[28] ha determinado que un marco de prevención de fraude debe considerar los siguientes elementos[29]:

Generar un ambiente interno disuasor y que evite el fraude interno. Puede asumirse que, si los directivos relevantes de una Entidad consistentemente actúan y se conducen en forma adecuada, existe una presunción razonable de que los empleados y demás funcionarios también lo harán.

- Contar con mecanismos y políticas para medir el riesgo de fraude. Es necesario que cada Entidad cuente con políticas y mecanismos adecuados a su operación en forma individual. Cada entidad debe tener la capacidad de evaluar los riesgos a los que está expuesta cada área para poder determinar el grado de riesgo de fraude que representa cada una de ellas.
- Contar con actividades de supervisión de control interno. Estas actividades, igualmente, deben ser específicas a la operación de cada entidad. A pesar de que existen actividades generales y buenas prácticas que las Entidades pueden adoptar para prevenir y detectar fraudes, deben crearse actividades ad hoc para la operación de cada Entidad que se ajusten a su personal, sus actividades principales y los riesgos más altos que enfrenta. Asimismo, estas actividades deben

[28] Para más información, visitar el sitio oficial de COSO: https://www.coso.org/Pages/default.aspx
[29] Dawson, Steve. (2015) Internal Control/Anti-Fraud Program Design for the Small Business.

comprender a todo el personal de las Entidades, incluyendo a los accionistas o Socios.

- Documentación de las actividades y operaciones. Todos los mecanismos descritos en esta sección deben estar documentados para su fácil consulta, conocimiento y actualización. En el caso de las SOCAP se requiere que dichas Entidades cuenten con un Manual de Control interno contemple, entre otras cosas, políticas y mecanismos de prevención de fraude.
- Comunicación. Este elemento se refiere a dos puntos principales: (i) en primer lugar, los mecanismos y políticas de control interno se deben comunicar a los empleados de la Entidad para su correcta implementación, y (ii) debe existir un ambiente de comunicación efectiva y eficiente dentro de la entidad que permita a los empleados reportar cualquier sospecha o detección de fraude.
- Monitoreo y mantenimiento rutinario de los mecanismos, sistemas, actividades y políticas de prevención de fraude. Este monitoreo y mantenimiento se refiere a examinar periódicamente la efectividad de los controles implementados y, en su caso, corregir las deficiencias que se detecten. Este elemento es especialmente relevante cuando se busca implementar una nueva forma de ofrecer los productos y servicios de la entidad, o bien, cuando se busca ofrecer nuevos productos o servicios, ya que los mecanismos y políticas que se tenían anteriormente pueden no tener la misma eficacia contra los riesgos que presenta esta modificación en la oferta.

7.3 Evaluación de riesgos de fraude.

La evaluación de riesgos es la base de cualquier marco de prevención de fraudes. Diagnosticar de forma específica los riesgos a los que están expuestas las Entidades y su alcance proveen el piso para comenzar a construir el resto del marco de actuación y pueden evitar que las Entidades enfrenten contingencias potencialmente desastrosas. El enfoque de las Entidades debe ser la prevención e identificación del riesgo. En concreto: una vez que las Entidades han comenzado con el proceso de digitalización de sus operaciones, uno de los primeros pasos, incluso antes de la implementación, es llevar a cabo una evaluación de los riesgos de ese proceso. Una vez detectados, la Entidad puede comenzar con la elaboración del marco de control interno, la modificación de los Manuales y demás documentos relevantes y la implementación de las políticas, atendiendo en todo

momento a los riesgos detectados. Para la elaboración de la evaluación de riesgos, sugerimos tomar en cuenta lo siguiente:

- Las metodologías de evaluación de riesgo son únicas y personalizadas[30]. Aunque existen propuestas sobre cómo realizar una metodología, cada Entidad debe considerar sus características propias para llevarla a cabo.
- Determinar las personas que serán responsables de llevar a cabo la evaluación de riesgos (Partes Responsables). Estas personas deben tener las autorizaciones y herramientas necesarias para poder recabar la información necesaria para llevar a cabo la evaluación de manera satisfactoria. Adicionalmente, es importante tomar en cuenta que posiblemente sea necesario designar un equipo de Partes Responsables de distintas áreas de la Entidad que puedan evaluar adecuadamente todos los riesgos potenciales.
- Determinar la manera en la que se recopilará la información. A modo de ejemplo, dependiendo el volumen de operaciones de las Entidades, los responsables de la vigilancia en la materia podrán optar por entrevistar a los empleados clave de la Entidad, tener reuniones con los directivos relevantes, practicar inspecciones oculares o cualesquiera otros métodos que el Consejo de Administración y las Partes Responsables estimen convenientes y efectivos.
- Identificar los riesgos a los que está expuesta la Entidad considerando de manera específica:

    - Actividades y servicios principales de la Entidad.
    - Volumen de operaciones de la Entidad.
    - Áreas más vulnerables a nivel interno.
    - Manejo de los recursos.
    - Controles internos que tiene la Entidad.
    - Tipos de fraude que con más frecuencia se cometen en contra de las Entidades.
    - Incidencia de fraude en la entidad federativa de la Entidad.
    - Cualesquiera otros que las Partes Responsables estimen.

[30] *Ibidem.*

- Determinar los riesgos de fraude que deben atenderse prioritariamente y asignarles una probabilidad de que se presenten[31]. Puede ser necesario consultar este paso con un asesor externo experto en materia de riesgos.
- Cuantificar el monto de las posibles contingencias por fraude.
- Una evaluación adecuada de los riesgos a los que están expuestas las Entidades debe realizarse interna y externamente. Es importante tomar en cuenta que el fraude es un término genérico para una multitud de conductas a las que están expuestas las Entidades, por lo que elaborar una tipificación detallada y específica es indispensable. En ese sentido, las vulnerabilidades de la empresa pueden ser internas, a nivel organización, gobierno corporativo o legales, para lo cual es indispensable realizar una evaluación de riesgos interna o externa, a nivel seguridad de la información, protección de datos personales, penetración de su infraestructura tecnológica o ciberseguridad, para lo cual será necesario contar con un asesor externo.
- Los seres humanos son factores que elevan el nivel de riesgo de cualquier transacción. Con ello no estamos sugiriendo que la automatización de procesos exente a las Entidades de que se cometan fraudes, sino simplemente destacar que utilizar a seres humanos para determinados procesos eleva considerablemente el riesgo de comisión de fraude. A modo de ejemplo, las aprobaciones de crédito realizadas de manera no automatizadas van acompañadas de riesgos como el descuido de un empleado, su estado de ánimo, la cantidad de trabajo que tenga (y el cansancio que eso provoque), entre otras. Contrario a lo anterior, en el caso de un sistema de aprobación de créditos que evalúa el score de crédito de todos los clientes por igual, no se encuentra expuesto a riesgos como los descritos anteriormente.
- La naturaleza de la tecnología y, por ende, de esta Guía Legal, es el constante cambio en los riesgos a los que están expuestas las Entidades. Los riesgos que las Entidades detecten en su evaluación inicial podrían no ser los mismos que aquellos que se susciten al momento de comenzar a operar, por lo cual se deben evaluar los riesgos constantemente[32].

[31] *Ibidem.*
[32] Para mayor información, visitar https://www.ey.com/en_gl/better-begins-with-you/how-an-ai-application-can-help-auditors-detect-fraud

- Utilizar un análisis sofisticado de información[33].

7.4 Control Interno, responsabilidades y actividades de control.

En términos generales, el Consejo de Administración de la Entidad auxiliado por el área contable, de riesgos y legal, será el encargado de aprobar y supervisar la implementación de los mecanismos de prevención de fraudes. Cada persona que trabaje en las Entidades tiene responsabilidades y obligaciones que, en conjunto, conforman políticas y mecanismos de control interno robustos. La separación de labores, la limitación de responsabilidades, la rendición de cuentas y cualesquiera otros valores que se incluyan en las políticas de prevención de fraudes, deben ser los ejes rectores de cualquier puesto dentro de las Entidades, sin importar el nivel jerárquico y la labor en específico que desempeñe el empleado.

Es importante tomar en cuenta lo siguiente al momento de diseñar las políticas de control interno de las Entidades:

- La Entidad debe contar con un organigrama claramente estructurado de su jerarquía. Este organigrama debe identificar claramente las líneas de comunicación con los superiores jerárquicos de cada empleado y, en este caso, el o las personas responsables de la prevención y mitigación de fraudes. Adicionalmente, debe anexarse al organigrama una descripción clara y detallada de las responsabilidades y obligaciones de cada uno de los directivos, administradores, empleados y socios de la Entidad en materia de prevención de fraudes. Este documento pretende evitar confusión sobre el alcance de la responsabilidad que tiene cada área de la empresa y evitar que las líneas de comunicación con los superiores no sean claras.
- En estrecha relación con lo anterior, es indispensable la capacitación de los empleados y el personal de las Entidades en materia de prevención de fraudes, en el conocimiento de sus obligaciones y responsabilidades y las de los demás. La capacitación puede variar dependiendo del puesto del empleado; sin embargo, es recomendable dar una capacitación con bases sólidas, que dé a conocer a los

[33] Para mayor información visitar: https://www.mckinsey.com/industries/financial-services/our-insights/fraud-management-recovering-value-through-next-generation-solutions#

empleados los potenciales riesgos a los que está expuesta la Entidad y cómo prevenirlos y mitigarlos.

- Actualización anual o cada vez que sea necesario respecto a nuevos riesgos a los que la Entidad esté expuesta por sus nuevas líneas del negocio o por las condiciones externas.
- Se deben diseñar controles y políticas que funcionen de forma efectiva independientemente de quién ocupe la posición[34]. Esto es, las políticas deben tener el mismo grado de efectividad sin importar si la rotación del personal en la Entidad es alta o baja. Los controles implementados deben atender a las funciones y responsabilidades de la posición, no de la persona.
- Los controles y las actividades de control deben contar con niveles de seguridad físicos y lógicos.
- Toda la información y documentación de las Entidades debe estar respaldada y resguardada en alguna tecnología que no permita su modificación (Ver **Sección 26** Activos Virtuales y Blockchain). A reserva de que la CNBV solicite que las Entidades cumplan con conservar la información y documentación de sus operaciones, es clave comenzar a migrar toda esa información a sistemas que sean fácilmente accesibles y los cuáles no puedan ser modificados o extraviados por el personal de las Entidades.
- Las Entidades deben contar con políticas de contratación con el objetivo de detectar de manera temprana a personas que son una contingencia potencial o, en su caso, evitar contratarlas.
- Las Entidades deben contar con cursos y capacitaciones especiales para todos los miembros de la estructura jerárquica para que conozcan las políticas de control interno y prevención de fraude de la Entidad
- Se debe evaluar el desempeño de los administradores, directivos y empleados periódicamente. A modo de sugerencia, podría evaluarse el desempeño de su puesto de manera independiente de sus responsabilidades y obligaciones en materia de prevención de fraudes (a menos que ambas estén muy relacionadas, como el caso del área contable).

[34] *Ibidem.*

- Contar con sistemas automatizados de evaluación y prevención de fraudes que eliminen, en la medida de lo posible, el error humano para procurar un sistema sólido que minimice márgenes de error en las evaluaciones de riesgo.
- Contratar personal especializado en ciberseguridad como un Oficial en Jefe de la Seguridad de la Información.
- Invertir en ciberseguridad. Cualquier proyecto de digitalización de una Entidad debe ir acompañado de proveedores de ciberseguridad que desarrollen e implementen mecanismos para proteger a las Entidades tanto interna como externamente. Esta inversión debe cubrir:
    - La información y documentación interna de la Entidad.
    - Los datos personales de los empleados, socios y clientes.
    - La protección de la página web o aplicación contra intentos de hackeo, virus y otros riesgos informáticos.
    - Las cuentas que las Entidades mantengan de forma electrónica.
- Establecer filtros de seguridad en los correos electrónicos de los empleados, sus teléfonos de oficina y demás sistemas. Es muy común que los fraudes traten de cometerse a través de un correo electrónico que pareciera inocente para infiltrar un virus informático a los sistemas de la empresa.

7.5 Detección e investigación.

La detección de los fraudes, por su parte, exige, por un lado, prever indicadores que las Personas Responsables puedan fácilmente identificar como fraudes potenciales y, por otro, contar con mecanismos y sistemas que permitan la detección de fraudes aun cuando no haya alguien supervisando los procesos de la Entidad. Al respecto, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional[35] propone, entre otros, los siguientes indicadores que pueden auxiliar a las Entidades en la detección de posibles fraudes. Estos indicadores han sido ajustados para adecuarse a las actividades propias de las Entidades:

[35]UNCITRAL. Detección y prevención del fraude comercial: indicadores de fraude comercial. (Internet) Consultado en: https://www.uncitral.org/pdf/spanish/texts/fraud/Recognizing-and-preventing-commercial-fraud-s.pdf

- Irregularidades en los documentos que las Entidades requieren para el *onboarding* y contratación.
- Secretismo indebido. Este indicador se extiende desde la comunicación entre los empleados de la Entidad hasta los potenciales proveedores.
- Operaciones excesivamente complejas o simples.
- Poca cooperación o negativa de llenar los formatos de identificación de los clientes (*KYC*, *due diligence*) en materia PLD/FT o cualesquiera otros que las Entidades requieran para ofrecer sus productos y servicios.
- Conflictos de interés que involucren afinidades o relaciones personales de los administradores, directivos, empleados o socios de las Entidades.
- Uso indebido interno de la tecnología de las Entidades.
- Detección de tráfico inusual en los servidores de las Entidades o de vulneraciones en las medidas de ciberseguridad implementadas.
- Utilizar el sistema de detección de fraudes que ofrecen algunos proveedores. Este sistema detecta inmediatamente movimientos inusuales dentro de las Entidades para que se puedan atender. A modo de ejemplo, este sistema detecta discrepancias en la información financiera y los recibos o CFDI, operaciones en las que se omita llevar a cabo el proceso interno, entre otras. Adicionalmente, en caso de que se busque detectar movimientos inusuales, es posible utilizar los parámetros que configuran un "movimiento inusual" de acuerdo con lo que establecen las disposiciones en materia PLD/FT.

Con el objetivo de mitigar cualesquiera fraudes o potenciales fraudes detectados, las Entidades deben contar también con un proceso que les permita investigar los incidentes de manera efectiva. Este proceso de investigación permite detectar las áreas y sistemas vulnerados para, posteriormente, tratar de mitigar la contingencia. Aunque ese procedimiento igualmente es hecho a la medida para cada Entidad, proponemos las siguientes directrices[36]:

[36] PriceWaterhouseCoopers Australia. *Fraud: A guide to its prevention, detection and investigation.* (Internet) Consultado en: https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf

- Recopilar evidencia del fraude: fotografías, capturas de pantalla, evidencia digital, evidencia informática, los estados financieros o cualquier otro documento o información que pueda ser relevante para la investigación. Cualquier detalle relacionado con el fraude debe estimarse altamente importante.
- Notificar inmediatamente a la CNBV sobre el fraude detectado y la estrategia de investigación y mitigación.
- Publicar notificaciones en la página web o aplicación de la Entidad para evitar que un mayor número de socios o clientes sean víctimas del fraude, en caso de que sea externo.
- Presentar una denuncia ante las autoridades competentes para que se comience una investigación.
- Consultar con un asesor externo las implicaciones y el alcance legal, contable y financiero que el fraude puede tener.
- Llevar a cabo entrevistas, cuestionarios o conversaciones con personas que pudieran estar involucradas (cuando el fraude sea interno).
- Llevar a cabo una investigación a partir de componentes físicos (documentos, empleados, entre otros) y electrónicos (servidores, proveedores, sistemas, entre otros). Los resultados de esa investigación deben entregarse al personal relevante y, en su caso, a los socios de las Entidades para dar a conocer el motivo, la forma en que se cometió el fraude y las acciones que se están tomando para mitigarlo.

Las estrategias de mitigación son responsabilidad directa de las autoridades de las Entidades. Estas estrategias pueden estar diseñadas y desarrolladas al momento en que se elaboran las políticas y mecanismos de prevención de fraude e implementarse cuando efectivamente ocurre el fraude. Al respecto, recomendamos considerar lo siguiente para poder hacer frente a una contingencia por fraude:

- Contar con herramientas que permitan minimizar las pérdidas por fraude, sin afectar la continuidad de las operaciones de las Entidades.
- Delegar la implementación de la estrategia de mitigación a miembros del Consejo de Administración o directivos de la Entidad que cuenten con facultades para administrar recursos humanos, informáticos y financieros.

- En general, aquellas estrategias de mitigación que se detecten conforme a los indicadores de riesgo que haya detectado cada Entidad.

7.6 Evaluación de proveedores.

La evaluación de proveedores de control interno o de software de prevención de fraude se lleva a cabo de forma similar a los proveedores tradicionales (Ver Sección 7 Prevención de Fraudes y Sección 15.- Contratación de Proveedores y Comisionistas.):

- En primer lugar, debe realizarse una evaluación de riesgos del proyecto de digitalización. Este diagnóstico permite detectar las áreas vulnerables de cada Entidad y seleccionar un proveedor que las cubra de forma específica.
- Deben evaluarse las necesidades de cada Entidad desde el punto de vista operativo. Una Entidad con baja transaccionalidad y que ofrece productos y servicios limitados, probablemente no requiera contratar un proveedor que elabore controles hechos a la medida; potencialmente, incluso, los controles pueden desarrollarse internamente sin incurrir en costos excesivamente altos. Por el contrario, si las Entidades cuentan con un volumen transaccional alto o tienen una oferta más amplia de servicios, es probable que tiendan a requerir proveedores externos para evitar los altos costos que conlleva el desarrollo interno de dichos controles.
- Posteriormente, deben evaluarse las modificaciones a nivel gobierno corporativo y organización interna que la Entidad debe realizar para efecto de robustecer su control interno
- Una vez realizado lo anterior, las Entidades estarán en posibilidades de analizar si será necesario contar con la autorización por parte de la CNBV para celebrar el contrato correspondiente con el proveedor.
- Detectar los proveedores que pueden ofrecer las soluciones (generales o personales) que las Entidades requieren para atender sus necesidades de prevención de fraude
- Realizar el due diligence correspondiente para verificar el cumplimiento de las obligaciones del proveedor (Ver Sección 15 Contratación de Proveedores y Comisionistas)

- Verificar que los proveedores cuenten con la capacidad humana, técnica y especializada que la Entidad requiere en concreto. Estos proveedores, asimismo, deberán estar en posibilidades de dar cumplimiento a las obligaciones de confidencialidad, regulatorias (Ver Sección 15 Contratación de Proveedores y Comisionistas) y de resistir una auditoría por parte de la CNBV sobre el servicio prestado, en caso de ser necesario.
- Someter los candidatos al Consejo de Administración de las Entidades para que evalúen la viabilidad financiera, operativa y técnica de contratar con cada uno de ello.
- Una vez que se haya elegido al proveedor, debe someterse el contrato a la CNBV para su visto bueno.

7.7 Implementación y Diagrama.

El programa de implementación de políticas y sistemas automatizados en materia de prevención de fraude estaría constituido por los siguientes pasos:

1. El Director General debe solicitar a las áreas de negocio, Auditoría Interna, Oficial de Cumplimiento y aquellas cuya responsabilidad consiste en supervisar el control interno de la Entidad reportes de incidencias de fraude. Uno de los más comunes es la suplantación de identidad. El informe deberá contener información como (i) volumen de incidencia de fraudes, (ii) tipicidad de los fraudes (es decir, si se trata de un flujo importante de identificaciones falsas, firmas hechizas, entre otros), (iii) costos y pérdidas relacionadas con los fraudes (por ejemplo, monto de las contingencias legales que deberá sufrir la Entidad), y (iv) observaciones que, en su caso, haya hecho CNBV a estos temas, de ser aplicables.

2. Es importante que cada tipicidad de fraude sea descrita de manera detallada. Es decir, el proceso de fraude requiere de una serie de pasos que concluyen, en su caso, con la aprobación de una operación por parte de funcionarios de la Entidad. El objetivo es descubrir patrones comunes de conducta y elementos similares en el tipo de fraude. Asimismo, el área de sistemas, en su caso, debe identificar aquellos “puntos ciegos” de los sistemas de la Entidad que pudieron haber propiciado o causado este tipo de fraude.

3. El Oficial de Cumplimiento deberá realizar un diagnóstico efectivo de la manera en que están llevando a cabo los procesos de identificación, los cuales son esenciales para la prevención de fraude. Esto en atención a que la identificación de los clientes se encuentra relacionada también con los procesos de prevención de lavado de dinero. El Oficial de Cumplimiento debe identificar los problemas que ha tenido para efecto de realizar validación de documentos y establecer cuáles son las capacidades humanas y tecnológicas que deben ser adquiridas para un plan antifraude eficaz.

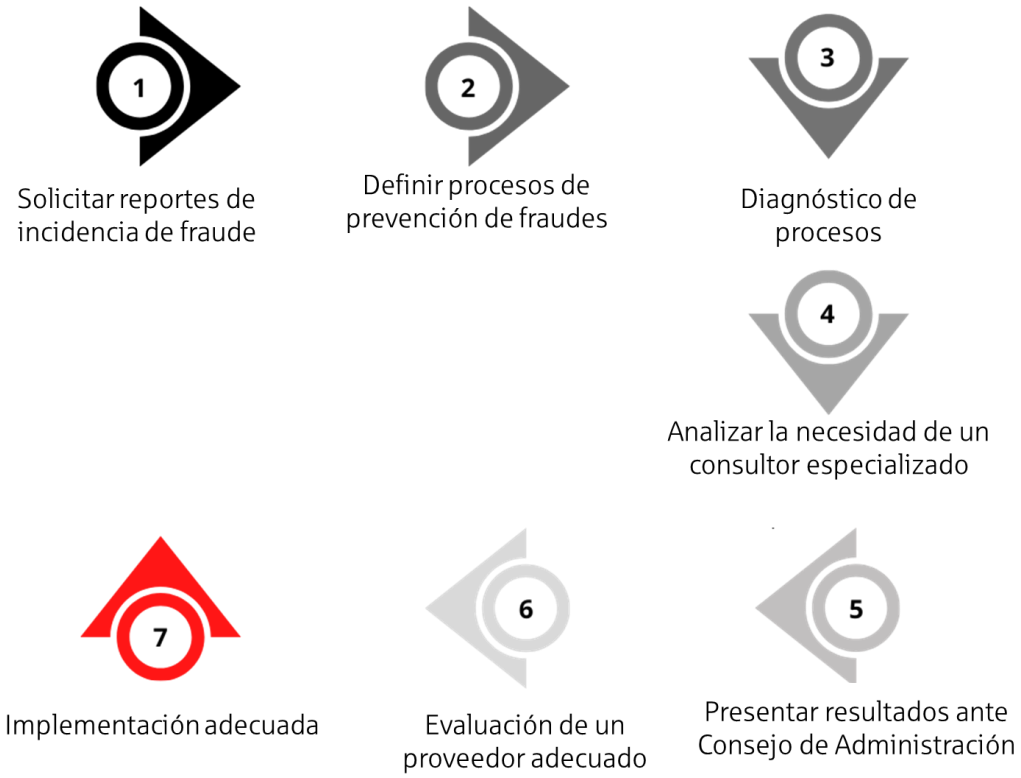
4. El Director General debe dirigir todos los esfuerzos adicionales. En algunos casos, puede optar por contratar a algún consultor especializado (por ejemplo, en materia forense) para determinar el origen y consecuencia de los fraudes cometidos en perjuicio de la Entidad. Esto es recomendable una vez que se hayan obtenido los reportes de las áreas internas para efecto de evaluar la veracidad de sus declaraciones y poder detectar posibles responsabilidades a nivel interno.

5. Los resultados de este informe deben ser presentados al Consejo de Administración, de modo que el proyecto siempre esté bajo su supervisión. Como hemos mencionado en secciones anteriores, el involucramiento de las áreas superiores de dirección de la Entidad es esencial.

6. El Director General deberá realizar la evaluación de un proveedor adecuado para implementar un sistema automatizado en materia antifraudes. No es recomendable que la Entidad invente o construya desde cero una solución: en nuestra experiencia, ya existen soluciones robustas adaptadas al sistema financiero que pueden ser muy eficaces para evitar el fraude, sobre todo, en Entidades que ya tengan cierto grado de digitalización en sus procesos. Esta evaluación debe hacerse conforme a lo mencionados en las Secciones 15 y Sección 16 para determinar si estamos ante un supuesto de Proveedor Relevante.

7. El cierre debe consistir en la implementación adecuada del sistema adquirido del Proveedor Relevante, la emisión y cambios de políticas y Manuales, así como la aprobación del Consejo de Administración.

Implementación de políticas y sistemas en materia de prevención de fraudes



Gráfica 7. Implementación de políticas y sistemas en materia de prevención de fraudes. Fuente: Vite Abogados

7.8 Aspectos prácticos.

Entre enero y septiembre del 2020, la Condusef detectó alrededor de 6.5 millones de fraudes totales, de los cuáles el 69% fueron fraudes cibernéticos y el 31% restante se debe a fraudes tradicionales[37]. Detectaron más de cuatro millones de reclamaciones en materia de comercio por internet presentadas ante las propias instituciones bancarias. Estas cifras revelan la importancia de tomar en cuenta los riesgos asociados con la digitalización de las operaciones de las entidades financieras.

El riesgo de fraude es cada vez más alto y más costoso para las empresas. Por ejemplo, en 2016, a través unos hackers, mediante estrategias fraudulentas, retiraron alrededor de mil

[37] Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros. (2020). México: *Cifras relevantes de Banco de México en Comercio Electrónico.* (Internet) Consultado en: https://www.condusef.gob.mx/?p=estadisticas

millones de dólares de la cuenta del Banco Central de Bangladesh en la Reserva Federal de Estados Unidos de América[38]. Ninguna entidad, sin importar su tamaño y su infraestructura, está exenta de enfrentar un intento de fraude. La mejor estrategia que pueden seguir las Entidades es: detectar oportunamente los factores de riesgos y, en la medida de lo posible, cubrirlos y posteriormente tener un sistema de detección temprana que permita hacer frente a la contingencia sin que ello represente pérdidas excesivas para las Entidades.

Con un marco de prevención de fraude sólido los beneficios de los procesos de digitalización de las Entidades tienen el potencial de superar las posibles contingencias y dar viabilidad a los Proyectos.

[38] *Idem.*

SECCIÓN 8.- SEGURIDAD DE LA INFORMACIÓN Y CONFIDENCIALIDAD Y CONTINUIDAD DE LA OPERACIÓN.

8.1 Seguridad y Confidencialidad de la Información.

8.1.1 Medidas de Seguridad en Medios Electrónicos

Las Entidades, en caso de utilizar Medios Electrónicos para la celebración de operaciones y prestar servicios, deben implementar medidas de seguridad en la transmisión, almacenamiento y procesamiento de la información para evitar su divulgación a terceros no autorizados. Para alcanzar este objetivo, las Entidades deben cumplir, entre otras, con las siguientes directrices conforme a su regulación aplicable:

- Cifrar los mensajes que transmitan Información Sensible a través de Medios Electrónicos, desde el Dispositivo de Acceso hasta la recepción para su ejecución. Para ello, la Entidad debe utilizar tecnologías que protejan la confidencialidad de la información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación para evitar que terceros no autorizados accedan a los datos. La responsabilidad por la administración de dichas llaves será de la Entidad.

- La información de cuentas, operaciones, contraseñas, números de identificación personal (NIP) o cualquier otro Factor de Autenticación, debe estar cifrada cuando se almacene en cualquier componente de los Medios Electrónicos.

- La transmisión de contraseñas y números de identificación personal sólo puede realizarse a través de correo electrónico, servicios de mensajería instantánea, mensajes de texto SMS si se cuenta con mecanismos de Cifrado, salvo algunas excepciones de Pago Móvil (siempre que CNBV lo autorice) y para estados de cuenta (si se implementan ciertos mecanismos de seguridad).

- La Entidad debe asegurarse que las llaves criptográficas y el proceso de Cifrado se encuentren instalados en equipos de alta seguridad que eviten accesos y divulgaciones no autorizadas.

En el caso de servicios de Pago Móvil, dadas sus características, es posible que la Entidad establezca medidas compensatorias en lugar de lo mencionado anteriormente; por ejemplo, en el Cifrado de la información o, incluso, se les exceptúa de la regla mencionada en el numeral 3, siempre que mantenga controles que permitan mantener a resguardo la información de los Usuarios y que obtenga la autorización previa de CNBV.

8.1.2 Controles de Acceso

Las bases de datos y los archivos de las Entidades relacionados con las operaciones y servicios efectuados a través de Medios Electrónicos deben resguardarse mediante controles de acceso y ajustarse a lo siguiente:

- El acceso a las bases de datos estará permitido sólo a personas autorizadas por la Entidad con base en sus funciones dentro de ésta. Los accesos deben ser registrados y fundamentados.
- Los accesos remotos deben ser cifrados.
- Contar con procedimientos seguros de destrucción de medios de almacenamiento de bases de datos y archivos con Información Sensible que provengan de su restauración a través de cualquier medio o dispositivo.
- Desarrollar políticas sobre el uso y almacenamiento de información que se transmita y reciba a través de Medios Electrónicos que incluyan la verificación de su cumplimiento por parte de sus proveedores y afiliados.

8.1.3 Información Sensible

En caso de que la Información Sensible de los Usuarios sea extraída, extraviada o se sospeche de algún incidente de acceso no autorizado a esa información, las Entidades deben:

- Enviar un reporte con información específica establecida en las disposiciones a CNBV y al Comité de Supervisión Auxiliar dentro de los cinco días naturales siguientes al evento.
- Investigar si la información puede ser objeto de uso indebido. Si es el caso, deberán notificar a los Usuarios dicha situación dentro de los siguientes tres días hábiles e

indicar las medidas que deben tomar al respecto. Asimismo, los resultados de esa investigación deben enviarse a la CNBV y al Comité de Supervisión Auxiliar en un plazo no mayor a cinco días naturales posteriores a su conclusión.

- Cifrar los mensajes o utilizar medios de comunicación cifrada en la transmisión de información sensible del Usuario procesada a través de Medios Electrónicos.
- Cifrar o truncar información de cuentas u operaciones, contraseñas, NIP, respuestas secretas o Factores de Autenticación si se almacena en un componente de Medios Electrónicos.

8.1.4 Controles de Acceso a Bases de Datos

Las Entidades deben contar con controles de acceso a las bases de datos y archivos correspondientes a las Operaciones realizadas a través de Medios Electrónico, y ajustarse a reglas similares a las expuestas en la sección anterior.

8.2 Continuidad de la Operación.

La continuidad de los servicios prestados por las Entidades es un tema que preocupa a los Reguladores, quienes han establecido las siguientes obligaciones para el SACP en las Disposiciones Generales SOCAP y en las Disposiciones Generales SOFIPO:

- Las Entidades deberán procurar la operación continua de la infraestructura de cómputo y de telecomunicaciones, así como dar pronta solución para restaurar los Servicios Electrónicos, en caso de presentarse algún incidente.
- En el contexto de la contratación de servicios de terceros relevantes (ver Sección 15 Contratación de Proveedores y Comisionistas), establecer y cumplir políticas y procedimientos para vigilar el desempeño del tercero o comisionista y el cumplimiento de sus obligaciones contractuales que tengan por objeto, entre otros, planes de continuidad del negocio, incluyendo los procedimientos de contingencia en caso de desastres. Asimismo, las Entidades deben asegurarse de que la contratación de terceros relevantes no ponga en riesgo la continuidad del negocio (se requiere que el Consejo de Administración incluso emita una resolución al respecto).

- La CNBV cuenta con la facultad de suspender parcial o total, temporal o definitiva, la prestación de los servicios o comisiones a través del tercero relevante cuando pueda verse afectada la continuidad operativa de la Entidad.
- El Sistema de Control Interno debe contemplar planes de contingencia a fin de asegurar la capacidad y continuidad de los sistemas. Dichos planes deben comprender las medidas necesarias que permitan minimizar y reparar los efectos generados por eventualidades que, según sea el caso, llegaren a afectar el continuo y permanente funcionamiento de los servicios.

» *COVID-19: Seguridad y Continuidad del negocio.*

La continuidad del negocio, así como la seguridad informática, se han vuelto un reto. En particular porque al momento de escribir estas líneas la pandemia ocasionada por el COVID-19 continúa teniendo un impacto considerable en esos temas, sobre todo en el primero.

El Fondo Monetario Internacional, en una edición especial de reportes sobre el COVID-19, ha preparado una serie de estudios sobre temas prácticos asociados a la pandemia ocasionada por ese virus. En el documento "*Pandemic Preparedness for Financial Institutions*[39]" el autor del documento señala los retos que la materia de continuidad ha enfrentado el sector financiero, entre los cuales se encuentran:

- La duración indeterminada de este fenómeno a diferencia de un desastre natural o actos terroristas.
- La escala global del problema y la facilidad con que se ha extendido por todo el planeta.
- Retos para continuar operando debido a incapacidad del personal o restricciones oficiales.
- Retos para llevar a cabo nuevas evaluaciones de riesgos y necesidad de revisión de los procesos administrativos para cubrir la posibilidad de impactos adversos en (i)

[39] IMF. Pandemic Preparedness for Financial Institutions. (Internet) Consultado en: https://www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-pandemic-preparedness-for-financial-institutions.ashx.

el desempeño de portafolios de crédito y otros activos, (ii) la valuación de los activos y (iii) liquidez.

- Presión sobre la Infraestructura Tecnológica de las entidades financieras para permitir al personal el trabajo desde casa.

El documento considera que las instituciones financieras deben adoptar un enfoque de "planeación" para asegurar que la continuidad de sus procesos operativos críticos y los servicios al público continúen activos. Recomiendan que esta preparación debe incluir los siguientes aspectos:

- Planeación estratégica: asignación adecuada de recursos para la supervisión, planeación, respuesta y recuperación de la pandemia en consonancia con las políticas públicas y que incluya medidas como:

  - La aprobación de Consejo de Administración de un plan para afrontar la pandemia. Esto para asegurar que se tomarán las medidas necesarias hacia el interior de la Entidad y que el presupuesto necesario estará disponible.
  - El Director General y los demás directivos relevantes deberán ser responsables de desarrollar, comunicar y evaluar el plan y, en su caso, reflejarlo en las políticas y Manuales de las Entidades.
  - Un equipo especial debe ser asignado al cumplimiento de los objetivos del plan bajo la supervisión de los directivos relevantes para atender diversos temas como: continuidad, aspectos legales, seguridad de la información, recursos humanos, comunicación interna, salud y seguridad.
  - Claridad sobre lo que puede ocurrir en caso de que se ausenten los titulares de áreas críticas del negocio.

- Revisar o crear planes de continuidad y actualizar los Manuales relevantes a la nueva realidad (identificar actividades y personal críticos, señalar sedes alternativas de trabajo, crear infraestructura informática para laborar desde casa, revisiones de la Infraestructura Tecnológica para asegurar que no será necesaria la presencia física, revisar que los proveedores principales cuentan con programas de continuidad, evaluar la necesidad de los Usuarios de contar con infraestructura electrónica para efecto de seguir operando normalmente, entre otros).

- Manejo adecuado de instalaciones: considerar que puede haber interrupciones en servicios o mantenimiento, establecer medidas sanitarias adecuadas para los equipos que normalmente están expuestos a aerosoles del virus (teléfonos, computadoras, escritorios), procedimientos para mantener distancia sana frente a visitantes o clientes, sanitización de monedas o billetes, como ejemplos elementales.
- Planeación en materia de salud y seguridad: Mantener al personal debidamente informado de los anuncios públicos en materia de salubridad, claridad en los supuestos en que será necesario el trabajo a distancia, monitoreo del personal enfermo y ayuda al mismo, compra de material desinfectante, distribución de cubrebocas y contratación de algún servicio médico auxiliar dentro de las oficinas y reducción (en lo posible) de viajes del equipo de la Entidad.
- Comunicación corporativa efectiva: contar con información suficiente del equipo para poder transmitir mensajes a ellos o a sus familiares (en caso de emergencia) y hacerles saber de las medidas adoptadas para enfrentar la pandemia.
- Retorno a la normalidad una vez que las autoridades competentes así lo permitan o lo indiquen y adaptación para el regreso pausado a las actividades normales dentro de las oficinas.

La lección de la pandemia puede ser importante para la Entidad: al final se habrán identificado los procesos que requieren de mayor o menor tecnología para realizarse a distancia y de aquellos que, de ser automatizados, reducen la exposición del personal a situaciones como esta.

SECCIÓN 9.- DATOS PERSONALES Y SECRETO FINANCIERO.

El principio general en el derecho financiero mexicano es que las entidades financieras, incluyendo aquellas que conforman el SACP, están obligadas a guardar confidencialidad sobre la información de sus Usuarios. Por otra parte, el régimen de protección de datos personales ofrece una garantía mínima del tratamiento que cualquier persona (entidad financiera o no) debe dar a la información que las personas físicas les entregan. Ambos constituyen la normativa central que debe tenerse en cuenta en muchos Proyectos de innovación. En la actualidad, los datos personales constituyen uno de los recursos más valiosos de las entidades, pero su manejo descuidado o ilegal puede acarrear consecuencias graves para las organizaciones y para los individuos. Los datos de Usuarios permiten conocer fortalezas y debilidades, generar oportunidades de negocio, mejorar sistemas internos, evaluar el desempeño de la Entidad a futuro y, en general, aportar al crecimiento de un negocio. A continuación, presentamos una introducción genérica a esos temas, así como algunos apuntes prácticos que deben tomarse en consideración para cualquier Proyecto que involucre datos personales.

El conocimiento y aplicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP") es importante debido no sólo a la relevancia que tienen los Datos Personales y Datos Financieros en los Proyectos, sino por los riesgos legales a los que pueden estar expuestas las entidades: multas de hasta treinta millones de pesos (aproximadamente) y, en algunos casos, penas corporales por la realización de conductas indebidas[40].

9.1 Conceptos Generales.

La LFPDPPP tiene como objeto la protección de los datos personales de las personas físicas ("Titulares"), así como su derecho a decidir libremente la manera en que las personas morales u otras personas físicas particulares llevan a cabo el tratamiento de sus datos personales, entendiendo lo anterior como "cualquier información concerniente a una persona física identificada o identificable". En ese sentido, todas las personas morales o físicas que deciden sobre el procesamiento de Datos Personales (consideradas por le ley

[40] "Al que, estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia se le aplicará pena de tres meses a tres años de prisión. Tratándose de datos sensibles la sanción será doble".

como “Responsables”), están sujetas a la LFPDPPP y al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (“RDP”).

De acuerdo con la LFPDPPP, el tratamiento de los datos personales se encuentra sujeto a una expectativa razonable de privacidad, que es un principio general de confianza según el cual una persona que entrega información personal a un Responsable asume que dichos datos serán tratados de acuerdo con la ley y los términos acordados entre ellos.

9.2 Aviso de Privacidad.

Es un documento físico, electrónico o en cualquier otro formato generado por el Responsable para ser puesto a disposición del Titular previo al tratamiento de sus Datos Personales. En todo momento el tratamiento de los Datos Personales debe limitarse al cumplimiento de las finalidades previstas en el documento mencionado. En caso de que se requiera o necesite tratar los Datos Personales para fines no expresados en el Aviso de Privacidad, entonces deberá recabarse el consentimiento del Titular.

Cuando el Aviso de Privacidad es puesto a disposición de los Titulares por medios electrónicos, entonces deben darse a conocer “de manera inmediata”, al menos (i) la identidad y el domicilio del Responsable y (ii) las finalidades del tratamiento de datos; lo anterior sin perjuicio de que se pongan a su disposición los mecanismos para conocer el texto completo del mismo. (Ver formato de Aviso de Privacidad en el Anexo I de este documento).

9.3 Medidas de Protección de Datos Personales.

Los Responsables deben establecer y mantener medidas de seguridad de carácter administrativo, técnico y físico que permitan proteger los Datos Personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Asimismo, el Responsable debe tomar en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los Titulares, serán informadas

de forma inmediata por el Responsable al Titular, a fin de que este último pueda tomar las medidas correspondientes para la defensa de sus derechos.

9.4 Consentimiento y Renunciabilidad.

Como regla general, el tratamiento de datos personales se encuentra sujeto al consentimiento de los Titulares. La LPDP, en su artículo 8, establece dos tipos de consentimiento (i) *expreso,* cuando la intención del Titular se otorga de forma verbal, por escrito o por medios ópticos o electrónicos o mediante cualquier otra tecnología o a través de signos inequívocos y (ii) *tácito,* cuando el Titular acuerda de forma tácita el tratamiento de los datos cuando le fue presentado el aviso de privacidad al Titular y no hubo objeción al respecto.

El consentimiento debe (i) otorgarse libremente y sin error, dolo o violencia que pudieran afectar la voluntad del Titular; (ii) ser específico, es decir, referido a uno o más propósitos específicos del tratamiento de los datos; y (iii) ser informado, es decir, que el Titular debe conocer el aviso de privacidad del tratamiento de los datos y el consentimiento debe otorgarse antes de que ocurran las consecuencias previstas en dicho aviso. En todo caso, el consentimiento expreso debe ser inequívoco, es decir, debe haber elementos suficientes que permitan acreditar o verificar dicho otorgamiento. Puede ser otorgado de manera verbal o por escrito, en este último caso, puede ser suficiente una firma electrónica o cualquier mecanismo o procedimiento que permita la identificación del Titular.

Asimismo, el Responsable está obligado a poner a disposición del Titular los medios necesarios para revocar su consentimiento en todo momento respecto a las finalidades de tratamiento de información expresadas en el Aviso de Privacidad. Respecto a lo anterior, el consentimiento siempre puede ser revocado por el Titular. El Responsable, por su parte, debe establecer mecanismos sencillos y gratuitos para efecto de que, a través de los mismos mecanismos (por ejemplo, digitales) mediante los cuales otorgó dicho consentimiento el Titular, notifique la revocación al Responsable.

9.5 Encargados.

Conforme a la LFPDPPP un “Encargado” es aquella persona física o moral que sola o conjuntamente con otra persona trata Datos Personales por cuenta del Responsable. Al

respecto, la LFPDPPP establece que no obstante la existencia del Encargado, la responsabilidad por el cumplimiento de los principios de dicha ley recae en el Responsable.

El Encargado tiene las siguientes obligaciones respecto del tratamiento que realice por cuenta del Responsable[41]:

- Tratar únicamente los datos personales conforme a las instrucciones del Responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el Responsable;
- Implementar las medidas de seguridad aplicables;
- Guardar confidencialidad respecto de los Datos Personales tratados;
- Suprimir los Datos Personales objeto de tratamiento una vez cumplida la relación jurídica con el Responsable o por instrucciones del Responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
- Abstenerse de transferir los Datos Personales salvo en el caso de que el Responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

En todo caso, los Acuerdos entre el Responsable y el Encargado relacionados con el tratamiento, deberán establecerse con estricta concordancia con el Aviso de Privacidad respectivo.

Las remisiones de Datos Personales entre un Responsable y un Encargado no requerirán ser informadas al Titular ni contar con su consentimiento.

El Encargado será considerado responsable con las obligaciones propias de éste cuando[42]:

[41] Artículo 50 del RDP.

[42] Artículo 53 del RDP.

- Destine o utilice los datos personales con una finalidad distinta a la autorizada por el Responsable, o
- Efectúe una transferencia, incumpliendo las instrucciones del Responsable.

El Encargado no incurre en responsabilidad cuando, bajo previa indicación expresa del Responsable, remite los Datos Personales a otro encargado designado por este último al que hubiera encomendado la prestación de un servicio, o transfiera los Datos Personales a otro Responsable legalmente.

9.6 Transmisión de Datos Personales.

La transmisión o cesión de Datos Personales a terceros debe incluir la notificación al cesionario del aviso de privacidad originalmente otorgado a los Titulares por parte del Responsable, especificando las finalidades originales para el tratamiento de los Datos Personales. En este supuesto, el tratamiento de los Datos Personales debe realizarse de acuerdo con los términos presentados en el Aviso de Privacidad original, el cual debe contener una cláusula que indique que el Titular (el cual es por definición el dueño de los Datos Personales) consiente expresamente la transferencia de dichos datos. Asimismo, el tercero receptor de los Datos Personales deberá asumir las mismas responsabilidades que le corresponden al Responsable original con respecto a dicha información.

Este tipo de transferencias de Datos se encuentran sujetas a las siguientes reglas: el cesionario de los datos debe seguir las medidas pertinentes que el "principio de calidad de los datos" se cumpla, mismo que incluye (a) el establecimiento por parte del receptor o cesionario de las medidas necesarias para garantizar que los datos sean precisos, completos, relevantes y actualizados para asegurar la veracidad y evitar un efecto negativo en el Titular; (b) cláusulas específicas para que el cesionario asuma las obligaciones de Responsable del tratamiento para todos los efectos legales y cumpla con las obligaciones establecidas en la LPDP y el Aviso de Privacidad que el transmisor originalmente otorgó al Titular, y (c) debe existir prueba de que el transmisor de los Datos Personales notificará al cesionario respecto de los términos y condiciones conforme a los cuales deben tratarse los datos.

La cesión de los Datos Financieros (así como los datos relacionados con el patrimonio de una persona física) requiere el consentimiento expreso del Titular, salvo por los supuestos o excepciones contempladas en la LPDP[43].

Las personas que realicen la cesión de los Datos Personales tienen la carga de probar que el consentimiento expreso, cuando sea requerido, fue otorgado de manera adecuada por el Titular.

9.7 Tratamiento de Datos Personales en la nube.

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de "cómputo en la nube[44]", en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación (por ejemplo, Amazon o similares), el Responsable sólo podrá utilizar aquellos servicios en los que el proveedor:

- Cumpla, al menos, con lo siguiente: (a) tener y aplicar políticas de protección de datos personales similares a la LFPDPPP y al RDP; (b) transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; (c) abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y (d) guardar confidencialidad respecto de los Datos Personales sobre los que se preste el servicio.
- Cuente, por lo menos, con mecanismos para: (a) dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; (b) permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; (c) establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; (d) garantizar la supresión de los datos personales una vez que haya concluido el

[43] Los más relevantes son: (i) permitido por una ley o un tratado; (ii) los datos son públicos; (iii) tienen el propósito de cumplir con una obligación relacionada con una relación jurídica entre el Titular y la empresa o un tercero; (iv) existe una emergencia que puede potencialmente dañar a un individuo o sus activos; (v) es necesario proporcionar un tratamiento médico, hasta el punto en que el Titular no pueda dar su consentimiento para el tratamiento; (vi) ciertas transferencias entre partes relacionadas; (vii) cuando es necesario ejecutar un acuerdo en beneficio del Titular; (viii) cuando el interés público o la aplicación de la ley así lo requiera; (ix) cuando sea necesario hacer valer un derecho en un procedimiento judicial.

[44] Conforme al RDP por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

servicio prestado al responsable, y que este último haya podido recuperarlos, e (e) impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

Lo anterior sin perjuicio de aplicar lo que respecto de prestadores de servicios relevantes sea aplicable para los supuestos anteriores conforme a la regulación financiera (ver Sección 15 Contratación de Proveedores y Comisionistas).

9.8 Secreto Financiero.

La información y documentación relativa a las operaciones y servicios que las Entidades están autorizadas a prestar es confidencial, por lo que las Entidades en protección del derecho a la privacidad de sus Socios o Usuarios, según sea el caso, de ninguna manera podrán dar noticias o información de los depósitos, operaciones o servicios, sino al depositante, deudor, titular, beneficiario, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.

No obstante, como excepción a lo dispuesto por el párrafo anterior, las Entidades están obligadas a dar las noticias o información mencionadas cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el Usuario titular o, en su caso, el depositante, deudor, titular o beneficiario sea parte o acusado. Asimismo, las Entidades también están exceptuadas de la obligación de guardar el secreto financiero y, por tanto, obligadas a dar las noticias o información mencionadas en los casos en que sean solicitadas por las autoridades siguientes:

- El Fiscal General de la República o el servidor público con facultades delegadas, así como el Procurador General de Justicia Militar para ello en procesos o investigaciones penales que así lo requieran.
- Fiscales o procuradores generales de justicia de los estados y de la Ciudad de México o subprocuradores, para los mismos efectos del punto anterior.
- Las autoridades hacendarias federales, para fines fiscales.
- La SHCP en relación con el cumplimiento de la regulación en materia de PLD/FT.

- El Tesorero de la Federación, cuando el acto de vigilancia lo amerite.
- La Auditoría Superior de la Federación, en ejercicio de sus facultades de revisión y fiscalización.
- El titular y los subsecretarios de la Secretaría de la Función Pública, en ejercicio de sus facultades de investigación o auditoría en el ámbito de sus funciones.
- La Unidad de Fiscalización de los Recursos de los Partidos Políticos, órgano técnico del Consejo General del Instituto Federal Electoral, para el ejercicio de sus atribuciones legales.

Los empleados y funcionarios de las Entidades son responsables por violación del secreto financiero y las Entidades están obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen.

PARTE III: INICIATIVAS DE INNOVACIÓN FINANCIERA.

SECCIÓN 10.- BANCA ELECTRÓNICA.

Concepto

La prestación de servicios a través de Internet es un fenómeno que ha alcanzado a la mayoría de los sectores de la economía. El tipo de atención que puede prestarse a través de Internet y de los dispositivos que permiten acceso a esta, puede variar. En el caso de los servicios financieros, la mayoría del sector presta servicios llamados "tradicionales" como son cajeros electrónicos y tarjetas. Las operaciones en línea tienen el potencial de aumentar el número de clientes y mejorar la lealtad de los Clientes. Esto a la vez que reduce costos operativos.

A pesar de la prevalencia en nuestro país de los teléfonos celulares, el uso de servicios financieros en línea o a través de dichos dispositivos (o en su defecto, de computadores), aún es baja. La exclusión de una gran parte de la población mexicana a servicios financieros impide el desarrollo de sectores poco favorecidos que urgentemente necesitan contar con créditos hipotecarios para viviendas dignas, créditos para pequeños negocios, préstamos para estudios, entre otros. Este fenómeno es más agudo en el sector rural, donde está proyectada la vocación del SACP.

El uso de los Servicios Electrónicos tiene ventajas múltiples, entre las que se encuentran:

(i) La seguridad de los receptores de pago de no traer grandes cantidades de efectivo.

(ii) Servir de base para servicios electrónicos más complejos o de mayor valor agregado.

(iii) Eficiencias en los procesos de las Entidades.

(iv) Reducción de la "fricción" en la relación entre los clientes y las Entidades.

Consideramos al momento de preparar esta Guía Legal que, para efecto de dar un enfoque sistemático a la misma y ahorrar al lector la tarea de consultar la regulación aplicable, era

necesario exponer la regulación de los Servicios Electrónicos de una manera resumida y fácil de consultar. Desde luego, esto no sustituye la necesidad de consultar las Disposiciones Generales en caso de requerir un estudio normativo más profundo.

Uno de los Servicios Electrónicos que más han cobrado auge son los "Servicios Básicos Móviles" o "Pago Móvil", al Servicio Electrónico en el cual el Dispositivo de Acceso se encuentra asociado con correspondencia unívoca al Identificador de Usuario, mediante cualquier información o datos únicos del propio Dispositivo de Acceso. Sin embargo, como veremos, no es el único y hay variedades de los Servicios Electrónicos que requieren una atención específica.

Las competencias mínimas que se recomiendan para este tipo de Proyectos son las siguientes[45] [46]:

- Alimentar una relación constructiva con los Reguladores.
- Crear confianza en el Cliente final mediante campañas de publicidad adecuadas, operación eficiente de las tecnologías, cumplimiento de las expectativas ofrecidas.
- Contar con un manejo transparente y eficiente de los fondos que se manejen a través de los Servicios Electrónicos, incluyendo (i) atención a clientes efectiva, (ii) reducción de tiempos en procesos de reclamación y (iii) establecer métricas de medición de satisfacción.
- Facilitar la entrada y salida de fondos: el Cliente debe tener la certeza de que su dinero está a salvo y que puede disponer de él en los momentos acordados en cada Servicio Electrónico.
- Planear de antemano la escalabilidad del Proyecto: en caso de Servicios Electrónicos que tienen el potencial de una adopción masiva o muy rápida, el sistema de la Entidad, así como los sistemas de los Proveedores Relevantes deben ser capaces de ampliar y satisfacer las necesidades de los nuevos clientes.
- Canales de atención accesibles y rápidos para aumentar índices de satisfacción en caso de que existan situaciones que requieran el apoyo de la Entidad para solucionar problemas del Cliente.

[45] MCCONNELL, Steve. Desarrollo y gestión de proyectos informáticos. Microsoft Press.
[46] EDINI GONZÁLEZ, Alejandro. Gestión de Proyectos de Software. (2002)

- Construir el modelo de Servicio Electrónico basado en la seguridad de la información (ver Sección 7), no sólo bajo los estándares de la ley y la regulación[47], sino en la constante mejora y revisión continua de vulnerabilidades.

10.1 Uso de Medios Electrónicos.

Desde el punto de vista normativo, la regulación[48] permite a las Entidades la celebración de operaciones y la prestación de servicios a sus Clientes (Socios o Usuarios, según sea el caso) mediante Servicios Electrónicos. Esto es, a través de los equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados y que previamente pacten las Entidades con sus socios para la celebración de sus operaciones y la prestación de sus servicios. Lo anterior siempre que las Entidades cumplan con las siguientes reglas:

I. En la contratación respectiva se establezca de manera clara y precisa, lo siguiente:

- Las operaciones y servicios que podrán proporcionarse a través de Medios Electrónicos.
- Los mecanismos y procedimientos de Identificación del Usuario y Autenticación, así como las responsabilidades del Usuario y de la Entidad respecto del uso de Servicios Electrónicos.
- Los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados por la Entidad, a través de Servicios Electrónicos.
- Los límites de los montos individuales y agregados diarios, específicos para los Servicios Electrónicos de que se trate (conforme a los límites regulatorios y el tipo de producto).
- Los mecanismos y procedimientos de cancelación de la contratación de Servicios Electrónicos, los cuales deberán ser similares a los de la propia contratación, considerando el tiempo de respuesta de la solicitud, canales de atención al Usuario y procedimientos de Identificación del Usuario y su Autenticación.

[47] LACP, LRASCAP, Disposiciones Generales SOFIPO y Disposiciones Generales SOCAP.
[48] *Ibidem.*

- Las restricciones operativas aplicables de acuerdo con el Medio Electrónico de que se trate.

II. Informen a los Usuarios de forma previa a la contratación los términos y condiciones para los Servicios Electrónicos, debiendo mantener dicha información disponible para su consulta en cualquier momento.

III. Comuniquen a los Usuarios los riesgos inherentes a la utilización de Servicios Electrónicos, así como que hagan de su conocimiento sugerencias para prevenir la realización de operaciones irregulares o ilegales, por ejemplo, mediante campañas periódicas de difusión de recomendaciones de seguridad.

Consentimiento y Reglas de Contratación

Las Entidades, para operar Servicios Electrónicos, deben obtener el consentimiento expreso de sus Usuarios mediante firma autógrafa, previa identificación de estos, o bien, mediante Firmas Electrónicas Avanzadas o Fiables de los propios Usuarios, siempre y cuando estas sean válidas conforme a la regulación aplicable (ver Sección 12 Implementación de la Firma Electrónica). Sin embargo, podrá obtenerse el consentimiento de sus Usuarios mediante alguna otra forma de contratación, tratándose de los servicios siguientes:

- Servicios de Pago Móvil;
- Servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, cuando estos se refieran exclusivamente a la operación de cuentas catalogadas como de Bajo Riesgo[49].

[49] Las cuentas de Bajo Riesgo deberán ajustarse a la suma de los abonos en el transcurso de un mes calendario y no podrán exceder al equivalente en moneda nacional a mil Unidades de Inversión. Sin embargo, las Disposiciones PLD/FT establecen que las cuentas de depósito a la vista en moneda nacional que ofrezcan las Sociedades serán consideradas de bajo Riesgo y, por lo tanto, podrán contar con requisitos de identificación simplificados, siempre y cuando sean abiertas de forma presencial por Clientes personas físicas, cuya operación se encuentre limitada a abonos iguales al equivalente en moneda nacional a tres mil Unidades de Inversión por Cliente, en el transcurso de un mes calendario.

- "Servicios Avanzados Móviles[50]", "Servicio por Internet[51]", "Servicio Telefónico Audio Respuesta[52]" y "Servicio Telefónico Voz a Voz[53]", cuando estén asociados a cuentas de Bajo Riesgo y sean operaciones diferentes a las que requieran Factores de Autenticación 3 o 4 (ver Sección 6):

- Los contratados a través de Cajeros Automáticos y Terminales Punto de Venta, siempre y cuando estos servicios sean utilizados para realizar operaciones monetarias hasta de Mediana Cuantía[54]. Para dicha contratación, la Entidad deberá solicitar a los Usuarios un segundo Factor de Autenticación de las Categorías 3 o 4[55] (según se explica posteriormente en la **Sección 10.2** del presente documento). De igual manera, la Entidad deberá asumir los riesgos y, por lo tanto, los costos de las operaciones realizadas a través de los servicios antes mencionados que no sean reconocidas por los Usuarios. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

Las Entidades pueden permitir a sus Usuarios la contratación de servicios y operaciones adicionales a las originalmente convenidas o modificar las condiciones previamente pactadas con el Usuario al contratar el uso de Servicios Electrónicos, siempre y cuando la Entidad requiera un segundo Factor de Autenticación de las Categorías 3 o 4, adicional al utilizado, en su caso, para iniciar la Sesión[56]. En estos casos, la Entidad deberá enviar una

[50] Significa el Servicio Electrónico, en el cual el Dispositivo de Acceso se encuentra asociado con correspondencia unívoca al Identificador de Usuario, mediante cualquier información o datos únicos del propio Dispositivo de Acceso.

[51] Servicio Electrónico efectuado a través de la red electrónica mundial denominada Internet, en el sitio que corresponda a uno o más dominios de la Sociedad, incluyendo el acceso mediante el protocolo WAP o alguno equivalente.

[52] Significa el Servicio Electrónico mediante el cual la Sociedad recibe instrucciones del Usuario a través de un sistema telefónico, e interactúa con el propio Usuario mediante grabaciones de voz y tonos o mecanismos de reconocimiento de voz, incluyendo los sistemas de respuesta interactiva de voz (IVR).

[53] Significa el Servicio Electrónico mediante el cual un Usuario instruye vía telefónica a través de un representante de la Sociedad debidamente autorizado por esta, con funciones específicas a realizar operaciones a nombre del propio Usuario.

[54] Operaciones de hasta el equivalente en moneda nacional a 1,500 UDIs diarias.

[55] Factor de Autenticación Categoría 3: Se compone de información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. El Factor de Autenticación Categoría 4: Se compone de información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras.

[56] Es decir, periodo en el cual los Usuarios podrán llevar a cabo consultas, Operaciones Monetarias o cualquier otro tipo de transacción, una vez que hayan ingresado a los Servicios Electrónicos con su Identificador de Usuario.

notificación conforme a lo señalado más delante y el servicio correspondiente quedará habilitado para su uso en el periodo determinado por cada Entidad, sin que pueda ser menor a treinta minutos contados a partir de que se haya efectuado la contratación.

Tratándose de los Servicios de Pago Móvil y aquellos ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, cuando estos se refieran exclusivamente a la operación de cuentas de Bajo Riesgo, la contratación podrá llevarse a cabo de conformidad con lo señalado anteriormente o bien, a través de operadores telefónicos de la propia Entidad, sujetándose a lo señalado en las reglas para Factores de Autenticación Categoría I. En todo caso, para el servicio de Pago Móvil, la Entidad deberá autenticar a los Usuarios utilizando procedimientos que aseguren que el propio Usuario es quien está solicitando el servicio.

Tratándose de operaciones de Cuentas de Bajo Riesgo, la Entidad deberá solicitar a sus Usuarios al momento de la contratación datos de algún medio de comunicación, tales como su dirección de correo electrónico o número de teléfono móvil para la recepción de mensajes de texto SMS, a fin de que la Entidad haga llegar las notificaciones requeridas para llevar a cabo la identificación.

10.2 Identificación y Autenticación de Usuarios.

La Entidad, para permitir el inicio de una Sesión, deberá solicitar y validar, al menos:

(a) El Identificador de Usuario, el cual debe ser de al menos seis caracteres, único para cada Usuario y permitir a la Entidad identificar todas las operaciones realizadas por el propio Usuario a través del Servicio Electrónico. Tratándose de operaciones realizadas a través de Terminales Punto de Venta y Cajeros Automáticos, el Identificador de Usuario podrá ser el número de la tarjeta de crédito o débito con la cual se accede a Servicios Electrónicos, y

(b) Un Factor de Autenticación de las Categorías 2 o 4.

El uso del Identificador de Usuario y los Factores de Autenticación, deberán ajustarse a lo siguiente:

(a) Proveer lo necesario para impedir la lectura en la pantalla del Dispositivo de Acceso, de la información de identificación y Autenticación proporcionada por el Usuario, salvo que se trate de Servicio Telefónico de Audio Respuesta.

En caso de que la tecnología utilizada en servicios de Pago Móvil no permita implementar lo anterior y la información de los Factores de Autenticación se almacene en el dispositivo, la Entidad podrá ofrecer tal servicio obteniendo la previa autorización de la CNBV, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.

Asimismo, la Entidad que obtenga la autorización a que se refiere el párrafo anterior, deberá prever que asumirá los riesgos y por lo tanto los costos de las operaciones realizadas a través de Pago Móvil que no cumplan con las normas anteriores y que no sean reconocidas por los Usuarios. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

(b) Se debe asegurar que, en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Usuario quien los reciba, active, conozca, desbloquee y restablezca. El Usuario podrá autorizar a un tercero para recibir dichos Factores de Autenticación, siempre que la Entidad mantenga procedimientos para que dichas autorizaciones sean de carácter eventual y puedan ser revocados por el Usuario cuando así lo solicite.

(c) Contar con procedimientos para invalidar los Factores de Autenticación para impedir su uso en Servicios Electrónicos cuando un Usuario o la misma Entidad cancele el uso de dicho servicio o cuando dicho Usuario deje de formar parte de la Entidad.

Factores de Autenticación

La Entidad deberá utilizar Factores de Autenticación para verificar la identidad de sus Usuarios y la facultad de estos para realizar operaciones a través de Servicios Electrónicos.

Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en la regulación conforme a lo siguiente:

Categoría	Descripción	Reglas de Uso
Categoría 1	Información obtenida mediante la aplicación de cuestionarios por parte de operadores telefónicos, en los cuales se requieran datos que el Usuario conozca. No deben componerse de información incluidas en comunicaciones electrónicas o impresas enviadas a los Usuarios. Las Entidad podrá usar un solo Factor de Autenticación de esta categoría en estos casos: Para la Autenticación de Usuarios que pretendan utilizar Servicio Telefónico Voz a Voz para realizar transacciones; Para la contratación de Pago Móvil, y Para el Desbloqueo de Factores de Autenticación, así como la reactivación o desactivación temporal del uso de Servicios Electrónicos, mediante operadores telefónicos.	Definición previa de los cuestionarios. Validación de al menos una de las respuestas del Usuario mediante medios informáticos, sin que el operador los conozca o pueda consultar los datos de Autenticación.
Categoría 2	Información que solo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como	No puede consistir en:

Categoría	Descripción	Reglas de Uso
	Contraseñas y Números de Identificación Personal (NIP). Para realizar operaciones con Cuentas Recurrentes la Entidad puede pedir un Factor de Autenticación Categoría 2, 3 o 4.	El Identificador de Usuario. Nombre de la Entidad. Más de tres caracteres consecutivos idénticos. Más de tres caracteres consecutivos numéricos o alfabéticos. Lo anterior no es aplicable a Pago Móvil ni para Servicios Avanzados Móviles ni operaciones de Cajeros Automáticos y Terminales Punto de Venta, si la Entidad informa al Usuario al momento de la contratación sobre la importancia de las medidas de seguridad para esos servicios. • La longitud deberá ser de al menos seis caracteres, salvo para servicios ofrecidos en Cajeros Automáticos y Terminales punto de Venta (cuatro), Pago Móvil (cinco) y Servicios por Internet (ocho). • La composición deberá incluir caracteres alfabéticos y números cuando el Dispositivo de Acceso lo permita. • La Sociedad debe permitir al Usuario cualquier cambio en su información de Autenticación

Categoría	Descripción	Reglas de Uso
		cuando lo requiera mediante Servicios Electrónicos. • Tratándose de contraseñas o NIP generados durante la contratación de los Servicios Electrónico o en su restablecimiento, la Entidad deberá prever mecanismos para su inmediata modificación. • Recomendar el uso de contraseñas seguras.
Categoría 3	Información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por la Entidad a sus Usuarios. Se debe utilizar un segundo Factor de esta Categoría o Categoría 4 para: Transferencias de recursos dinerarios a cuentas destino de terceros u otras Entidades, así como instrucciones de domiciliación, salvo ciertos casos de cuentas destino preautorizadas donde un solo Factor de Autenticación será necesario.	Contar con propiedades que impidan su duplicación o alteración. • Ser información dinámica que no podrá ser utilizada en más de una ocasión. • Tener una vigencia que no podrá exceder los dos minutos (salvo por contraseñas dinámicas). • No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Entidad o por terceros. Dentro de esta categoría se encuentra la información del chip de tarjetas de crédito o débito siempre

Categoría	Descripción	Reglas de Uso
	Pago de contribuciones. Establecimiento e incremento de límites de monto para Operaciones Monetarias. Registro de cuentas Destino de terceros u otras Entidades. Alta y modificación del medio de notificación de eventos relacionados con los Servicios Electrónicos. Consultas de estados de cuenta u otras consultas que permitan conocer información relacionada con el Usuario, salvo algunas excepciones para operaciones de crédito. Contratación de Servicios Electrónicos o de operaciones y servicios adicionales a los originalmente convenidos, conforme a las disposiciones aplicables. Desbloqueo de contraseñas o NIP.	que la información se obtenga de ahí por el Dispositivo de Acceso. La Entidad que apruebe la celebración de operaciones mediante el uso de tarjetas de crédito y débito sin circuito integrado, en Cajeros Automáticos y Terminales Punto de Venta, debe pactar con sus Usuarios que asumirá los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación. Tratándose del Servicio de *Host to Host*[58], la Sociedad podrá utilizar como Factor de Autenticación de esta categoría, cualquier mecanismo que les permita verificar que los equipos de cómputo o dispositivos utilizados por los Usuarios, para establecer la

[58] Servicio Electrónico mediante el cual se establece una conexión directa entre los equipos de cómputo del Usuario previamente autorizados por la Sociedad y los equipos de cómputo de la propia Sociedad, a través de los cuales estos últimos procesan la información para la realización de servicios y operaciones. Este tipo de servicios incluirán a los proporcionados a través de las aplicaciones conocidas como "Cliente-Servidor".

Categoría	Descripción	Reglas de Uso
	Retiro de efectivo en Cajeros Automáticos. Lo anterior no será necesario en el caso de operaciones de Pago Móvil, pues en ese caso puede utilizarse con al menos un Factor de Autenticación Categoría 2. Operaciones de "Micro Pagos[57]"realizadas en Terminales Punto de Vista o celulares no requieren de factores de autenticación, siempre que las Entidades asuman los riesgos derivados de dichas operaciones. En el caso de servicios prestados a personas morales deberá utilizarse un Factor de Autenticación de esta categoría cuando existan esquema de firmas compartidas para validar transacciones. Alta de Cuentas de Destino Recurrentes. Para realizar operaciones con ellas la Entidad puede pedir un Factor de Autenticación Categoría 2, 3 o 4.	comunicación, son los que la propia Sociedad autorizó. Se permite el uso de tablas aleatorias de contraseñas como Factor de Autenticación 2, siempre que se cumplan con ciertas características y se obtenga la previa autorización de CNBV. En este caso la Entidad asumirá los riesgos y costos de operaciones no reconocidas y asumir la obligación de abonar estas operaciones a más tardar cuarenta y ocho horas después de la reclamación.

[57] Operaciones de hasta el equivalente en moneda nacional a 70 UDI.

Categoría	Descripción	Reglas de Uso
Categoría 4	Información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras. En general su uso es idéntico al de los Factores Categoría 3.	Aplicar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario. La Entidad podrá considerar dentro de esta categoría la firma autógrafa de sus Usuarios en los comprobantes generados por las Terminales Punto de Venta o bien la plasmada en dispositivos ópticos que produzcan la imagen digitalizada de la firma, únicamente cuando los propios Usuarios realicen Operaciones Monetarias referidas al pago de bienes o servicios a través de dichas Terminales Punto de Venta.

Tabla 1. Factores de Autenticación

Autenticación de Servicios por Internet.

Las Entidades, al inicio de Sesión del Usuario, están obligadas a realizar lo siguiente:

- Proporcionar al Usuario información suficiente para que antes de ingresar su identificación y Autenticación, sea posible determinar que se trata efectivamente del sistema de la Entidad, mediante (i) uso de información proporcionada previamente por el Usuario o éste haya señalado para ese fin, o (ii) aquella que el Usuario pueda verificar mediante un dispositivo o medio puesto a su disposición para ese fin.
- Verificada la identificad de la Entidad, esta debe proporcionar los datos de ingreso de la última Sesión, así como el nombre del Usuario.

10.2.1 Operación de Servicios Electrónicos

Para la operación de Servicios Electrónicos, existen varias reglas relacionadas con el alta y uso de las Cuentas Destino:

- Para la celebración de transferencias de recursos y pagos de operaciones a través de Servicios Electrónicos, las Entidades deberán asegurarse de que los Usuarios registren en los Servicios Electrónicos de que se trate, las Cuentas Destino previamente a su uso.
- Respetar los tiempos de espera para dar de alta las Cuentas Destino.
- Validar la estructura de la Cuenta de Destino.
- Para las Operaciones Monetarias que se realicen a través del Servicio Host to Host, Terminales Punto de Venta, Cajeros Automáticos y Pago Móvil, no se requerirá que los Usuarios registren las Cuentas Destino; tampoco para las que se realicen mediante Servicios Avanzados Móviles, siempre que, tratándose de este último, el monto de dichas operaciones sea hasta el equivalente a las de Mediana Cuantía por cada operación.

Asimismo, las Entidades pueden permitir el uso de Cuentas Destino con el carácter de Recurrente, siempre que se cumplan con ciertos requisitos, por ejemplo, (i) haber

transcurrido más de noventa días desde su registro como Cuenta Destino, (ii) que se haya utilizado la Cuenta Destino en tres ocasiones al menos y (iii) no existan reclamaciones en relación con dichas operaciones durante ese periodo de noventa días.

Modificación de límites de Operaciones Monetarias

Las Entidades pueden permitir a los Usuarios establecer límites de monto para las Operaciones Monetarias siempre que se obtenga el consentimiento de los Usuarios mediante la firma autógrafa en las oficinas de la Entidad, con previa identificación de éstos.

Tipo de Servicio	Requisito
Reducción de límites para monto de Operaciones Monetarias en Servicios Electrónicos.	Factor de Autenticación Categoría 2.
Reducción de límites para monto de Operaciones Monetarias en Servicios Telefónicos de Voz a Voz.	Factor de Autenticación Categoría 1.
Establecimiento de límites de transferencias de dinero y pago de contribuciones.	Medidas tomadas por la Entidad (por regla general estas requieren Factores de Autenticación Nivel 3 o 4 para su celebración).
Servicios por Internet.	Medidas tomadas por la Entidad.
Servicios Telefónicos Voz a Voz.	Medidas tomadas por la Entidad.
Servicios Telefónicos Audio Respuesta.	Medidas tomadas por la Entidad.
Servicios Avanzados Móviles.	Medidas tomadas por la Entidad.
Cajeros Automáticos.	El monto acumulado diario de Operaciones Monetarios con cargo a la cuenta del Usuario no podrá

Tipo de Servicio	Requisito
	exceder las Operaciones Monetarias de Media Cuantía, salvo algunas excepciones específicas por tipo de servicio.
Pago Móvil.	No podrá exceder las Operaciones Monetarias de Media Cuantía por cuenta en un día ni 6,000 UDI mensuales.
Micro Pagos.	El saldo disponible de la cuenta asociada al teléfono móvil no podrá superar las 250 UDI.

Tabla 2. Tipos de Servicio

No obstante lo anterior, las Entidades pueden definir límites inferiores específicos para Servicios Electrónicos, siempre y cuando no se contravenga la normatividad secundaria.

Confirmación de Operaciones

Las Entidades deberán solicitar a los Usuarios que confirmen la celebración de una Operación Monetaria, previo a que se ejecute, haciendo explícita la información suficiente para darle certeza al Usuario de la operación que se realiza.

Se exceptúa de lo anterior a los Servicios Electrónicos ofrecidos a través de Terminales Punto de Venta.

Comprobantes

Las Entidades deben establecer mecanismos y procedimientos para que los Servicios Electrónicos generen los comprobantes correspondientes respecto de las operaciones y servicios realizados por los Usuarios a través de dichos Servicios Electrónicos.

Notificación de Eventos

Las Entidades están obligadas a notificar a la brevedad posible a sus Usuarios, a través de los medios de comunicación que estos hayan elegido para tal fin, cualquiera de los siguientes eventos realizados a través de Servicios Electrónicos:

- Transferencias de recursos dinerarios a cuentas de terceros u otras Entidades, incluyendo el pago de créditos y de bienes o servicios, así como las autorizaciones e instrucciones de domiciliación de pago de bienes o servicios;
- Pago de contribuciones;
- Modificación de límites de montos de operaciones;
- Registro de Cuentas Destino de terceros u otras Sociedades, así como el registro de estas como Cuentas Destino Recurrentes;
- Alta y modificación del medio de notificación al Usuario, debiendo enviarse tanto al medio de notificación anterior como al nuevo;
- Contratación de Servicios Electrónicos o modificación de las condiciones para el uso de Servicios Electrónicos previamente contratado;
- Desbloqueo de Contraseñas o Números de Identificación Personal (NIP), como también para la reactivación del uso de Servicios Electrónicos;
- Modificación de Contraseñas o Números de Identificación Personal (NIP) por parte del Usuario, y
- Retiro de efectivo en Cajeros Automáticos.

Las Entidades deben asegurarse de que la información transmitida para notificar al Usuario sobre los eventos referidos no contenga números de cuenta completos, domicilios, ni saldos de cuentas de depósito. No obstante, las Entidades podrán transmitir la información del saldo de la cuenta para Pago Móvil, siempre que la cuenta asociada a dicho servicio sea de Bajo Riesgo.

Las notificaciones sobre la realización de las (i) transferencias de recursos y (ii) pagos de contribuciones efectuadas a través de Pago Móvil, Cajeros Automáticos y Terminales Punto de Venta, deberán ser enviadas cuando el acumulado diario de dichas operaciones por

Servicios Electrónicos de que se trate sea mayor al equivalente en moneda nacional a 600 UDIs, o bien, cuando las Operaciones Monetarias en lo individual sean mayores al equivalente en moneda nacional a 250 UDIs. Este último caso, se presentará siempre que las Entidades cuenten con esquemas específicos de prevención de fraudes con el fin de revisar continuamente aquellas operaciones que puedan constituir un uso no autorizado de los Servicios Electrónicos.

En ningún caso las Entidades permitirán la modificación del medio de notificación a través de Cajeros Automáticos y Terminales Punto de Venta. Las Entidades deberán permitir a los Usuarios modificar el medio de notificación de los Servicios Electrónicos ofrecidos en Cajeros Automáticos o Terminales Punto de Venta mediante atención telefónica, utilizando un Factor de Autenticación Categoría 1.

Se exceptúa de lo anterior a las operaciones realizadas mediante el Servicio *Host to Host*.

10.3 Seguridad de la Información de Banca Electrónica.

Este tema fue tratado en la Sección 7 de la presente Guía Legal.

Seguridad en Sesiones

Las Entidades, para efecto de garantizar que las Sesiones de los Usuarios, no puedan ser usadas por un tercero. Deberán establecer mecanismos: (i) para dar por terminada la Sesión de forma automática en ciertos supuestos e (ii) impedir el acceso en forma simultánea, entre otras reglas.

Bloqueo de Contraseñas

Las Entidades deben establecer mecanismos para bloquear el uso de Contraseñas y otros Factores de Autenticación para los Servicios Electrónicos, por lo menos en los casos en que (i) se intente ingresar a dichos servicios utilizando información de autenticación incorrecta, o (ii) cuando el Usuario se abstenga de realizar operaciones por un periodo que determine la Entidad en sus Manuales de acuerdo con el Medio Electrónico correspondiente.

Las Entidades podrán desbloquear el uso de Factores de Autenticación que previamente hayan sido bloqueados conforme a lo anterior, para lo cual podrán utilizar un Factor de Autenticación Categoría 1, o bien, realizar a los Usuarios preguntas secretas[59], cuyas respuestas deben conservarse almacenadas en forma cifrada.

Con independencia de lo anterior, las Entidades deberán permitir al Usuario el restablecimiento de Contraseñas y Números de Identificación Personal (NIP).

Manejo de Contraseñas y Factores de Autenticación

Para el manejo de Contraseñas y otros Factores de Autenticación, las Entidades se sujetarán a lo siguiente:

- Deben mantener procedimientos que proporcionen seguridad en la información contenida en los dispositivos de Autenticación en su custodia, para su distribución, así como en la asignación y reposición de estos.
- Prohibición de contar con mecanismos, algoritmos o procedimientos que les permitan conocer, recuperar o descifrar los valores de cualquier información relativa a la Autenticación de los Usuarios.
- Tendrán prohibido solicitar a los Usuarios, a través de sus funcionarios, empleados, representantes o comisionistas, la información parcial o completa, de los Factores de Autenticación de las Categorías 2 o 3.

Se exceptúa de lo anterior a las operaciones realizadas por Servicio Telefónico Voz a Voz, siempre y cuando el Usuario haya iniciado la llamada, se requiera información parcial del Factor de Autenticación de las Categorías 2 o 3 y cuando éste sea utilizado exclusivamente para Servicios Electrónicos.

[59] Se entenderá por pregunta secreta al cuestionamiento que define el Usuario o la Entidad durante el proceso de contratación de Servicios Electrónicos, respecto del cual se genera información como respuesta. Cada pregunta secreta que se defina únicamente podrá ser utilizada en una ocasión.

Desactivación de Servicios Móviles

Las Entidades deben establecer procedimientos para que los Usuarios de Pago Móvil y Servicios Avanzados Móviles puedan, en todo momento, desactivar su uso de forma temporal en caso de requerirlo, así como establecer procedimientos para reactivar el uso cuando el Usuario lo disponga.

La desactivación del uso de manera temporal de los Servicios Electrónicos mencionados debe realizarse en todo momento dentro de una Sesión en el mismo servicio, o bien, a través de algún otro servicio que el Usuario tenga contratado, debiendo requerir en ambos casos, un Factor de Autenticación de cualquier Categoría.

Para la reactivación del uso de Servicios Electrónicos de Pago Móvil o Servicios Avanzados Móviles, los Usuarios podrán utilizar los mismos mecanismos usados para la contratación de éstos, o bien, un Factor de Autenticación Categoría 1.

Servicios a través de Operadores Telefónicos, Cajeros Automáticos y Puntos de Venta.

Las Entidades deben establecer procedimientos para que los Usuarios de Pago Móvil y Servicios Avanzados Móviles puedan, en todo momento, desactivar su uso de forma temporal en caso de requerirlo, así como establecer procedimientos para reactivar el uso cuando el Usuario lo disponga. La desactivación del uso de manera temporal de los Servicios Electrónicos mencionados en el párrafo anterior deberá realizarse en todo momento dentro de una Sesión en el mismo servicio, o bien, a través de algún otro servicio que el Usuario tenga contratado, debiendo requerir en ambos casos, un Factor de Autenticación de cualquier Categoría.

Para la reactivación del uso de Servicios Electrónicos los Usuarios podrán utilizar los mismos mecanismos señalados para la contratación de estos, o bien, un Factor de Autenticación Categoría 1.

En el caso de servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta (propios o de terceros contratados por la Entidad), éstos deben contar con lectores que permitan obtener la información de las Tarjetas de crédito o débito con Circuito

Integrado (debiéndose leer la información del propio chip). Se exceptúa de lo anterior a los siguientes:

- Los dispositivos conectados a teléfonos móviles y funcionen de manera similar a las Terminales Punto de Venta.
- Las Terminales Punto de Venta en las que únicamente se acepten tarjetas emitidas por la Sociedad adquirente.

En todo caso, las Entidades deberán dar cumplimiento a las reglas de uso de Factores de Autenticación que correspondan.

10.4 Monitoreo de Operaciones por Banca Electrónica.

Mantener mecanismos de control para la detección y prevención de eventos que se aparten de los parámetros de uso habitual de los Usuarios a través de Medios Electrónicos es obligatorio para las Entidades. Para tales efectos, las Entidades podrán:

- Solicitar a los Usuarios la información que estimen necesaria para definir el uso habitual que estos hagan de Servicios Electrónicos.
- Aplicar, bajo su responsabilidad, medidas de prevención, tales como la suspensión de la utilización de Servicios Electrónicos o, en su caso, de la operación que se pretenda realizar, en el evento de que cuenten con elementos que hagan presumir que el Identificador de Usuario o los Factores de Autenticación no están siendo utilizados por el propio Usuario, debiendo informar a éste tal situación de forma inmediata.

Las Entidades deberán mantener en bases de datos las incidencias, fallas o vulnerabilidades detectadas en los Servicios Electrónicos, así como todas las operaciones efectuadas a través de Servicios Electrónicos que no sean reconocidas por los Usuarios, incluyendo información relacionada con las fallas, o eventos y aquella relacionada con operaciones no reconocidas, entre otras[60].

[60] "La información deberá mantenerse en la Sociedad durante un periodo no menor a cinco años contado a partir de su registro, sin perjuicio de otras disposiciones que resulten aplicables".

Bitácoras y huellas de auditoría.

Las Entidades deben generar registros, bitácoras, huellas de auditoría de las operaciones y servicios realizados a través de Medios Electrónicos y, en el caso del Servicio Telefónico Voz a Voz, grabaciones adicionales de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso de Servicios Electrónicos, observando ciertas reglas mínimas de almacenamiento de información.

Asimismo, deben contar con mecanismos para que la información de los registros de las bitácoras en los diferentes equipos críticos de cómputo y telecomunicaciones utilizados en las operaciones de Servicios Electrónicos sea consistente.

Robo o extravío de Dispositivos de Acceso o Autenticación

Las Entidades deberán proveer procedimientos y mecanismos para que los Usuarios les reporten el robo o extravío de los Dispositivos de Acceso o, en su caso, de su información de identificación y Autenticación, que impidan el uso indebido de los mismos. Asimismo, deberán establecer políticas que definan las responsabilidades tanto del Usuario como de la Entidad, respecto de las operaciones que hayan sido efectuadas previas al reporte.

Las Entidades deberán contar con procedimientos y mecanismos para que el reporte de robo o extravío pueda ser enviado por el Usuario tanto a través de Medios Electrónicos, como por cualquier medio que defina la Entidad. Cada reporte de robo o extravío deberá generar un folio que se haga del conocimiento del Usuario y que le permita dar seguimiento a dicho reporte.

Adicionalmente, la Entidad debe establecer procedimientos y mecanismos para la atención y seguimiento de las operaciones realizadas a través de Servicios Electrónicos que no sean reconocidas por los Usuarios.

Las Entidades están obligadas a realizar revisiones de seguridad enfocadas a verificar la suficiencia en los controles aplicables a la infraestructura de cómputo y telecomunicaciones utilizada para la realización de operaciones y prestación de servicios a través de Medios Electrónicos. Las revisiones deben realizarse al menos en forma anual, o bien, cuando se presenten cambios significativos en dicha infraestructura, debiendo

comprender ciertos temas, entre ellos unos mecanismos de Autenticación, configuración de controles, actualización, análisis de vulnerabilidades, entre otros.

Asimismo, las Entidades deben mantener en su infraestructura de cómputo y telecomunicaciones para la operación de Servicios Electrónicos, dispositivos y medios automatizados para detectar y prevenir eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los Usuarios, así como aquellos que eviten conexiones y flujos de datos entrantes o salientes no autorizados. Igualmente, las Entidades deberán mantener controles que eviten la divulgación no autorizada de la información de configuración de dicha infraestructura.

Áreas de Soporte

Las Entidades están obligadas a contar con áreas de soporte técnico y operacional encargadas de atender y dar seguimiento a las incidencias que tengan los Usuarios de Servicios Electrónicos, así como a eventos de seguridad relacionados con el uso de Medios Electrónicos.

En todo caso, las Entidades deben procurar la operación continua de la infraestructura de cómputo y de telecomunicaciones, así como dar pronta solución, para restaurar los Servicios Electrónicos en caso de presentarse algún incidente.

Responsabilidad de la Dirección General.

La Dirección General debe asegurar que la Entidad cuente con medidas preventivas, de detección, disuasivas y procedimientos de respuesta a incidentes de seguridad, controles y medidas de seguridad informática para mitigar amenazas y vulnerabilidades relacionadas con los servicios proporcionados a través de Servicios Electrónicos que puedan afectar a los Usuarios o a la operación de la Entidad. Las medidas y procedimientos deben ser evaluados por el área de Auditoría Interna para determinar su efectividad y, de ser necesario, realizar las actualizaciones correspondientes. En caso de que se detecte la existencia de vulnerabilidades y riesgos asociados a los servicios mencionados, deberán tomarse medidas de forma oportuna previniendo que los Usuarios o la Entidad puedan verse afectados.

Acciones Correctivas

Las Entidades deberán implementar las acciones correctivas que CNBV les requiera como resultado de la identificación de riesgos asociados con el uso de Servicios Electrónicos.

Fuerza Mayor

En caso de catástrofes naturales u otras situaciones que afecten la adecuada oferta a nivel nacional de operaciones y servicios, y que por su naturaleza justifiquen temporalmente el uso masivo de Medios Electrónicos, la CNBV podrá autorizar a las Entidades prestar Servicios Electrónicos en términos distintos a los señalados en la normatividad, de acuerdo con las necesidades del Público Usuario y con los riesgos asociados, por un determinado periodo hasta que se restablezcan las condiciones normales.

10.5 Implementación de Banca Electrónica.

En la Sección 2 hemos delineado la metodología de planeación de los Proyectos, misma que puede considerarse para la implementación de un Proyecto relacionado con Banca Electrónica. Como se ha visto en la descripción de la normativa anterior, existen varios conceptos reconocidos bajo dicha denominación. En ese sentido cada Proyecto deberá atender a las características regulatorias del tipo de Servicio Electrónico seleccionado.

10.6 Diagrama y Plan de Trabajo.

La idea de esta sección es ofrecer herramientas prácticas y conceptuales generales para implementar un Servicio Electrónico. Los particulares de cada caso deben ser tenidos en consideración, sobre todo porque la regulación, tal como se expuso en las secciones anteriores hace distinciones importantes dependiendo el tipo de Servicio. Nuestro objetivo es que las Partes Responsables de un Proyecto encargado de implementar un sistema de Banca Electrónica puedan asignar las tareas y objetivos específicos y verificar el avance del Proyecto. Esto, de manera típica involucra al Consejo de Administración (cuando no a la asamblea de accionistas), al Director General, Auditoría Interna y a las demás personas mencionadas en la Sección 3. Asimismo, estos Proyectos requieren de la participación de proveedores o prestadores de servicios tecnológicos, por lo que será necesario incorporar a la planeación los aspectos mencionados en la Sección 14.

Sugerimos que un proceso de implementación de un Proyecto de Servicios Electrónicos, considerando el marco genérico que señalamos en la Sección 2 de la presente Guía Legal, adopte los siguientes pasos:

A. Definición del proyecto.

La definición del Proyecto implicará la investigación de los Servicios Electrónicos, incluyendo:

(a) La identificación de los beneficios que obtendrá la Entidad derivados de la existencia de un Servicio Electrónico (costos, eficiencias operativas, mayor acceso a servicios financieros por parte de los clientes potenciales o existentes, mejoras en la valuación de la Entidad, acceso a nuevos financiamientos o apoyos gubernamentales o internacionales).

(b) Identificar los servicios o procesos donde la Entidad utiliza el efectivo de manera preponderante. Para ello será necesario contar con el punto de vista y la evaluación realizada por las diversas áreas de la Entidad. Para ello será necesario (a) hacer un listado de los procesos que involucran efectivo en la Entidad, (b) crear diagramas de flujo de cada uno de los procesos que involucran efectivo, (c) documentar los valores, volúmenes, frecuencia, tipo y valores relacionadas con pagos dentro de esos procesos, (d) identificar los puntos de cada proceso donde se realiza la administración del dinero, y (e) identificar barreras e ineficiencias.

(c) Realizar un estudio de costo-beneficio: revisar los costos financieros y transaccionales de los Servicios Electrónicos e identificar ventajas de realizar procesos en línea en lugar de realizarlos físicamente, etc.

(d) Estudio de mercado: México cuenta con una oferta de servicios financieros importante, no sólo por parte de instituciones de banca múltiple, sino también por las entidades Fintech. Es necesario establecer el mercado potencial, requerimientos de los clientes actuales o potenciales e indagar sobre fuentes públicas sobre el estado de los servicios financieros en México. Este estudio debe responder a estas preguntas:

- ¿Qué prestadores de servicios será necesario contratar? ¿Qué servicios requerimos en específico para cierto tipo de Servicio Electrónico? ¿Dónde prestan los servicios?
- ¿Qué necesitan los clientes? ¿Usan otros servicios electrónicos? ¿Qué esperarían de un Servicio Electrónico?
- Delinear los retos regulatorios y normativos: límites para cada Servicio Electrónico.

(e) Desde el punto de vista legal, la definición del Proyecto debe considerar para su implementación los requerimientos legales mínimos e indispensables que se deben satisfacer para cumplir con la normatividad aplicable.[61]

B. Planificación del Proyecto.

(a) Hacer una proyección del Servicio Electrónico que contenga, por lo menos:

- Descripción del Servicio Electrónico.
- Mercado objetivo: descripción detallada del cliente final y del alcance geográfico que tendrá el Servicio Electrónico.
- Estudio de mercado: análisis de competencia
- Análisis de tecnologías necesarias para la implementación.
- Evaluación de los riesgos, con base en lo establecido en el Manual de Riesgos de la Entidad o, en su caso, identificación de nuevos riesgos.

(b) Asegurarse que el Proyecto cuenta con la autorización e involucramiento del Consejo de Administración y el Director General para asegurar su compromiso con el desarrollo del proyecto.

(c) Con el apoyo de un asesor legal calificado realizar el siguiente diagnóstico del Servicio Electrónico:

[61] LACP, LRASCAP, Disposiciones Generales SOFIPO y Disposiciones Generales SOCAP

- Necesidad de actualizar o redactar un Contrato de Adhesión para el nuevo Servicio Electrónico.
- Análisis de las comisiones, intereses o demás contraprestación y su adecuación a las LTSOF y a las disposiciones de transparencia emitidas por Condusef.
- Determinación de la necesidad de cálculo de CAT o GAT.
- Análisis de los servicios de Proveedores Relevantes.

(d) El área o encargado de finanzas en el interior de la Entidad deberá realizar un diagnóstico de (i) los costos que estarán asociados al Proyecto y (ii) los ajustes a los procesos financieros que requerirá realizar la Entidad.

(e) El Director General deberá designar a la Partes Responsables y señalar las responsabilidades que tendrá cada una en el desarrollo del Proyecto.

(f) Establecer a la persona que fungirá como Administrador del Proyecto para efecto de que prepare el plan de trabajo.

(g) Con el fin de seleccionar a un proveedor, luego de que se ha determinado la necesidad de uno, es necesario conjuntar tanto al equipo tecnológico, operativo y legal para revisar:

- Alcance de los servicios en relación con los procesos que se desea cubrir, es decir, con cada uno de los procesos que se han identificado como necesarios para el Proyecto.
- Solicitar y requerir una demostración del programa: establecer una sesión en donde se muestren las funcionalidades del programa a ser contratado.
- Identificar las tecnologías que serán relevantes para la implementación del Servicio y establecer (i) capacidades internas y (ii) necesidad de proveedores externos.
- Ponderar con ayuda del Oficial de Cumplimiento, y con base en lo expuesto anteriormente, la viabilidad de realizar el proceso de firma e identificación de los Clientes de manera remota y las limitaciones que, en su caso, tendría dicha opción (para temas de firma electrónica favor de referirse a la Sección 12 de la presente Guía Legal).

- Confirmar la necesidad de realizar procesos de cobranza adicionales a los establecidos previamente por la Entidad y, en su caso, diseñar la estrategia de cobranza con base en las reglas secundarias emitidas por Condusef.
- Preparar los convenios de confidencialidad que deberán firmar las Partes Responsables, así como los asesores externos y posibles proveedores.
- Verificar los requisitos para la contratación de proveedores relevantes (ver Sección 15 de la presente Guía Legal).
- Establecer las notificaciones que, en su caso, sería necesario presentar a CNBV, en relación con los proveedores relevantes (ver Sección 15).

(h) Diagramas y Presentación del Proyecto: El Administrador del Proyecto deberá coordinar la preparación de una presentación guía con los siguientes elementos del Proyecto: (a) nombre provisional del servicio, (b) mapeo de procesos de efectivo, (c) mapeo de los nuevos procesos sin efectivo a través de los Servicios Electrónicos, (d) identificación de las áreas involucradas, (e) revisión de los Manuales que serán objeto de modificación, (f) identificación de proveedores relevantes y supuestos de regulación de cada uno de ellos (ver Sección 15 del presente Manual), (g) montos y límites de cada servicio, y (h) resumen de proyección financiera y evaluación preliminar de riesgos.

(i) Con base en el mapeo de procesos de efectivo realizado en la etapa anterior, crear un mapa de procesos que muestre cómo se verían dichos procedimientos una vez implementado el Servicio Electrónico. Con esa información se deberá:

- Analizar los cambios potenciales o actuales a los Manuales y políticas de la Entidad.
- Establecer las áreas que tendrían que participar en el Proyecto.
- Analizar las tecnologías y proyectos

(j) Establecer contacto con CNBV para exponer de manera detallada la Presentación de Proyecto, donde se muestren los alcances del nuevo Servicio Electrónico propuesto, de modo que exista (i) una notificación informal pero efectiva a dicho Regulador sobre el nuevo Proyecto, y (ii) revisar el cumplimiento de los requisitos regulatorios previamente identificados.

(k) Preparar las autorizaciones corporativas necesarias: para este efecto será necesario recabar y proveer al Consejo de Administración (o en su caso a la asamblea de accionistas) de todos los elementos necesarios para tomar una decisión. A ellos iría dirigida la Presentación de Proyecto mencionada en el inciso (h) anterior.

(l) Realizar una prueba de concepto del Servicio Electrónico para efecto de que toda la Entidad se familiarice con el mismo. Sugerimos realizarlo siguiendo las siguientes recomendaciones:

- Seleccionar a las personas que estarán involucradas en la prueba de concepto.
- Ampliar la prueba de concepto cuando haya pasado una primera fase con el grupo inicial.
- Realizar formatos de entrevista a los participantes con el objetivo de conocer su punto de vista sobre el potencial Servicio Electrónico.
- Establecer con el asesor legal la posibilidad de realizar dicha prueba con un número limitado de personas no pertenecientes a la Entidad y, en su caso, los requerimientos en materia de transparencia y protección de Datos Personales.

(m) Negociación y preparación de los contratos a celebrarse con los proveedores relevantes incluyendo el clausulado mínimo requerido por la normatividad, así como preparación de la notificación o autorización respectiva ante CNBV, en caso de ser necesario (ver Sección 15).

(n) Realizar la presentación de las notificaciones o autorizaciones que sean necesarias ante CNBV para efecto de autorizar a los proveedores relevantes.

(o) Verificar o fortalecer políticas antifraude que, además de incluir los elementos de seguridad aplicables a dichos Proyectos, deberá considerar la posibilidad de contratar a un Proveedor Relevante en la materia que tenga experiencia en ello.

C. Entrega del Proyecto

(a) Preparar una carpeta de cierre con la documentación relevante para efecto de que sea archivada y debidamente conservada por la Entidad.

(b) El Administrador del Proyecto, junto con las áreas responsables del mismo, deberá negociar y celebrar el contacto con los proveedores relevantes, el en cual se deben estipular los tiempos de entrega e implementación correspondientes.

(c) Someter a consideración del Consejo de Administración el cierre del Proyecto para su aprobación junto con los Manuales y procesos que será necesario modificar o crear para finalizar la implementación del Proyecto.

(d) Establecer un plan de publicidad para dar a conocer a los clientes o posibles Clientes el nuevo Servicio Electrónico, los beneficios, requisitos de contratación y demás temas relacionados con este proceso. Un profesional del derecho deberá realizar la validación de (i) información publicitaria a ser ofrecida en la página de Internet de la Entidad (por ejemplo, incluyendo el CAT y el GAT, según corresponda) y (ii) asegurarse de que los registros correspondientes ante Condusef se realicen de manera adecuada previo al lanzamiento del producto, incluyendo sin limitar Contrato de Adhesión, comisiones (ver Sección 5).

(e) Revisión de los Avisos de Privacidad de la Entidad para asegurarse de que los procesos de identificación, recolección o tratamiento de Datos Personales sean acordes con el nuevo Servicio Electrónico.

(f) Realizar una serie de validaciones finales por parte de las siguientes áreas:

- Auditoría Interna: temas relacionados con seguridad de la información, registros y control interno y demás procesos de su competencia.
- Oficial de Cumplimiento: cambios en el Manual de Cumplimiento, verificación de envío de Manual de Cumplimiento a CNBV y cambios en el plan de capacitación anual respecto a los nuevos temas planteados por el Servicio Electrónico.

(g) Implementación de acuerdos sobre el tratamiento de Datos Personales por parte de proveedores de servicios relevantes que actúen como Encargados para estos efectos.

D. Cierre del Proyecto.

(a) Aprobación por parte del Consejo de Administración del cierre del Proyecto, incluyendo las modificaciones a los Manuales relacionados con el nuevo Servicio Electrónico.

(b) Establecimiento por parte de la Dirección General de procesos de capacitación y apoyo del personal a cargo de operar el nuevo Servicio Electrónico por parte de proveedores, en su caso.

(c) Registro del Contrato de Adhesión en el RECA.

(d) Registrar de comisiones relacionadas con el nuevo Servicio Electrónico en el RECO.

(e) Realizar la publicación del CAT o GAT, según corresponda, realizando el cálculo conforme a las disposiciones emitidas por Banxico[62].

(f) Capacitar al personal a cargo del manejo de atención a clientes, incluyendo al titular de la Unidad Especializada de Atención a Usuarios ("UNE").

(g) Entregar notificaciones a CNBV en relación con (i) modificación de los Manuales que correspondan, en su caso, y (ii) aspectos relacionados con proveedores, según corresponda (ver Sección 15).

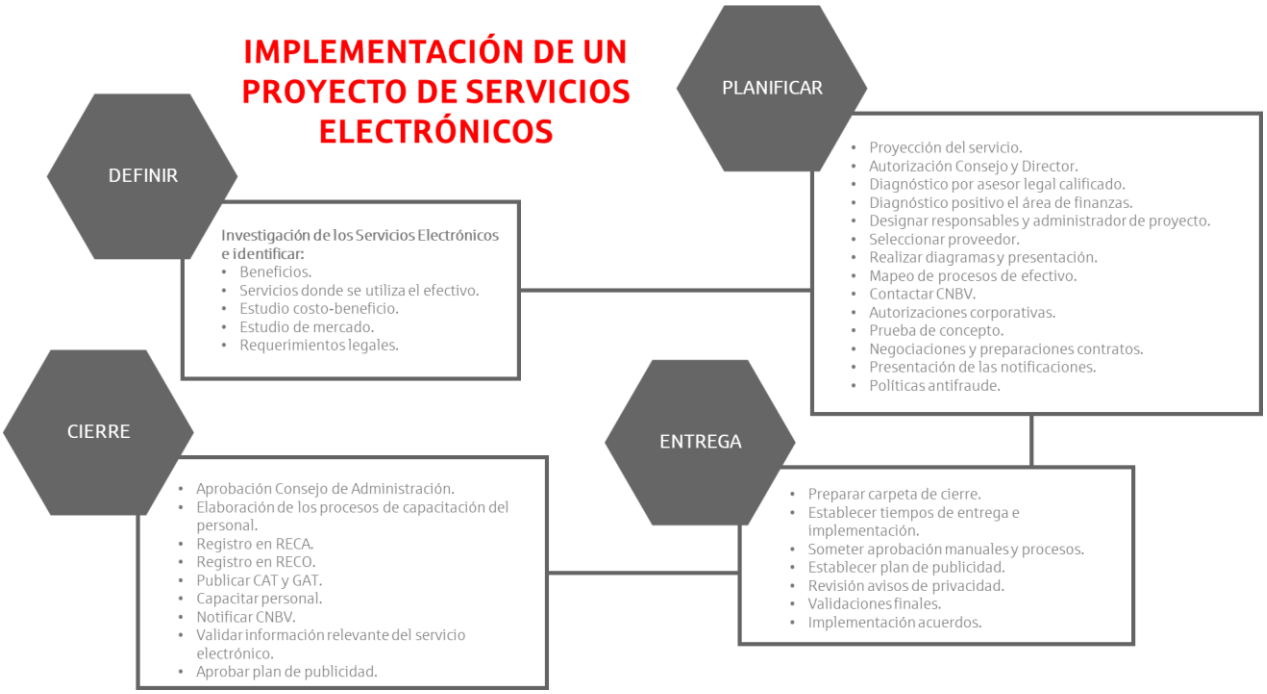
(h) Validar la información relevante del Servicio Electrónico que será subida a la página de Internet de la Entidad, así como en la publicidad que será utilizada atendiendo a los parámetros emitidos por Condusef en materia de transparencia (ver Sección 5 de la presente Guía].

(i) Aprobar un plan de publicidad y difusión del nuevo Servicio Electrónico con el apoyo del asesor legal que permita a los clientes actuales o potenciales: (i) entender de manera detallada la manera de realizar la contratación y los requisitos necesarios para ello, (ii) generar tutoriales y materiales de ayuda y publicitarios que permitan realizar dicha contratación y contesten las siguientes preguntas que ellos se harían:

[62] Circular 21/2009 y Circular 35/2010

¿En qué consiste el nuevo Servicio Electrónico? ¿Cómo se usa y para qué sirve el Servicio Electrónico? ¿Cómo puedo acceder a mi cuenta? ¿Cómo dispongo de mi dinero? ¿Qué medidas de seguridad existen?

(j) Puesta en marcha de un programa de capacitación que permita a todas las áreas identificadas como relevantes para el nuevo Servicio Electrónico familiarizarse con los procesos que serán de su responsabilidad, así como con el software que, en su caso, deban operar.



Gráfica 8. Implementación de un proyecto de servicios electrónicos. Fuente: Vite Abogados

10.7 Aspectos Prácticos.

Para una implementación exitosa de Banca Electrónica se recomienda[63]:

- El cliente final debe estar al centro del diseño de la estrategia de Servicios Electrónicos. Las necesidades, perfiles demográficos, características socioeconómicas y el contexto en que opera cada Entidad, son esenciales para un diseño adecuado.
- Establecer como parte del Proyecto o en adición al mismo, un plan de comunicación hacia el interior de la Entidad para efecto de (i) adaptar a los directivos relevantes a la nueva cultura orientada a medios ópticos y electrónicos, y (ii) establecer planes de capacitación para el equipo de la Entidad que manejará todos los procesos del nuevo servicio.
- La administración de riesgos debe adaptarse y reflejar la nueva realidad de los Servicios Electrónicos. Deben identificarse los nuevos riesgos legales, financieros, operacionales y tecnológicos y contar con un plan de mitigación en caso de materializarse.
- Mantener en mente que los clientes comenzarán a generar cierta (y nueva) cantidad y calidad de datos que puede aportar mucho a los objetivos de las Entidades. El tratamiento y análisis de esa información requiere de la adaptación de temas técnicos y legales (ver Sección 9 relacionada con Datos Personales).
- Buscar a otras Entidades u organizaciones que hayan transitado hacia entornos digitales para obtener su punto de vista y aprender de sus procesos.
- No perder de vista los aspectos relacionados con prevención de fraudes: si bien hay un estándar mínimo en la regulación sobre seguridad de transacciones (ver Sección 7), es necesario buscar asesoría de un Proveedor Relevante que permita prever estos supuestos.

[63] MAROUS, Jim. 10 ways to improve the Digital Banking Experience (Internet). Consultado en: https://thefinancialbrand.com/62845/digital-banking-experience-strategy-online-mobile/

10.8 Diferencias relevantes entre la regulación de las Entidades.

A pesar de que la regulación para las SOCAP y las SOFIPO es similar en materia de banca electrónica, existen algunas diferencias que vale la pena tomar en cuenta al momento de implementar un Proyecto de esta naturaleza. A continuación, listamos algunas de las diferencias que consideramos más relevantes respecto a la regulación secundaria de las entidades mencionadas:

- Las SOCAP deben obtener el consentimiento expreso mediante firma autógrafa de sus usuarios, o bien, mediante Firma Electrónica Avanzada para todos aquellos servicios avanzados móviles, servicios por internet, servicios telefónicos audio respuesta y servicio telefónico voz a voz, así como servicios ofrecidos a través de cajeros automáticos y terminales punto de venta cuando estén asociados a cuentas de bajo riesgo. Adicionalmente, tanto las SOFIPO como las SOCAP deben solicitar el consentimiento mencionado para (i) servicios de pago móvil y (ii) servicios ofrecidos a través de cajeros automáticos y terminales punto de venta cuando sean utilizados para realizar operaciones monetarias de mediana cuantía.
- Las SOCAP cuenta con reglas adicionales en caso de que la información sensible del usuario sea extraída, extraviada o en caso de que las SOCAP supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán enviar por escrito a la CNBV y al Comité de Supervisión Auxiliar, dentro de los cinco días siguientes al evento de que se trate, la información contenida en el anexo correspondiente. Adicionalmente, la SOCAP deberá llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, en cuyo caso deberán notificar esta situación, en los siguientes tres días hábiles, a sus usuarios afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deben tomar. La SOCAP deberá enviar el resultado de la investigación en un plazo no mayor a cinco días naturales posteriores a que concluya.

KZ: un caso de éxito.

La innovación en los servicios financieros, como reflejo de lo que pasaba en el mundo, dio pasos muy importantes en México en los últimos años. Muchas personas, sin contar con licencia o registro ante los Reguladores (porque no era preciso ya que estaban en un área gris y decidieron afrontar el riesgo legal), decidieron implementar esquemas de pagos y de servicios que facilitaran la vida de muchos consumidores. Una de esas compañías, que llamaremos "KaufZahl" o "KZ" por motivos de confidencialidad, fue uno de dichos ejemplos.

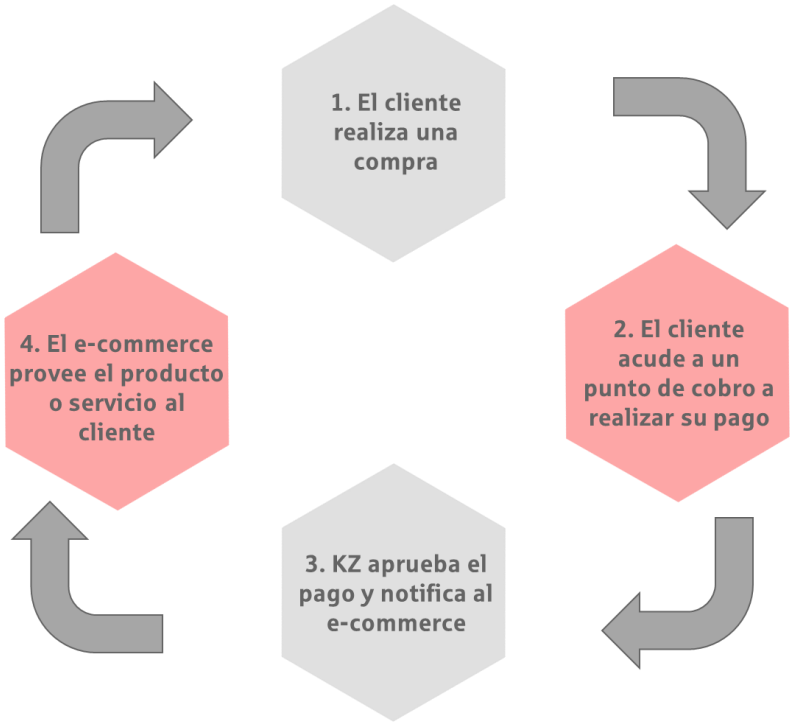
KZ fue fundada en el 2013 con el objetivo de acercar el comercio electrónico a aquellas personas sin acceso a una cuenta bancaria: KZ comenzó a operar como procesador de pagos en línea enfocado en el efectivo. De la mano de una inversión importante comenzó formalmente sus operaciones en la Ciudad de México en el 2014. Posteriormente, levantó más capital y para el ejercicio de 2018 procesaba alrededor de 250 mil transacciones con un monto promedio de 800 pesos.

El objeto de los servicios de KZ era actuar como intermediario entre comercios en Internet, recibiendo y enviando recursos, y almacenando un saldo a los comercios en cuentas electrónicas, algo que, actualmente, en el marco de la Ley Fintech corresponde a los "fondos de pago electrónico".

El funcionamiento era relativamente sencillo:

1. El cliente realizaba una compra en un comercio electrónico.
2. Acudía a un punto de cobro a realizar su pago (por ejemplo, una tienda de conveniencia, farmacias, tiendas gubernamentales) o realizarlo mediante transferencia.
3. KZ verificaba y aprobaba el pago.
4. El comercio prestaba el servicio o entregaba el producto

Diagrama de funcionamiento de “KZ”



Gráfica 9. Diagrama de funcionamiento de “KZ”. Fuente: Vite Abogados

La intermediación del dinero se hacía mediante una cuenta concentradora, no por medio de cuentas individualizadas.

KZ ofrecía diferentes herramientas, mismas que podían integrar los comercios a sus plataformas que iban desde: la inclusión en el sitio web de un botón de pago, hasta la integración personalizada, en distintas aplicaciones, dependiendo de las necesidades de los comercios y los conocimientos técnicos con los que contaban.

Tipos de Herramientas de Integración		
Herramienta	Descripción	Conocimientos Técnicos
Sitio web, blog o Facebook.	Adición de un botón de pago en el portal de internet o compartible en Facebook.	Copiar y pegar el botón de pago.
Comercio Electrónico.	Instalación de un *plugin* de KZ para soluciones como Magento o WooCommerce.	Habilidades para instalar un *plugin*.
Integración Personalizada.	Integración de una API.	Habilidades avanzadas de programación.

Tabla 3. Tipos de Herramientas de Integración

De manera específica, las operaciones que permitían realizar cada una de las herramientas son las siguientes:

(a) Botón KZ. Icono que brindaba la opción de recibir pagos en efectivo en el portal de internet:

- No se requería contar con niveles avanzados de programación.
- Sólo se necesitaba "copiar" un enlace de pago presionando la tecla CTRL + C y posteriormente presionar las teclas CTRL + V para "pegar" dicho enlace en el sitio que se desee.
- KZ se responsabilizaba por la seguridad de la información.
- Los clientes de los comercios no requerían registrarse para poder pagar algún producto de una tienda en línea.

(b) *Plugins*[64]. Se utilizaron *plugins* que cuentan con alta demanda dentro del comercio electrónico, tales como: Magento, WooComerce, Open Cart, WHMCS.

(c) Integración con terceros. Permitían la integración de los *plugins* más demandados en plataformas de comercio electrónico.

(d) API y librerías. Son aplicaciones cuya función consiste en compartir información de otros sitios de internet y que permiten una rápida integración.

(e) Terminal. Una terminal de KZ consistía en la inserción de una interfaz que permitía generar órdenes de ventas telefónicas, ajustar las propiedades de las órdenes de pago conforme a las necesidades de cada cliente y permitía incorporar la terminal desde cualquier dispositivo móvil.

Los servicios de KZ consistían en plataforma tecnológica o aplicación las cuales estarán disponibles en los siguientes dispositivos:

- Computadora.
- Tablets.
- Teléfonos inteligentes.

Los participantes en la operación de los servicios y algunas empresas con las cuales existen acuerdos son las siguientes:

- Bancos.
- Tiendas online.
- Tiendas de conveniencia
- Tiendas departamentales
- Farmacias.

Si bien las actividades descritas están en línea con un enfoque más parecido al de un Agregador y a una Institución de Fondos de Pago Electrónico ("IFPE"), este ejemplo de innovación con un entorno normativo, que en ese entonces no era claro, deja varias lecciones para el SACP:

[64] Un plugin es una aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software.

- Las Entidades cuentan con ventajas comparativas respecto a otras entidades financieras pues, conforme a lo que establece la ley, pueden realizar operaciones de captación y transmisión de dinero.
- En el ejemplo de KZ, la operación de cuentas si bien es a través de un tercero, que era el banco que guardaba los fondos en una cuenta concentradora, el valor agregado vino de satisfacer una necesidad mediante el uso de tecnologías accesibles. En ese sentido, el acceso a SPEI es un tema importante que trataremos en la Sección 19 (Sistema de Pagos) del presente documento.
- La normatividad puede jugar a dos bandas: por un lado, establece estándares de aplicación bajo la cuales siempre tienen que operar las Entidades (tal como se expuso en esta sección) y, por la otra, la misma otorga certeza y estabilidad a cualquier plan de negocios a largo plazo de una Entidad.

El uso de tecnologías que permiten una contratación rápida, aunque se encuentran sujetos a los parámetros en materia de PLD/FT (Sección 6 Prevención de Lavado de Dinero y Financiamiento al Terrorismo), control interno (Sección 4 Control Interno y Manuales) y demás límites y requisitos establecidos en la regulación, y brevemente reseñados anteriormente, es una herramienta que puede hacer que la oferta de las Entidades se realice de manera amplia en un área geográfica que puede abarcar incluso toda la República Mexicana.

SECCIÓN 11.- PROCESO CREDITICIO.

Una de las actividades básicas que pueden desarrollar las Entidades, es el otorgamiento de crédito, en cualquiera de sus modalidades. Dicha actividad se describe en el Código Civil bajo la figura del "mutuo" o "préstamo civil", que implica la obligación del mutuante (acreedor) de transferir la propiedad de dinero o de otras cosas fungibles al mutuario (acreditado), quien se obliga a devolver otro tanto de la misma especie y calidad. Por su parte, las leyes mercantiles son más precisas y definen a la operación de "apertura de crédito" como aquel en la cual el acreditante se obliga a poner una suma de dinero a disposición del acreditado, o a contraer por cuenta de éste una obligación, para que el mismo haga uso del crédito concedido en la forma y en los términos y condiciones convenidos, quedando obligado el acreditado a restituir al acreditante las sumas de que disponga, o a cubrirlo oportunamente por el importe de la obligación que contrajo, y, en todo caso, a pagarle los intereses, prestaciones, gastos y comisiones que se estipulen.

En el caso de las Entidades, existen ciertas restricciones a los términos y condiciones de los créditos dependiendo de su nivel de operaciones. Por ejemplo, las Cajas de Ahorro con Nivel de Operaciones I, podrán otorgar a sus Socios créditos con un plazo máximo de sesenta meses.

11.1 Digitalización del Proceso Crediticio.

Disponibilidad de la Información Crediticia.

Como parte del Sistema de Control Interno de la Entidad los sistemas de información dentro de la Entidad deben permitir que la información sobre el estado en que se encuentren los créditos sea completa y oportuna y disponible para el Comité de Supervisión Auxiliar, la CNBV, así como para el personal que se considere autorizado para acceder a dicha información.

11.2 Proceso Crediticio.

El proceso de crédito de las Entidades, es decir, los pasos que deben seguir y las reglas que deben aplicar para efecto de generar, administrar, contratar y realizar la cobranza de su cartera crediticia, se encuentra establecido en la regulación secundaria y depende, en alguna medida, de su Nivel de Operaciones.

Plazos

Los créditos en moneda nacional o UDI que las Cajas de Ahorro otorguen deben sujetarse a las siguientes características:

Plazo de Créditos	
Nivel de Operaciones	Plazo Máximo
Nivel I	Hasta 60 meses, siempre y cuando en las condiciones del contrato se pacten pagos periódicos de capital e intereses.
Nivel II	Hasta 96 meses, siempre y cuando en las condiciones del contrato se pacten pagos periódicos de capital e intereses.
Nivel III y IV	Superior a los 96 meses[65], sin embargo, no pueden superar los 30 años

Tabla 4. Plazos de Crédito

En el caso de que los préstamos o créditos que otorguen las SOCAP se pacten a pago único de principal al vencimiento, el plazo máximo será de hasta dieciocho meses y solo en aquellos casos que el destino del crédito sea para una actividad en la que se espere un flujo de recursos en dicho plazo.

[65] A pesar de que las Disposiciones Generales SOCAP indican que las Entidades con nivel de operación III y IV podrán otorgar créditos superiores a 60 meses, asumimos que, dado que las entidades con nivel II de operación pueden otorgar créditos hasta por 96 meses, las entidades con niveles III y IV podrán otorgarlos por un plazo superior a este último.

Por lo que respecta a las SOFIPO, los plazos de sus créditos deben someterse a las siguientes reglas:

Plazo de Créditos	
Nivel de Operaciones	Plazo Máximo
Nivel I	Hasta 60 meses, siempre y cuando en siempre y cuando al momento de su otorgamiento el monto total de dichos créditos, no excedan del 20% de su cartera crediticia.
Nivel II	Hasta 96 meses, siempre y cuando al momento de su otorgamiento el monto total de dichos créditos, no excedan del 20% de su cartera crediticia.
Nivel III y Nivel IV	Superior a 96 meses.

Tabla 5. Plazo de Créditos

Las SOFIPO podrán otorgar préstamos o créditos a sus Clientes, a plazos superiores a los señalados, cuando los préstamos o créditos se otorguen con recursos provenientes de instituciones de crédito, instituciones integrantes de la administración pública y fideicomisos públicos, constituidos por el Gobierno Federal o estatales para el fomento económico, que realicen actividades financieras, siempre que dichas instituciones y fideicomisos se constituyan como titulares o cotitulares de los respectivos derechos de crédito y asuman total o parcialmente el riesgo de incumplimiento en el pago, en cuyo caso, los plazos se ajustarán a las políticas y lineamientos que, al efecto, establezcan las instituciones de banca de desarrollo o fideicomisos de que se trate.

En ningún caso las SOFIPO podrán dar créditos por plazos superiores a los treinta años.

Adicionalmente, las Entidades deberán ajustarse a los límites máximos de plazo y monto del crédito o préstamo que al efecto determine el Consejo de Administración conforme a lo establecido en la normatividad aplicable.

Tasas de interés.

De acuerdo con lo dispuesto por el artículo 13, fracción I, inciso b) de las Disposiciones Generales SOCAP, las Cajas de Ahorro pueden convenir con sus Socios la tasa de interés que pretendan cobrar por los préstamos o créditos, debiendo pactar una sola tasa de interés ordinaria y, en su caso, una sola tasa de interés moratoria. Asimismo, pueden dividir en dos o más períodos el plazo de vigencia de los préstamos o créditos y establecer desde el momento del inicio de la vigencia del préstamo o crédito respectivo la tasa de interés aplicable a cada uno de los períodos, los cuales no deben ser menores a 3 años.

La tasa de interés deberá determinarse conforme a alguna de las tres opciones siguientes:

- Una tasa fija.
- Una tasa variable, la cual podrá ser determinada bajo cualquier fórmula acordada con el Socio, siempre y cuando esta use como referencia una sola tasa que se elija de entre las tasas de referencia señaladas más adelante.
- Una tasa variable con un límite máximo fijo.

Las tasas de interés pactadas se deberán calcular sobre saldos insolutos y sólo podrán cobrarse por anticipado en los supuestos que determine Banxico.

Tratándose de aperturas de líneas de crédito en las que las Entidades no hayan renunciado al derecho de denunciarlas en cualquier tiempo, las partes podrán pactar que la tasa de interés aplicable se fijará en el momento en que se efectúe cada una de las disposiciones respectivas. Lo anterior debe ser acordado por las partes en el instrumento que documente el crédito.

Modificación de la tasa de interés.

De acuerdo con lo dispuesto por el artículo 13, fracción I, inciso c) de las Disposiciones Generales SOCAP, las Cajas de Ahorro no pueden modificar unilateralmente la tasa de

interés a la alza o los mecanismos para determinarla, durante la vigencia del préstamo o crédito de que se trate, salvo por créditos otorgados a sus empleados donde la misma puede modificarse en caso de que deje de existir una relación laboral donde, para que surta efecto esta excepción, debe pactarse de antemano el incremento aplicable a la tasa de interés. Esto sin perjuicio de que se modifiquen de mutuo acuerdo los términos del crédito, dejando constancia por medios escritos o "cualquier medio que deje constancia de ello".

Tratándose de contratos de apertura de crédito en cuenta corriente[66] en moneda nacional, las Entidades, a través de los medios que pacten con sus Socios, deberán darles a conocer las modificaciones a las tasas de interés, por lo menos con treinta días naturales de anticipación a la fecha prevista para que dichas modificaciones surtan efectos. En ese supuesto los Socios dentro de los sesenta días naturales siguientes a que surtan efectos las modificaciones, tendrán derecho a dar por terminado el contrato en caso de no estar de acuerdo con ellas, sin que la Entidad pueda cobrarle cantidad adicional alguna por este hecho, con excepción de los adeudos ya generados a la fecha de terminación.

Tasa aplicable y periodo de cómputo de intereses.

Las tasas de interés ordinarias y moratorias deberán expresarse exclusivamente en términos anuales simples, considerando años de 360 días.

En el supuesto de que se pacte una tasa de referencia, también deberá pactarse que dicha tasa de referencia deberá ser la última publicada durante el período que se acuerde para la determinación de dicha tasa de interés, o la que resulte del promedio aritmético de dichas tasas, publicadas durante el referido período.

Tasas de referencia en moneda nacional.

En los préstamos o créditos denominados en moneda nacional, únicamente se podrá utilizar como tasa de referencia: (i) la TIIE; (ii) CETES; (iii) el CCP; (iv) la Tasa Nafin (TNF) que se publique en el Diario Oficial de la Federación; (v) la tasa que se hubiese pactado en los

[66] La apertura de crédito en cuenta corriente da derecho al acreditado a hacer remesas, antes de la fecha fijada para la liquidación, en reembolso parcial o total de las disposiciones que previamente hubiere hecho, quedando facultado, mientras el contrato no concluya, para disponer en la forma pactada del saldo que resulte a su favor.

instrumentos que documenten préstamos o créditos de la banca de desarrollo o de fideicomisos públicos de fomento económico, solamente en los préstamos o créditos que sean objeto de descuento con tales instituciones de banca de desarrollo o de esos fideicomisos, o que sean otorgados con recursos provenientes de dichas instituciones o fideicomisos; (vi) la tasa ponderada de fondeo bancario o (vii) la tasa ponderada de fondeo gubernamental. Estas dos últimas tasas serán las que el Banco de México dé a conocer en su página de Internet.

En los préstamos o créditos denominados en UDIS, únicamente podrá utilizarse como referencia la tasa de rendimiento en colocación primaria de UDIBONOS.

Cuando se acuerde una tasa de referencia, deberá pactarse una o más tasas de referencia sustitutivas en el evento de que deje de existir la tasa de referencia originalmente pactada, debiendo convenir el orden en que, en su caso, dichas tasas de referencia sustituirían, de ser necesario, a la original.

Garantías.

Tratándose de SOCAP con nivel de operaciones I, únicamente podrán otorgar créditos o préstamos revolventes, siempre y cuando dichas operaciones estén cubiertas en su totalidad por garantías líquidas que cumplan con lo que se establece en la regulación. Esta disposición no es aplicable para las SOFIPO.

11.3 Manual de Crédito.

En el Manual de Crédito se establecen los límites respecto al otorgamiento de préstamos o créditos, incluyendo el crédito neto que pueda otorgar cada Entidad y la proporción de la cartera otorgada a un solo pago de capital; así como el tipo de acreditados y de productos crediticios que ofrecerá la Entidad.

De acuerdo con lo dispuesto por el artículo 32, fracción I de las Disposiciones Generales SOCAP, corresponde al Consejo de Administración de las Cajas de Ahorro aprobar el Manual de Crédito y aprobar la revisión de este cada dos años.

El Manual de Crédito es el documento que contiene las políticas y los procedimientos de crédito de la Entidad, y como mínimo, los lineamientos siguientes para el caso de las Cajas de Ahorro con Nivel I de Operaciones[67]:

(a) Promoción y otorgamiento de crédito.

(b) Las Entidades deberán establecer dentro del manual de crédito, metodologías para la evaluación, aprobación y otorgamiento de los distintos tipos de crédito, debiendo observar en todo caso, según corresponda, lo siguiente:

1. Ningún crédito podrá pasar a la etapa de análisis y evaluación, sin que se cuente con la información y documentación mínima que se haya establecido en el Manual de Crédito y en la regulación.
2. La evaluación deberá considerar cuando menos:
   - **(i)** En su caso, la información que valide la experiencia de ahorro del acreditado.
   - **(ii)** La experiencia de pago del acreditado, revisando para tal efecto información cuya antigüedad no sea mayor a un mes, obtenida a través de una consulta realizada a alguna Entidad de Información Crediticia, así como la información con la que cuente la propia Entidad.
   - **(iii)** La capacidad de pago a través de los ingresos estimados del probable acreditado, de la relación entre el ingreso del posible deudor y el pago de la obligación y la relación entre el plazo de los créditos y la capacidad de generar recursos; así como del análisis de la totalidad de otros créditos y demás pasivos que el posible deudor tenga con la Entidad y otras entidades financieras.
3. El plazo de los créditos se deberá establecer en función de los plazos de los recursos captados.
4. Cualquier cambio significativo a los términos y condiciones que hubieren sido pactados en un crédito, será motivo de una nueva evaluación y aprobación, debiéndose seguir al efecto, los procedimientos del Manual de Crédito.

[67] Dependiendo del nivel de operaciones que tenga la Entidad el Manual de Crédito y los demás manuales tendrán requisitos adicionales, por lo que será necesario consultar las Disposiciones aplicables para atenderlos.

(c) Integración de expedientes de crédito: Las políticas y procedimientos para la integración de un expediente único por cada acreditado, en el cual se contenga en todo momento cuando menos la documentación e información siguiente:

1. Identificación del solicitante.
2. La solicitud de crédito debidamente requisitada y, en su caso, copia del acta del Consejo de Administración o del Comité de Crédito en la que conste su aprobación, según corresponda.
3. Documentación que acredite su capacidad de pago.
4. Copia de los contratos y títulos de crédito con los que se haya documentado el crédito. Los contratos y demás instrumentos jurídicos que documenten las operaciones deberán ser aprobados por el área jurídica o un responsable designado por el Director o Gerente General.
5. La documentación que acredite haber formulado ante una Entidad de Información Crediticia una consulta previa sobre la información sobre el historial del acreditado.
6. En su caso, correspondencia con el acreditado, como cartas, telegramas, correos electrónicos y otros relacionados con modificaciones a los términos y condiciones del crédito otorgado.
7. Comprobante de domicilio.
8. Garantías. Documentación que deba recabarse con el fin de evidenciar la existencia de garantías a favor de la Entidad por el crédito otorgado, e información relativa a la guarda, custodia y seguimiento que se dé respecto de las mismas.

Asimismo, en el Manual de Crédito deberá preverse quién es el personal responsable de integrar y actualizar los expedientes, así como de controlar el servicio de consulta de los mismos.

La documentación e información contenida en los expedientes podrá conservarse en forma física, electrónica o microfilmada, siempre y cuando se encuentren disponibles en todo momento para su consulta

(d) Evaluación y Seguimiento: La metodología para evaluar y dar seguimiento a cada uno de los créditos de su cartera, la cual deberá ser definida por el Comité de Crédito.

(e) Recuperación de cartera crediticia.

Igualmente, el manual de crédito deberá contener una sección específica de las políticas y procedimientos para la gestión y otorgamiento de Microcréditos Productivos[68], los cuales están sujetos a reglas específicas.

Autorizaciones Automáticas

Las Cajas de Ahorro pueden establecer en el Manual de Crédito procesos de autorizaciones automáticas de créditos que permitan otorgar el crédito correspondiente a cualquier Socio. Dichos procesos, por ejemplo, para el caso de SOCAP con Nivel I de Operación[69], deberán comprender lo siguiente:

(i) El establecimiento de la documentación mínima a ser entregada por tipo de crédito.

(ii) Las características de los depósitos que el Socio deberá mantener en la Entidad.

(iii) El monto máximo a otorgar según el resultado de la información entregada.

(iv) El establecimiento de las tasas de interés conforme a sus políticas.

Las autorizaciones automáticas se podrán otorgar respecto de créditos para un mismo Socio, incluyendo a sus dependientes económicos, cuyo importe en lo individual o en su conjunto, no sea mayor a 10,000 UDIS.

En el caso de las SOFIPO, las autorizaciones automáticas para otorgar créditos estarán limitadas a 5,000 UDIS para un mismo cliente, incluyendo a sus dependientes económicos.

Vigilancia del Proceso Crediticio

Conforme a la normatividad vigente y dependiendo de su Nivel de Operaciones siguientes partes se encuentra involucradas en el proceso crediticio de las Cajas de Ahorro:

[68] Son los créditos otorgados por las Sociedades a sus Socios o a grupos de Socios, destinados a financiar la actividad productiva de los acreditados y cuya fuente de pago la constituyan los flujos originados por la propia actividad productiva.

[69] Dependiendo del nivel de operaciones que tenga la Entidad el Manual de Crédito y los demás manuales tendrán requisitos adicionales, por lo que será necesario consultar las Disposiciones aplicables para atenderlos.

Consejo de Administración	Aprobación y revisión del Manual de Crédito y establecimiento de límites de riesgo crediticio, entre otras.
Comité de Auditoría	Asegurarse de que se lleve a cabo la vigilancia de las operaciones crediticias y de su apego a las medidas de control establecidas en el Manual de Crédito.
Comité de Crédito	Responsable de la aprobación de los créditos, debiendo observar el Manual de Crédito
Director General	Vigilar el cumplimiento de los límites de crédito establecidos por el Consejo de Administración, así como el estado de la cartera vencida, entre otros, mediante reportes al Comité de Auditoría y al Consejo de Vigilancia.
Auditor Interno o Área Designada	Vigilar el cumplimiento de los límites y políticas de riesgos.

Tabla 6. Vigilancia del Proceso Crediticio

Los funcionarios, Consejeros o miembros del Comité de Crédito, no podrán participar en ninguna etapa del proceso crediticio, cuando el crédito en cuestión pueda representar conflictos de intereses para dichas personas.

Provisionamiento de cartera y coeficiente de liquidez.

Las Entidades en su política crediticia, dependiendo de su Nivel de Operaciones, deben tener presentes los siguientes aspectos para una correcta implementación:

(i) Calificar y constituir las estimaciones preventivas para riesgos crediticios correspondientes a su cartera crediticia de conformidad con la metodología establecida en la regulación,

(ii) Mantener niveles de liquidez mínimos en relación con sus operaciones pasivas de corto plazo,

(iii) Ajustarse a los lineamientos de diversificación de riesgos establecidos en la normatividad.

Riesgo de Crédito

Las Cajas de Ahorro, a partir de Nivel de Operación II, deben establecer medidas para efecto de llevar a cabo la administración del riesgo crediticio, riesgo en la administración de cartera crediticia y riesgo de operaciones con instrumentos financieros.

11.4 Diagrama y Plan de Trabajo.

La digitalización de un producto o servicio de crédito pasa por los pasos y aspectos mencionados esencialmente en la Sección 9 anterior. En ese sentido, es necesario tomar en cuenta que transformar un servicio de crédito a un sistema digital es un proceso complejo que involucra esencialmente:

A. Definición del proyecto

Definición del plan de negocio y cambio en el modelo financiero de la Entidad. Se debe revisar el plan utilizado por la Entidad actualmente y establecer:

(a) El mercado objetivo del nuevo servicio.
(b) Planteamiento de los riesgos del nuevo servicio.
(c) Revisión de la situación financiera y contable de la Entidad para preparar el modelo de negocio con base en las cifras e información actual de la Entidad.
(d) Tipo de crédito: revolvente o no, así como la manera de obtener un repago seguro.
(e) Destino de los créditos.
(f) Definición de existencia o no de garantías
(g) Tasas de interés y comisiones.

(h) Definición de todas las etapas del proceso crediticio para el nuevo servicio: desde la originación, contratación, desembolso, pago, cancelación o cobranza.

(i) Canales de marketing.

(j) Identificación de las necesidades tecnológicas para efecto de llevar a cabo la prestación de servicio.

(k) Identificación preliminar de los proveedores tecnológicos relevantes.

(l) Planeación de la arquitectura tecnológica de la nueva plataforma (e.g. una aplicación, sitio web).

(m) Revisión de control de fraudes.

(n) Revisión de calidad crediticia.

(o) Identificación de clientes.

(p) Canales de celebración de los contratos.

(q) Canales de administración del crédito: manera en que el saldo será desembolsado, la administración de saldo.

B. Planeación

La planeación debe abarcar la implementación de todos los aspectos mencionados anteriormente para efecto de fijar lo siguiente:

(a) Partes Responsables del proceso crediticio, considerando: administración de la Entidad (Consejo de Administración, Director General, Auditoría Interna, áreas de negocio involucradas en el Proyecto y asesor externo legal y tecnológico).

(b) Elaboración de un documento que contenga las etapas del Proyecto, así como un cronograma.

(c) Establecimiento de las metas de cada una de las Partes Responsables.

(d) Preparación de una presentación del Proyecto donde se establezca:

- Partes Responsables.
- Antecedentes e identificación del nuevo servicio.
- Necesidades que atiende el servicio.
- Mercado objetivo del servicio.
- Características de negocio (garantías, tasas de interés, entre otras).
- Aspectos regulatorios generales.

- Aspectos técnicos involucrados.
- Aspectos que requerirán contratación de nuevos servicios o de aspectos tecnológicos externos.
- Inclusión de diagramas de flujo y explicativos de cada una de las fases del crédito, así como identificación de cambios que será necesario realizar en cada uno de los procesos preliminarmente identificados.

(e) Reuniones con cada una de las áreas impactadas por el nuevo servicio para realizar:

- Mapeo de procesos que serán objeto de digitalización y cuáles podrían quedar sin cambios o con adecuaciones menores.
- Documentar sus opiniones: objeciones, sugerencias y preocupaciones sobre el nuevo Proyecto.

(f) Preparar el nuevo modelo de servicio estableciendo: crecimiento esperado por año, factores que afectarán ese crecimiento, visualización de los estados financieros de la Entidad con base en la inclusión del nuevo servicio.

(g) Establecer contacto con CNBV para efecto de prestar la iniciativa, utilizando, por lo menos, los elementos mencionados en el inciso (d) anterior.

(h) Contactar con los Proveedores Relevantes para efecto de establecer:

- Tipo de servicios que se prestarán.
- Vinculación del servicio que se prestará con los procesos identificados como parte del nuevo negocio.
- Pruebas de los servicios que se pretende contratar con intervención de las áreas tecnológicas y del Asesor Externo para efecto de evaluar la adecuación del producto con lo que requiere la Entidad.
- Firma de los convenios de confidencialidad y cartas compromiso que sean necesarias para efecto de asegurar que cualquier información compartida con ellos tendrá tal carácter y contar con un respaldo sobre los términos y condiciones que serán acordados con ellos.

(i) Establecer procesos de evaluación crediticia adecuados que estén alineados con los procesos de contratación e identificación de clientes (PLD/FT).

(j) Contratación del Administrador del Proyecto o AP.

C. Entrega

(a) Establecimiento de ruta crítica que involucre: (i) autorizaciones internas, (ii) aprobaciones de las áreas a cargo de control interno, (iii) revisión y documentación de los nuevos procesos para revisión de Manuales y autorizaciones de Proveedores Relevantes (ver Secciones 15 y 16) de la presente Guía Legal.

(b) Revisión y adaptación del plan del Proyecto a los tiempos y temas que las áreas técnicas y Proveedores Relevantes tengan para efecto de que exista orden y expectativas realistas en la implementación.

(c) Firma de los contratos con Proveedores Relevantes, incluyendo a los mismos los planes de trabajo detallados, así como los niveles de servicio bajo los cuales trabajarían éstos.

D. Cierre

(a) Establecimiento por parte de la Dirección General de procesos de capacitación y apoyo del personal a cargo de operar el nuevo Servicio Electrónico por parte de proveedores, en su caso.

(b) Ver **Sección 2 de la presente Guía Legal (Aspectos Generales de la Administración de un Proyecto).**

Digitalización de un producto o servicio de crédito.

Gráfica 10. Digitalización de un producto o servicio de crédito. Fuente: Vite Abogados

En algunos supuestos es posible que sea necesario contratar a un Proveedor Relevante para efecto de que realice algunos de los procesos relevantes para este tipo de Proyectos, en cuyo caso el diagrama y plan de trabajo mencionados deberán adaptarse para reflejar los procesos correspondientes ante CNBV (ver Sección 16 Prestadores de Servicios Operativos).

11.5 Aspectos Prácticos.

Las actividades crediticias experimentan una mayor competencia que muchos servicios financieros tradicionales debido a que no se requiere licencia o autorización para efecto de su ofrecimiento y ejecución frente al público en general de manera profesional y habitual. Asimismo, existe una presencia cada vez mayor de las grandes empresas tecnológicas (Amazon, Google, Facebook, entre otras) en los servicios financieros. Por ejemplo, Amazon ha implementado un servicio denominado *Amazon Loans* para financiar

capacidades de venta a escalas mayores. Es un servicio solo por invitación que se ofrece estrictamente a "vendedores seleccionados" en los mercados donde Amazon tiene operaciones. Mediante un algoritmo, Amazon selecciona a los vendedores para recibir préstamos en función de la frecuencia con la que se agotan sus productos, la popularidad de éstas y demás variables. Si el vendedor es elegible recibe un correo notificándole de su precalificación para el préstamo y el monto del crédito. El objetivo es que puedan comprar inventario y aumentar ventas. Aprobado el crédito los fondos se desembolsan a la cuenta de vendedor de Amazon en aproximadamente cinco días hábiles. El pago mensual del crédito se deduce automáticamente de su cuenta de vendedor de Amazon. Las tasas de interés se ubican alrededor del 10% al 13%, mucho más barato que los créditos en tarjeta.

Con esto, Amazon se encuentra financiando "actividades productivas" a ciertas personas que de algún modo son sus "socios" (en un sentido no legal del término) en sus operaciones. De la experiencia de Amazon son valiosas las siguientes lecciones para el SACP:

- Las Big-tech (empresas con preponderancia en el mercado de los servicios tecnológicos como la mencionada) almacenan cantidades gigantescas de datos y cuentan con herramientas que les permiten extraer conclusiones y predecir comportamientos futuros (incluyendo los financieros) de sus clientes.
- La capacidad y penetración de las Big-tech podría representar un competidor muy importante para el sector financiero y, para lo cual, aún están por escribirse reglas más claras (además de las que actualmente existen en materia de competencia económica).
- La interacción y conocimiento constante con los Socios y usuarios de las Entidades es esencial para (i) crear lealtad y acostumbrar a los clientes al uso de las aplicaciones y/o herramientas que la Entidad ponga a su disposición, y (ii) poder competir en nichos específicos que atiendan a su función social y evitar el impacto que tendrá la entrada de las Big-tech en los servicios financieros.

» *Fraude en línea: un problema muy real.*

Existe un mercado muy grande que se dedica a la falsificación de documentos, al tráfico de información personal y de maneras de suplantar electrónicamente la identidad de otra

persona que muchos actores en el sector financiero, sobre todo en el mercado crediticio, incluso han dejado de operar debido a la prevalencia de estas prácticas por el impacto tan grande que tienen en su viabilidad.

Si bien no existe una receta simple ni una manera única de prever el fraude o la suplantación de identidad, pueden identificarse ciertos aspectos que podrían reducir su impacto en las Entidades que transiten hacia un proceso de digitalización:

- Auditoría Interna. Esta área, al conocer de manera detallada la Entidad, sus procesos, y el entorno en que realiza sus negocios tiene una capacidad importante para implementar herramientas de prevención, disuasión y detección del fraude, tanteo externo como interno. Se recomienda que esta área no sea subcontratada: la formación de un equipo interno es esencial para alinear intereses, prever rotación de personas responsables del área y garantizar que se tomarán el tiempo necesario para atender sus deberes. Se requiere digitalizar y automatizar los procesos de esta área para lograr que la misma pueda obtener información inmediata y organizada de lo que ocurre en la Entidad.
- Auditoría Externa. Si bien existen reglas especiales emitidas por CNBV para la contratación de auditores externos, la realidad es que estos profesionales no tienen un enfoque antifraude, sino a reflejar la situación financiera de manera global y libres de cualquier error. Existen factores que impiden un enfoque antifraude: falta de tiempo, información limitada o genérica, etc. Por lo tanto, debe diferenciarse bien entre un estado financiero bien realizado y una Entidad libre de fraudes.
- Códigos de Conducta. Debe reforzarse la difusión del Código de Conducta hacia el interior de la Entidad y capacitar al personal sobre su contenido. Asimismo, debe ser adaptado para reflejar la cero tolerancia de la Entidad hacia el fraude o actividades perjudiciales. Se sugiere que el mismo sea un anexo de los contratos de trabajo del personal para darle el carácter de documento vinculante.
- Políticas y Programas Anti-Fraude. Deben existir los mecanismos y las adecuaciones en los procesos de la Entidad que impidan o hagan muy complicado el fraude. Actualmente, existen muchos prestadores de servicios que conocen bien el sector financiero y que cuentan con programas muy efectivos para lograr estos propósitos, incluso incorporando técnicas de IA y análisis de datos. Su

implementación puede requerir, dependiendo de las características del prestador de servicios, la autorización de CNBV (ver Sección 15). En todo caso, las políticas y el sistema deben ir de la mano: el documento debe establecer funciones, categorías, procesos y descripción de consecuencias, mientras que el programa debe fungir como una herramienta principal en la implementación de ese documento.

- Sistema de Control Interno. Se ha hablado en la Sección 4 del control interno y de su importancia. Queremos retomar ese tema: el control interno es la columna vertebral de la eficiencia operativa de las Entidades, es el sustento de la confianza de los reportes de información legal o financiera y tiene como objeto la supervisión adecuada del cumplimiento normativo. Su refuerzo minimiza la posibilidad de que se formen camarillas o asociaciones de empleados con fines ilegales dentro de la Entidad, incide en la reducción de errores y fraudes por parte de los empleados.

- Manual de Riesgos. El Manual de Riesgos debe reforzarse para efecto de prevenir y detectar el fraude: la evaluación de riesgos puede prevenir un porcentaje alto de fraudes potenciales. La identificación de señales de alerta, así como mitigación deben encontrase ahí o en un documento similares. Dichas señales pueden ser, entre otros, estilos de vida lujosos o inusuales de empleados o colaboradores de la Entidad, documentación falsa o sospechosa y controversias con proveedores o créditos otorgados a personas con historial crediticio deficiente.

- Delatores Internos. Esta práctica conocida como *whistle blowing* es común y efectiva. Es lo que en México conocemos como "dar el pitazo". Consiste en el diseño de un sistema que permita realizar denuncias sobre actividades que podrían perjudicar a la Entidad. Debe abarcar a todos los elementos de la Entidad. Ante todo, debe haber un equilibrio entre la anonimidad de las denuncias y la necesidad de pruebas y de elementos para iniciar investigaciones y castigar a los culpables. Asimismo, debe haber un catálogo de medidas correctivas para aquellos casos en los que si bien no se materializa el fraude existe un riesgo efectivo del mismo.

- Contabilidad Forense. Existen servicios especializados de contabilidad forense: una mezcla de auditoría, investigación y contabilidad. Se trata de especialistas que recopilan y analizan documentos y datos de la Entidad para determinar la posible existencia de un delito financiero. La contratación eventual de estos profesionales puede ser un fuerte elemento disuasorio para cometer fraudes.

- Procesos de Contratación. Es necesario verificar las referencias y antecedentes de cada empleado de la Entidad. Su comportamiento anterior puede ser referencia de su comportamiento futuro.
- Procesamiento de Datos. La minería de datos hace uso de datos pasados de un fraude o serie de fraudes ya realizados para construir un marco de referencia que permita identificar riesgos futuros. Se trata de la extracción patrones y tendencias examinando los informes de la Entidad para descubrir patrones desconocidos o únicos que pueden indicar un posible fraude. Las técnicas usadas son: programación genética y redes neuronales. Incluso es posible que sea más fácil de usar en empresas más pequeñas pues los patrones y fuentes de información son más accesibles y fáciles de identificar.
- Firewalls. Los *firewall*s o cortafuegos también son esenciales para impedir el acceso de terceros no autorizados a los sistemas de la Entidad.
- Capacitación. Los empleados son esenciales para controlar el fraude. Deben saber qué es, cuándo ocurre (a diferencia, por ejemplo, de errores involuntarios), posibles causas y consecuencias. El personal debe identificar las señales de alerta y tener las herramientas para notificar cualquier elemento sospechoso.

SECCIÓN 12.- IMPLEMENTACIÓN DE FIRMA ELECTRÓNICA.

Para efecto de manifestar el consentimiento o la voluntad (elemento esencial de los actos jurídicos), tradicionalmente se ha utilizado la "firma autógrafa" que no tiene una definición jurídica como tal. Se trata de rasgos (realizados siempre de la misma manera) que permiten identificar o atribuir su autoría a una persona y tienen como función dar autenticidad o certeza de la voluntad de su emisor. La firma autógrafa se ha usado consuetudinariamente con ese objetivo, salvo por aquellos casos en que no es viable o requerida (e.g. huella dactilar).

El derecho mexicano permite y acepta el uso de "firmas electrónicas". Actualmente el Código Civil Federal menciona que el consentimiento será expreso cuando se manifieste, entre otras formas, por tecnología electrónica, óptica o de cualquier otro tipo. Agrega que en los casos en que se requiera que el consentimiento sea por escrito, dicho requisito se considerará cumplido cuando la información electrónica sea imputable a los obligados y pueda ser posteriormente consultada. En consonancia con ello, el Código de Comercio establece que "en los actos de comercio y en la formación de estos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología".

Al respecto, el Código de Comercio menciona que los actos jurídicos que se celebren por medios electrónicos quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones que la modifican. Asimismo, reglamenta en una sección específica el comercio electrónico, reconociendo expresamente la formación de actos de comercio a través de medios electrónicos y, por lo tanto, abriendo la posibilidad legal de la firma electrónica.

12.1 Concepto de Firma Electrónica.

La firma electrónica consiste en los datos electrónicamente consignados en un "Mensaje de Datos", adjuntados o lógicamente asociados al mismo por cualquier tecnología, que se utilizan para identificar al firmante en relación con dicho Mensaje de Datos y con el objeto de indicar que el firmante aprueba la información contenida ahí. Dicha firma produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio. Es decir, la firma electrónica tendrá la misma validez que la firma autógrafa siempre que sea transmitida mediante un Mensaje de Datos atribuible a su autor.

Hay varias definiciones relevantes que hay que tener en cuenta para este concepto:

- Emisor: es toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, sin que haya actuado a título de Intermediario.
- Mensaje de Datos: significa toda información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología. El Mensaje de Datos es el medio por el cual viaja la información entre las partes contratantes y que sirve para hacer evidente el consentimiento para obligarse.
- Sistema de Información: significa aquel sistema utilizado para generar, enviar, recibir, archivar o procesar los Mensajes de Datos. En materia de derecho mercantil no existe regulación sobre aspectos esenciales del Sistema de Información, que como veremos en las secciones siguientes, sí existe para el caso de Entidades Financieras.
- Certificado: significa un Mensaje de Datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de Firma Electrónica.

Se presume la atribución de un Mensaje de Datos si se ha sido enviado: (i) por el propio emisor; (ii) usando medios de identificación, tales como claves o contraseñas del emisor o por alguna persona facultada para actuar en nombre del emisor respecto a ese Mensaje de Datos, o; (iii) por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

La ley establece que existe una presunción de que el Mensaje de Datos ha sido enviado por el emisor: (i) cuando éste haya aplicado en forma adecuada el procedimiento acordado previamente con el Emisor, con el fin de establecer que el Mensaje de Datos provenía efectivamente de éste, o (ii) el Mensaje de Datos que reciba el destinatario resulte de los actos de un intermediario que le haya dado acceso a algún método utilizado por el emisor para identificar un Mensaje de Datos como propio. Lo anterior tiene algunas reglas de no aplicación establecidas en el propio Código de Comercio para salvaguardar el principio de atribución de la firma electrónica.

Las reglas de recepción del Mensaje de Datos y de procedencia de este, así como las guías técnicas para su implementación y prueba, están contenidos en el Código de Comercio y en la N*orma Oficial Mexicana NOM*-151-SCFI-2016 (NOM 151), respectivamente.

12.2 Tipos de Firmas Electrónicas.

Nuestra legislación distingue los siguientes tipos de Firmas Electrónicas:

- Firma Electrónica Simple**:** significa, por exclusión, aquella que no cumple con los requerimientos para ser considerada como una Firma Electrónica Avanzada. Se trata de información consignada en forma electrónica que es posible atribuir al Emisor de esta como un consentimiento válido. Ejemplos de lo anterior serían: números de identificación personal, huellas digitales, entre otros.

- Firma Electrónica Avanzada o Fiable. Cuando la ley requiera o las partes acuerden la existencia de una firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una firma electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos. Se considera que la Firma Electrónica es Fiable cuando: (i) los datos de creación de la firma corresponden exclusivamente al firmante; (ii) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante; (iii) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y que, (iv) respecto de la integridad de la información de un Mensaje de Datos, sea posible detectar cualquier alteración de ésta hecha después del momento de la firma. Un ejemplo de lo anterior es la FIEL que, si bien tiene una regulación especial en el Código Fiscal y demás disposiciones, se encuentra en este supuesto.

La Firma Electrónica Avanzada deberá estar amparada por un Certificado digital vigente que confirme el vínculo entre el firmante y los datos de creación de la Firma Electrónica Avanzada. Es decir, para que los sujetos puedan utilizar la Firma Electrónica Avanzada en los actos, deberán contar con:

(a) Un Certificado digital vigente, y
(b) Una clave privada, generada bajo el exclusivo control del firmante.

Este Certificado digital debe contar con las siguientes características: (i) número de serie; (ii) autoridad certificadora que lo emitió; (iii) algoritmo de firma; (iv) vigencia; (v) nombre del titular del certificado digital; (vi) dirección de correo electrónico del titular del certificado digital; (vii) Clave Única del Registro de Población (CURP) del titular del certificado digital; y (viii) clave pública.

Son consideradas "Autoridades Certificadoras", es decir, autoridades con la capacidad de gestionar la creación de certificados a usuarios finales, dando fe de la identidad del titular de una firma, la SHCP, la Secretaría de Economía y el Servicio de Administración Tributaria. Asimismo, las dependencias y entidades, distintas a las mencionadas, así como los prestadores de servicios de certificación deberán cumplir con ciertos requisitos para obtener tal carácter, entre ellos contar con un dictamen favorable por parte de la SHCP.

Existe una figura denominada "Prestadores de Servicios de Certificación" quienes conforme a la NOM 151 prestan servicios relacionados con (i) emisión de certificados digitales de firma electrónica con el objeto de vincular la identidad de una persona a un documento electrónico y (ii) emisión de sellos de tiempo, mismos que demuestran que el documento electrónico existe desde cierta fecha y no ha sido alterado, entre otros.

12.3 Regulación y Validez.

Como se mencionó anteriormente, el uso de la Firma Electrónica es legal, pues en las legislaciones civil, mercantil, laboral y administrativa se encuentra previsto su uso. En todo caso la Firma Electrónica, salvo que el acto jurídico requiera de otras formalidades, produce los mismos efectos jurídicos que la firma autógrafa, teniendo el mismo valor probatorio que ésta.

12.4 SACP y Firma Electrónica.

Para la contratación de Servicios Electrónicos con los Usuarios, las Entidades están obligadas, además de lo mencionado en la Sección 9 de la presente Guía Legal, a obtener el consentimiento expreso mediante firma autógrafa de sus Usuarios, previa identificación de estos, o bien, mediante Firmas Electrónicas Avanzadas o Fiables de los propios Usuarios, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio (tal como se ha expuesto anteriormente). En todo caso, podrá obtenerse el consentimiento de sus

Usuarios mediante alguna otra forma de contratación, tratándose de los siguientes servicios:

(a) Servicios de Pago Móvil.

(b) Aquellos ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, cuando estos se refieran exclusivamente a la operación de Cuentas de Bajo Riesgo.

(c) Servicios Avanzados Móviles, Servicio por Internet, Servicio Telefónico Audio Respuesta y Servicio Telefónico Voz a Voz, cuando estén asociados a Cuentas de Bajo Riesgo y sean operaciones diferentes a transferencias, pagos de contribuciones, entre otros.

(d) Los contratados a través de Cajeros Automáticos y Terminales Punto de Venta para realizar operaciones monetarias hasta de Mediana Cuantía.

12.5 Proveedores de Firma Electrónica.

La selección de un proveedor de Firma Electrónica es uno de los aspectos más relevantes para la digitalización de productos o servicios novedosos y el lanzamiento digital de una Entidad. Como se muestra en la Sección 15, existen ciertas reglas que deben cumplirse y además la implementación tecnológica debe ser específica para la Entidad.

La búsqueda del proveedor de Firma Electrónica Avanzada debe comenzar con un plan que responda a las siguientes preguntas:

- ¿Se tiene determinado ya el Servicio Electrónico que se quiere ofrecer al público? ¿Conforme a las reglas mencionadas anteriormente es viable el uso de la Firma Electrónica?
- ¿La Firma Electrónica sería operada directamente por la Entidad o será utilizada por algún tercero, por ejemplo, un comisionista que maneje algún sitio web por cuenta de la Entidad?
- ¿Cuáles son los requisitos para dicho Servicio Electrónico, en específico límites de montos por cada servicio establecidos en la regulación para la Entidad? ¿Es

compatible el monto y el plan de negocios para efecto de realizar la contratación en línea?

- ¿La necesidad de la Firma Electrónica obedece a una estrategia antifraude o de expansión?
- ¿Se requieren servicios complementarios para efecto de implementar la Firma Electrónica, por ejemplo, capacidad de almacenamiento dentro de la Entidad para efecto de poder manejar la documentación electrónica o es algo que requeriremos de un proveedor?
- ¿El proveedor tiene experiencia en el proceso de digitalización con Entidades reguladas, ya sea del SACP, Fintech o banca múltiple? ¿Sus contratos han estado sujetos a un proceso de aprobación por parte de CNBV con alguna otra entidad regulada? ¿Cuáles fueron las observaciones anteriores?
- ¿Cuenta el proveedor con una fundamentación legal adecuada de sus servicios en el marco de la regulación financiera? ¿Responde adecuadamente a preguntas concretas generadas por un asesor legal de la Entidad?
- ¿El proveedor conoce a fondo el contenido de la NOM151 y de los estándares relacionados con la misma, por ejemplo, normas ISO?
- ¿Existe un sistema previo de contratación electrónica dentro de la Entidad o se trata de una implementación nueva?
- ¿El proveedor ofrece de manera clara una explicación visual de las funcionalidades de su sistema? ¿Entiende las consecuencias legales en caso de que decida administrar u operar bases de datos con información de los clientes o Socios de la Entidad?
- ¿Pueden acreditar la experiencia previa con otras Entidades en la implementación de la Firma Electrónica?
- ¿Existe una definición clara de las etapas del proceso de firma: desde la puesta a disposición del documento, los pasos que debe seguir el cliente, la manera de coordinar la emisión de firma con los requisitos en materia de identificación PLD/FT, así como el almacenamiento y envío de originales de los documentos firmados?
- ¿El Proveedor cuenta con técnicas avanzadas de encriptación de los datos que recibirá por parte de los Socios o clientes? ¿Cuenta con las herramientas técnicas necesarias para salvaguardar la confidencialidad de la información y tomar medidas necesarias que prevengan el fraude?

- ¿Es posible individualizar el sistema de Firma Electrónica para incorporar la marca de la Entidad? ¿Es necesario que el cliente salga de las páginas o aplicaciones de la Entidad para efecto de completar el proceso de firma?
- ¿Pueden mostrar cómo sería la experiencia de usuario? ¿Sería potencialmente complicado para los futuros Clientes o Socios generar la firma o es algo que puede darse sin generar fricción o aparecer como excesivamente complicado?

Así mismo, la Firma Electrónica Avanzada no es lo único que debe considerarse en la contratación a distancia con los clientes o Socios de las Entidades. También hay que considerar que, previo a la celebración de una operación, tal como lo mencionamos en la Sección 6 (Prevención de Lavado de Dinero y Financiamiento al Terrorismo) de esta Guía Legal, es necesario realizar la identificación del Cliente. Este proceso, cuando se realiza a distancia, también requiere del cumplimiento de requisitos específicos, como también lo mencionamos en esa parte de la Guía Legal. Existen proveedores que también ofrecen herramientas de apoyo en la identificación de clientes de manera adicional a los servicios de Firma Electrónica Avanzada.

12.6 Diagrama y Plan de Trabajo.

Si bien creemos que los aspectos mencionados en la Sección 2 Aspectos Generales de la Administración de un Proyecto Legal son válidos para efecto de implementar un Proyecto de implementación de Firma Electrónica, el mismo debe considerar estas fases:

1. Definición de la necesidad de utilizar una Firma Electrónica mediante la preparación de los casos de uso de la misma que contenga:

    (a) Breve resumen de la descripción del caso de uso (por ejemplo, firma de contratos de crédito que no rebasen ciertos montos).
    (b) Identificar las eficiencias y los propósitos de implementar una Firma Electrónica Avanzada dentro de la Entidad (por ejemplo, eliminar la necesidad de papeleo en ciertos procesos).
    (c) Volumen esperado de transacciones mediante el uso de la Firma Electrónica.
    (d) Establecer con apoyo del área de sistemas los requerimientos para poder integrar la Firma Electrónica a los procesos de contratación: por ejemplo, páginas web, Sistema Automatizado PLD/FT, y revisión de procesos internos

para verificar las áreas impactadas y que tendrán intervención en la aplicación de la Firma Electrónica.

(e) Establecer los criterios que deben utilizarse para seleccionar a un proveedor considerando lo mencionado en esta sección y establecer prioridades.

2. Establecer el tipo de Servicio Electrónico que utilizará la Firma Electrónica.

3. Hacer un mapeo de los procesos relacionados con la Firma Electrónica para efecto de determinar a las Partes Responsables, considerando por lo menos:

   (a) Integración con aplicaciones o tecnología existente de la Entidad o necesidad de adquirir nueva tecnología para efecto de que sea operativa la Firma Electrónica.

   (b) Establecer si el proceso de contratación debe ser realizado total o parcialmente en línea (por ejemplo, si la Firma Electrónica sólo es para cerrar el contrato y la identificación es presencial para efectos de no tener restricciones en materia de PLD/FT).

   (c) Plan de comunicación con los posibles Clientes o Socios sobre la nueva manera de contratar.

   (d) Identificar los procesos y aspectos relacionados con el almacenamiento y visibilidad de los documentos firmados electrónicamente.

4. Generar un mapa del proceso de *onboarding* o identificación y contratación con los potenciales Clientes y Socios que permita que la información esencial esté disponible para todas las Partes Responsables.

5. Determinar con las áreas legales: la validez de utilizar la Firma Electrónica Avanzada para cierto Servicio Electrónico y revisar los requerimientos que podrían detonarse en caso de que el proveedor se encuentre en alguno de los supuestos mencionados en la Sección 15 (Contratación de Proveedores y Comisionistas) de la presente Guía Legal.

6. Involucrar a los directivos relevantes y al Director General en el proceso de implementación y recabar su punto de vista y validación para el plan de trabajo, incluyendo a las Áreas de Auditoría Interna y Oficial de Cumplimiento.

7. Evaluar, con apoyo del área de sistemas y el responsable legal, a los posibles proveedores del servicio de Firma Electrónica con apoyo de los aspectos mencionados anteriormente.

8. Realizar con el apoyo de las áreas legales y de sistemas una planeación de los elementos que será necesario modificar para lograr la plena implementación de la Firma Electrónica, incluyendo modificación de los Manuales (Manual de Control Interno, Manual de Crédito, Manual de Captación, Manual de Administración Integral de Riesgos, Manual de Tecnologías de la Información y Manual PLD/FT) y su aprobación por el Consejo de Administración.

9. Elaborar un proyecto de contrato con el proveedor que contemple, por lo menos, los siguientes supuestos:

   (a) Obligaciones en materia de apoyo e implementación.

   (b) Clausulado mínimo que, en su caso, podría ser requerido conforme a la Sección 15 del presente documento.

   (c) Niveles mínimos de servicio.

   (d) Clarificación sobre mantenimiento y apoyo.

   (e) Niveles mínimos de operatividad de servicios.

   (f) Confidencialidad de la información.

   (g) Obligatoriedad de encriptación de la información.

   (h) Declaraciones sobre validez de la Firma Electrónica.

   (i) Indemnizaciones a cargo del proveedor.

10. Establecer los pasos de implementación que consideren, por lo menos, los siguientes aspectos:

    (a) Evaluar el impacto financiero y de riesgos de la Firma Electrónica dentro de la Entidad.

(b) Documentación técnica interna y del proveedor elegido que será necesaria para poder realizar cambios dentro de la Entidad y poder documentar el proceso ante CNBV, de ser necesario.

(c) Considerar los requerimientos y etapas regulatorias del proceso, incluyendo:

- Presentación de la iniciativa a CNBV. Se sugiere a las Entidades presentar el estudio sobre la implementación de la Firma Electrónica, el tipo de Servicio Electrónico que se utilizará, mapeo sobre las políticas y procesos que implementará la Entidad en relación con la Firma Electrónica, la planeación de los elementos que será necesario modificar, así como el proyecto de contrato con el proveedor.
- Preparación y revisión de documentación técnica por parte del proveedor verificando que cumpla con todos los requerimientos legales que se deban de cumplir.
- Expediente técnico.
- Firmas necesarias tanto de la Entidad como del proveedor.
- Plazos de respuesta de CNBV.

11. Vigilar el proceso de implementación con base en el contrato firmado con el proveedor, estableciendo claridad en las metas y en el nivel de servicio al que se ha obligado a realizar sus actividades.

12.7 Aspectos Prácticos.

Los servicios de Firma Electrónica Avanzada pueden requerir de la entrega de un aviso a CNBV para efecto de que el servicio pueda ser prestado si se cae en los supuestos mencionados en la Sección 15 (Contratación de Proveedores y Comisionistas) de la presente Guía Legal, en virtud del manejo de información que hará. Esto puede ocurrir, sobre todo, en el momento de almacenar o tener acceso al documento. Recordemos que, como se mencionó en la Sección 8 (Seguridad de la Información y Confidencialidad y Continuidad de la Operación), la Entidad tiene un deber de confidencialidad de la información de sus Clientes o Socios, por lo que es necesario acreditar que se cuenta con la capacidad técnica y las herramientas necesarias para garantizar la confidencialidad en los casos en que sea necesario notificar a la CNBV la celebración de este.

Por otra parte, es posible que, dadas las características de los servicios, se requiera celebrar un contrato de remisión de datos personales entre la Entidad y el proveedor de Firma Electrónica conforme a lo mencionado en la Sección 8 (Seguridad de la Información y Confidencialidad y Continuidad de la Información) de la presente Guía Legal.

SECCIÓN 13.- APERTURAS DE CUENTAS REMOTAS.

La apertura de cuentas remotas es uno de los elementos que caracterizan a la Banca Electrónica. Gradualmente, los clientes o Socios de las Entidades están volviéndose digitales, haciendo que los modelos basados en sucursal pierdan atractivo o viabilidad.

Las Entidades, por ley[70], se encuentran autorizadas a recibir depósitos de dinero a la vista, de ahorro, a plazo, retirables en días preestablecidos y retirables con previo aviso. En ciertos casos, dichas operaciones pueden realizarse con menores de edad, en términos de la legislación común aplicable, siempre y cuando sus padres o tutores sean Socios.

Si bien ya comentamos en secciones anteriores los requerimientos de la Banca Electrónica para las Entidades (Sección 9 de la presente Guía Legal), consideramos que la apertura de cuentas a distancia constituye uno de los pasos más importantes en los procesos de digitalización de una Entidad. En este sentido recomendamos que al considerar un proceso de apertura de cuentas remotas:

(i) La prioridad en ello debe estar en el Socio o el cliente, es decir, estos procesos deben responder a una necesidad identificada de un potencial usuario final. Entender de qué manera se puede facilitarles el manejo de su dinero.

(ii) Identificar procesos burocratizados o inefectivos e incorporarlos en las iniciativas de apertura de cuentas remotas. Por ejemplo, complementar la apertura remota con el manejo remoto y evitar, en la medida permitida por la regulación, el desplazamiento físico del cliente.

(iii) Establecer en los sistemas de apertura herramientas que permitan identificar comportamientos y preferencia de los usuarios.

[70] LACP y LRASCAP.

Contratación remota

Gráfica 11. Contratación Remota. Fuente: Vite Abogados

13.1 Apertura de cuentas no presenciales.

Las cuentas a las que hacemos referencia esencialmente son a las que constituyen depósito de dinero a la vista en efectivo, pues son las que de manera explícita permiten la apertura remota. Conforme a la regulación[71], las cuentas en que se lleven a cabo estos depósitos podrán abrirse con un expediente completo o bien, con un expediente simplificado para aquellas consideradas de Bajo Riesgo conforme a establecido en las Disposiciones PLD/FT (Ver Sección 6 Prevención de Lavado de Dinero y Financiamiento al Terrorismo).

Las cuentas de Bajo Riesgo deben ajustarse a la suma de los abonos en el transcurso de un mes calendario y no podrán exceder al equivalente en moneda nacional a mil UDIS. Se pueden recibir depósitos mensuales adicionales al límite establecido, hasta por el equivalente en moneda nacional de seis mil UDIS, siempre que el origen de los recursos provenga exclusivamente de subsidios relativos a programas gubernamentales de apoyo a determinados sectores de la población. Para realizar el cálculo en UDIS las Entidades deberán tomar el valor de dicha unidad de cuenta del último día del mes calendario anterior al mes de que se trate.

Para determinar el monto máximo de los abonos en las cuentas de Bajo Riesgo en el transcurso de un mes calendario, las Entidades podrán abstenerse de incluir los importes relativos a intereses, devoluciones por transferencias electrónicas de fondos y cualquier otra bonificación que dichas Entidades realicen por el uso o manejo de la cuenta que, en su caso, se efectúen en el periodo relevante.

Adicionalmente, la apertura de cuentas de Bajo Riesgo, a través de la recepción o captura de datos de forma remota deben contar con la previa autorización de la CNBV. La solicitud de autorización debe establecer la descripción de los procedimientos que implementarán para evaluar los controles que minimicen los riesgos asociados a esta operación, los cuales deberán considerar al menos lo previsto en los apartados de control interno, según la regulación prudencial que le corresponda a la Entidad conforme a su Nivel de Operaciones.

[71] Disposiciones PLD/FT

Asimismo, es necesario que la Entidad, en el momento de implementar este tipo de servicio, considere:

- Un plan de negocios que considere sus niveles de liquidez como resultado de la implementación de este tipo de servicio.
- Las reglas de diversificación de pasivos que sean aplicables a cada Entidad.
- Identificar los riesgos que podría representar el nuevo servicio conforme al Nivel de Operaciones que le corresponda a la Entidad.

13.2 Tipos de cuentas.

Las Entidades, de conformidad con el Anexo 2 de las Disposiciones PLD/FT, podrán celebrar contratos de forma no presencial para la apertura de las siguientes cuentas:

1. Clasificadas como de Bajo riesgo;

2. Apertura de cuentas de depósito, siempre que se pacte en los contratos respectivos que la suma de los abonos en el transcurso de un mes calendario no debe exceder del equivalente en moneda nacional a 30,000 UDI; y

3. Créditos comerciales que se otorguen a personas físicas con actividad empresarial y créditos al consumo, en ambos casos por montos menores al equivalente en moneda nacional a 60,000 UDI.

13.3 Consideraciones PLD / FT.

Conforme a las Disposiciones PLD/FT la apertura de cuentas de Bajo Riesgo tiene las siguientes implicaciones cuando son abiertas de manera remota:

- Los expedientes de identificación de los clientes deben contener: los datos relativos al nombre completo sin abreviaturas, género, entidad federativa de nacimiento, fecha de nacimiento, así como domicilio de estos.
- Las Entidades pueden llevar a cabo la recepción o captura de los datos de forma remota, en sustitución de una entrevista presencial, siempre y cuando la Entidad

de que se trate, verifique la autenticidad de los datos del Cliente, mediante el siguiente procedimiento:

- Las Entidades, ya sea directamente o a través de un tercero, deberán realizar una consulta al Registro Nacional de Población a fin de integrar la Clave Única del Registro de Población del Cliente y validar que los datos proporcionados de manera remota por el mismo, con excepción del domicilio, coincidan con los registros existentes en las bases de datos de dicho Registro.
- Adicionalmente, en el caso de cuentas que se encuentren ligadas a un teléfono móvil u otro dispositivo de comunicación equivalente, las Entidades deberán validar el número de teléfono móvil proporcionado, mediante el procedimiento que para tal efecto establezcan las Entidades en su Manual de Cumplimiento.

La validación de los datos de identificación a que se refiere las Disposiciones PLD/FT podrá llevarse a cabo a través de procedimientos distintos a los antes señalados, previa autorización de la CNBV, con opinión de la SHCP.

Remitimos al usuario de esta Guía Legal a la Sección 6 del presente documento donde se establecen las consideraciones adicionales sobre temas PLD/FT.

13.4 Limitaciones y Características de los Servicios.

Los servicios deben ceñirse, para la apertura de cuentas de depósito, a aquellas a la vista en efectivo y de Bajo Riesgo.

Asimismo, para los detalles de implementación del Servicio Electrónico correspondiente que se daría a través de estas cuentas nos remitimos a la Sección 9 (Datos Personales y Secreto Financiero) de la presente Guía Legal.

13.5 Diagrama y Plan de Trabajo.

Consideramos que el plan que debe seguirse para efecto de implementar la apertura de cuentas remotas o a distancia, es esencialmente el establecido en la Sección 9 (Datos Personales y Secreto Financiero) atento que las mismas son parte de los Servicios

Electrónicos de la Entidad. Sin embargo, este Proyecto estaría sujeto a las siguientes particularidades:

(a) Realizar un estudio de mercado, sobre todo entre Clientes o Socios existentes de la Entidad para verificar cuál es su experiencia en la apertura y uso de cuentas bancarias, incluyendo: destino de las cuentas, experiencia en los procesos en sucursal, principales problemas para abrir y operar.

(b) Alinear la apertura de cuentas remotas con los objetivos y el plan de negocios de la Entidad. La apertura a distancia de cuentas no es un tema que deba tomarse como necesario o deseable en todos los casos, sobre todo por el esfuerzo y costo implicados. En ese sentido la conversación debe darse a nivel de la Dirección General y Consejo de Administración y, posteriormente, ante las áreas involucradas en los procesos principales de la Entidad.

(c) Realizar una consulta interna con las áreas tecnológicas, Auditoría Interna, Oficial de Cumplimiento, legal y financiera de la Entidad para entender las limitaciones que existen para este tipo de Proyecto y diagnosticar las capacidades tecnológicas y operativas con las que se cuenta para ello. En ese sentido, dado el carácter legal de este documento nuestro énfasis es en los aspectos PLD/FT y demás regulación que limita montos y desarrolla de manera específica los requisitos del *onboarding* a distancia, pero es necesario realizar un diagnóstico en materia de:

- Riesgos a los que estaría expuesta la Entidad, no sólo los que ordinariamente pueden estar reflejados a esa fecha en el Manual de Riesgos Respectivos, sino aquellos de índole tecnológica derivados del uso de tecnologías informáticas.
- Necesidad de modificar la metodología de riesgos de la Entidad en materia de PLD/FT.
- Diagnosticar la capacidad de los sistemas actuales de la Entidad para soportar los requerimientos en materia de Banca Electrónica (Sección 9), continuidad y seguridad de la información (Sección 7).
- Identificar las tecnologías que será necesario obtener de parte de Proveedores Relevantes y, en su caso, las autorizaciones que serían necesarias por parte de CNBV (Sección 15).

(d) El Director General deberá realizar la asignación de equipos de trabajos concentrados en las siguientes áreas o temas relevantes para la implementación:

- Administrador del Proyecto: para efecto de implementar la metodología mencionada en la Sección 2, incluyendo el cronograma y, si es requerido, la selección de las herramientas tecnológicas que podrán rastrear el seguimiento del Proyecto.
- Tecnológica: tendrán a su cargo realizar la revisión de los Proveedores Relevantes, establecer de manera general la necesidad de contratación de capacidades adicionales y validar y verificar que dichos proveedores presten sus servicios con los niveles de calidad convenidos.
- Legal: el área legal debe coordinar los aspectos regulatorios y normativos, por ejemplo, la verificación de los requisitos legales para la apertura de cuentas, la validación de los elementos económicos del nuevo producto (comisiones y tasas de interés), asesoría sobre cambios en Manuales, validación de contratos con Proveedores Relevantes y validación de los cambios en la publicidad de la Entidad.
- Financiero: esta área debe realizar las proyecciones de crecimiento del nuevo producto, formular el modelo financiero, establecer el mercado objetivo y apoyar con la evaluación de riesgos para efecto de no poner en riesgo los niveles de capitalización de la Entidad.

(e) Elaboración de una presentación con los elementos esenciales del Proyecto, para efecto de que pueda ser aprobada por el Consejo de Administración. En este documento debe quedar claro:

- Antecedentes del Proyecto.
- Partes Responsables.
- Necesidad de la apertura remota.
- Consideraciones legales.
- Capacidades tecnológicas requeridas o adicionales.
- Proyección financiera.
- Costos involucrados y, en su caso, autorización para erogar las cantidades que se requieran para comenzar, planear y concluir el Proyecto.

(f) Establecer contacto con CNBV para efecto de llevar hacia ellos los puntos mencionados en la presentación anterior y tener su retroalimentación sobre la posibilidad de éxito. Recordemos que ellos tienen mayor visibilidad global del SACP y que son repositorio muy valioso de experiencias en otras Entidades.

(g) Exploración y evaluación de Proveedores relevantes.

(h) Establecimiento de reuniones de retroalimentación donde estén presentes las áreas responsables y las Partes relacionadas para validar un documento elaborado por parte del Administrador del Proyecto en donde se establezcan:

- Los pasos a seguir y los responsables de cada uno, así como los tiempos estimados de cierre.
- Un cronograma de actividades que considere plazos razonables para la implementación y cierre del Proyecto.

(i) El Director General deberá solicitar al Administrador del Proyecto una metodología de seguimiento que puede consistir:

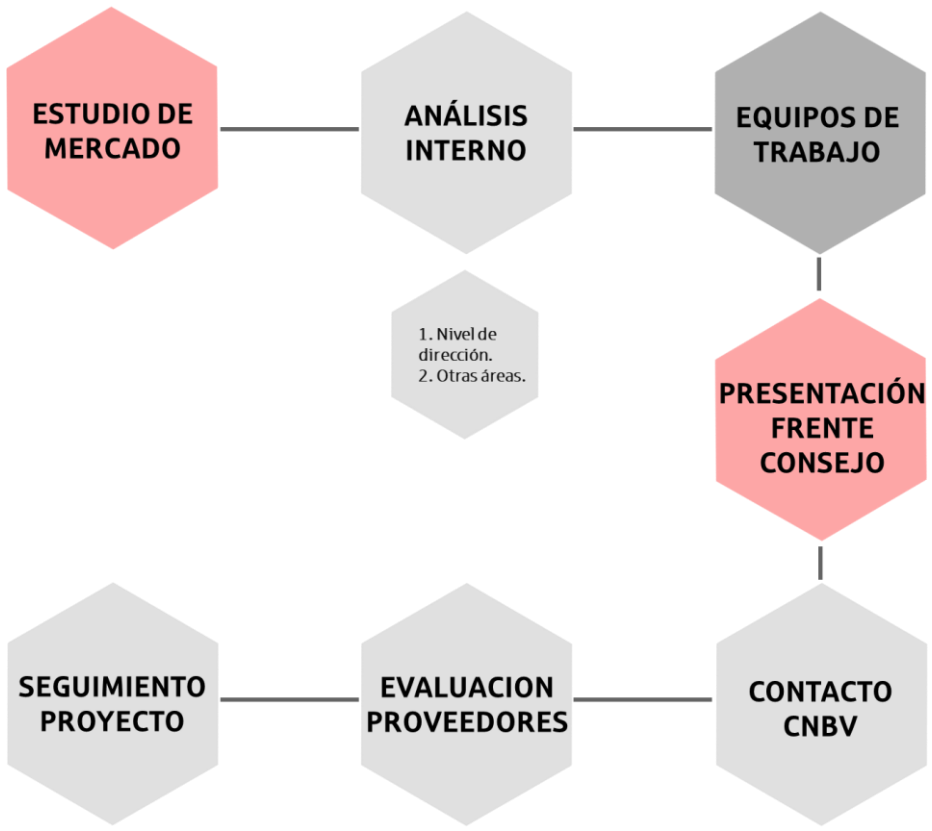
- En alguna herramienta informática ya presente en el mercado que permita: (i) visibilidad de todas las partes de los temas pendientes y próximos a cubrir, así como una demarcación de hitos que deben completarse, (ii) subir documentos e información útil para todos y facilitar la administración de los documentos del Proyecto y (iii) asignar responsabilidades de manera rápida y efectiva, (por ejemplo, mediante correo electrónico).
- A través de conferencias telefónicas o cualquier otro medio, realizar la revisión periódica de los avances involucrando a todas las áreas responsables.

(j) El avance del Proyecto debe ser presentado por el Director General al Consejo de Administración de manera continua para que, en el cierre del mismo, este órgano se encuentre con suficiente información para aprobar los resultados del mismo.

(k) Realizar cualesquier notificaciones o avisos a CNBV par efecto de mantenerla al tanto de la salida del Proyecto, así como realizar las adaptaciones y validaciones

necesarias que requiere Condusef en materia de transparencia (ver Sección 5 Transparencia y Ordenamiento de los Servicios Financieros).

Proceso de análisis para evaluar la conveniencia de abrir cuentas de manera remota



Gráfica 12. Proceso de análisis para evaluar la conveniencia de abrir cuentas de manera remota. Fuente: Vite Abogados

13.6 Temas Prácticos.

Existen temas regulatorios ya expuestos sobre los cuales debe existir una planeación exhaustiva y precisa, sobre todo por los requisitos que marca el Anexo 2 de las Disposiciones PLD/FT, entre los que se encuentran los siguientes:

(i) Controles de Verificación de Identidad. Al obtener información de identificación, se debe tener en cuenta el tipo y la naturaleza de los documentos y la información que

contienen. Es importante que las Entidades tengan en cuenta la validez y autenticidad de los datos, la documentación y la información obtenida con respecto a sus futuros clientes pues las Disposiciones PLD/FT establecen que la verificación de la autenticidad de los documentos será responsabilidad de las Entidades. Deben considerar controles para garantizar que los documentos de identidad no han sido alterados o falsificados. Ello puede implicar una limitación para el número y tipo de documentos aceptables para realizar la identificación y verificar la identidad de las personas.

Las Disposiciones PLD/FT no contemplan la forma en que las Entidades deben verificar la autenticidad de los documentos, sin embargo, establecen que se considerarán como documentos válidos de identificación personal, la licencia de conducir y las credenciales emitidas por autoridades federales o equivalentes del país de que se trate. La verificación de la autenticidad de los documentos será responsabilidad de las Entidades. Además, establecen que cuando los documentos de identificación proporcionados presenten tachaduras o enmendaduras, las Entidades deberán recabar otro medio de identificación o, en su defecto, solicitar dos referencias bancarias o comerciales y dos referencias personales, que incluyan el nombre o nombres y apellidos paterno y materno sin abreviaturas, domicilio y teléfono de quien las emita, cuya autenticidad será verificada por las Entidades con las personas que suscriban tales referencias, antes de que realicen aportaciones al capital social de las Entidades, se abra la cuenta o se celebre el contrato respectivo.

(ii) Interacción en tiempo real. En relación con las interacciones en tiempo real, es necesario implementar requisitos técnicos y precisos para efecto de llevar a cabo y establecer facultades suficientes para que el Oficial de Cumplimiento pueda determinar si la interacción es válida o si existen elementos de fraude. Pueden y deben integrarse en el Manual de Cumplimiento de las Entidades elementos adicionales que permitan establecer la identidad de la persona: por ejemplo, la exhibición de una fotografía o de un documento (además del código de un solo uso que exige el Anexo 2). Asimismo, es necesario capacitar y dar pautas al personal que hará la interacción.

(iii) Autenticación de Documentos. Además de las reglas para autenticar y validar credenciales emitidas por INE y el CURP, para efecto de robustecer su proceso, la

Entidad puede realizar no solo la validación en fuentes públicas y bases de datos existentes que proporcionan información detallada sobre documentos de identidad, sino también utilizar procedimientos que identifiquen si otras características de los documentos podrían ser objeto de falsificación, por ejemplo, numerales, características de las fotografías. Asimismo, lo anterior se puede complementar con minería de datos y análisis de redes sociales, geolocalización de IP (es decir las coordenadas geográficas de latitud y longitud en que se encuentre el dispositivo), entre otros.

Un ejemplo de forma de autenticación es mediante el escaneo de códigos QR con la cámara de dispositivos móviles que algunos documentos de identificación oficial, como la credencial de elector, ya incluyen.

(iv) Comunicaciones. Las comunicaciones establecidas para realizar el proceso de identificación deben ser seguras, es decir, incluir los protocolos necesarios para garantizar la autenticidad e integridad de la información y documentos que viajan por el sistema de la Entidad.

» *La cuenta por la cuenta*

¿Y ahora qué? La apertura remota de una cuenta obedece a una necesidad particular. La gente no requiere de la prestación de servicios sólo porque sí: tiene que haber una razón, un ahorro de tiempo, de esfuerzo que esté detrás de la búsqueda de un tercero, en este caso, las Entidades. Asimismo, abrir por abrir una cuenta a distancia, en principio parece un esfuerzo poco útil: los montos son reducidos y, como vimos en esta y varias secciones, la regulación establece procesos que deben seguirse de manera específica para efecto de poder aplicar Servicios Electrónicos.

Algunos de los Servicios Electrónicos aquí expuestos pueden combinarse: siempre hay que tener presente que la variedad de actividades que pueden realizar las Entidades puede mezclarse (dentro de los límites financieros y legales que les apliquen) para crear un nuevo producto.

Esta Guía Legal no es un menú de negocios posibles, pero sí de algunas ideas que consideramos pueden inspirar al SACP para innovar.

Por ejemplo, Filipinas, un país con bajo nivel de bancarización y alta penetración de teléfonos móviles, cuenta con casos de éxito interesantes. GCash es una aplicación móvil ofrecida por Globe Telecom (un prestador de servicios de telecomunicaciones en ese país) a los sectores de menos ingresos de ese país. Esta aplicación ha permitido a sus usuarios convertir sus celulares en auténticas carteras de pago digital. Entre las características de dicha aplicación, se encuentran de manera importante:

- La capacidad de enviar y recibir dinero de otros usuarios mediante mensajes, así como realizar compras en línea con ciertos comercios afiliado o habilitados por Globe Telecom.
- Pagos y envío de nómina.
- Implementación de pagos sin necesidad de uso de tarjetas a través de una asociación con Mastercard y American Express.
- Implementación de servicios de ahorro bajo la marca "GSave" en alianza con una entidad bancaria filipina.

En este supuesto, pensamos que la apertura remota de cuentas puede servir como el principio de una nueva relación con los clientes o Socios de las Entidades, permitiendo que a través de la cuenta de depósito la misma permita actividades complementarias similares a las que GCash ha logrado extender por Filipinas, con gran éxito. Una de las fortalezas de GCash es su fuerte y extendida red de alianzas para efecto de lograr un impacto innovador mucho mayor. Al respecto, nos extenderemos sobre este tema en la Sección 24, cuando exploremos la posibilidad que tiene el SACP de lograr interacciones con el sector Fintech.

SECCIÓN 14.- ALMACENAMIENTO EN LA NUBE.

El cómputo en la nube, tal como lo define alguno de los principales jugadores en ese mercado es[72] "la entrega de servicios informáticos, incluidos servidores, almacenamiento, bases de datos, redes, software, análisis e inteligencia, a través de Internet ("la nube") para ofrecer una innovación más rápida, recursos flexibles y economías de escala".

El cómputo en la nube es una de las tecnologías de mayor alcance en los próximos años. En el momento de escribir estas líneas, gran parte de las cadenas productivas y la posibilidad de realizar trabajo desde casa tienen su sustento en algún tipo de tecnología en la nube[73]. En el caso de las instituciones financieras, su uso requiere especial cuidado en cuestiones regulatorias en materia de seguridad, procesos operativos, administrativos y de continuidad de negocio.

Se trata de una tecnología que no sólo permite innovar, sino también el ahorro de costos, al permitir que los recursos tecnológicos sean propiedad de un tercero y no repercutan como gastos de capital propios para las Entidades: en los modelos típicos el usuario de la nube sólo paga por los servicios que utiliza, por lo que se puede utilizar infraestructura de terceros con mayor eficiencia y conforme a las necesidades de cada proyecto (pues el servicio se ofrece de manera escalable y muchos casos graduado a los requerimientos de cada usuario de esta tecnología). Los proveedores de tecnología en la nube están capacitados y tienden a innovar de manera rápida, haciendo que sus clientes se beneficien de manera inmediata de esos adelantos. Asimismo, el usuario se beneficia de la experiencia en implementación de sistemas informáticos: equipo renovado continuamente, gestión de seguridad informática más avanzada.

Entre los beneficios del cómputo en la nube se encuentran:

- Permite escalar más rápidamente los servicios de una Entidad sin tener que realizar adquisiciones costosas de equipo propio.

[72] Microsoft Azure. What is cloud computing. (Internet) Consultado en: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

[73] CNR. 10 future cloud computing trends to watch in 2021. (Internet) Consultado en: https://www.crn.com/news/cloud/10-future-cloud-computing-trends-to-watch-in-2021

- Acceso a tecnología novedosa y segura mediante un programa de suscripción, impulsando así una modernización "por sí misma" dentro de las empresas que contratan estos servicios.
- Reducción de procesos manuales debido a la automatización.
- Apoyo en la continuidad del negocio.
- Reducción de riesgos en materia de ciberseguridad.

Pocas instituciones financieras cuentan con una estrategia de implementación de esta tecnología y aún menos han definido un modelo operativo para transferir aplicaciones existentes a la nube y agregar sistemáticamente aplicaciones nuevas.

En muchos aspectos, como se verá más adelante, los mismos principios y reglas para Proveedores Relevantes son aplicables para este tipo de servicios. Ver Sección 15 (Contratación de Proveedores y Comisionistas) y Sección 16 (Prestadores de Servicios Operativos).

14.1 Tipos de servicios en la nube.

Los servicios en la nube, en cuanto a su modelo operativo pueden clasificarse de la siguiente manera[74]:

- Nube pública: una nube pública es un entorno de nube de acceso público que pertenece a un proveedor de nube externo.
- Nube comunitaria: una nube comunitaria es similar a una nube pública, excepto que su acceso está limitado a una comunidad específica de usuarios. La nube comunitaria puede ser propiedad conjunta de los miembros de la comunidad o de un proveedor de nube externo que aprovisione una nube pública con acceso limitado.
- Nube privada: una nube privada es propiedad de una sola organización y permite que una organización utilice la tecnología de computación en la nube como un

[74] GlobalDots. Cloud computing types of clouds. (Internet) Consultado en: https://www.globaldots.com/blog/cloud-computing-types-of-cloud

medio para centralizar el acceso a los recursos de tecnología de la información por diferentes partes, ubicaciones o departamentos de la organización.

- Híbrido: una nube híbrida es un entorno de nube compuesto por dos o más modelos de implementación de nube diferentes. Por ejemplo, un usuario de nube puede optar por implementar servicios en la nube para procesar datos confidenciales en una nube privada y otros servicios en la nube menos sensibles en una nube pública.

Por su parte los modelos de prestación de servicios son los siguientes:

- Software como servicio (SaaS): en este supuesto el programa es propiedad de uno o más proveedores y es entregado y administrado de forma remota. El proveedor entrega software basado en un conjunto de códigos comunes y definiciones de datos que son consumidos en un modelo de uno a muchos (*one too many*) sobre una base de pago por uso o suscripción.
- Plataforma como servicio (PaaS): implica un entorno de desarrollo e implementación en la nube, con recursos que permiten a los proveedores de la nube entregar aplicaciones específicas y habilitadas (en algunos casos mediante la apertura de módulos adaptados para cada necesidad). Bajo este modelo las Entidades serían las encargadas de desarrollar aplicaciones para sus consumidores (por ejemplo, algún Servicio Electrónico) y los proveedores de servicios en la nube se hacen responsables de todos o una parte importante de los procesos relacionados con ello.
- Infraestructura como servicio (IaaS). Bajo este modelo, una Entidad en lugar de comprar servidores y centros de datos, alquilan a un proveedor de servicios en la nube dicho servicio. Las soluciones IaaS brindan la infraestructura subyacente para las aplicaciones PaaS y SaaS permitiendo gran flexibilidad para configurar y administrar sus propios sistemas.

Desde luego, el contenido de esta Guía Legal es exponer de manera lo más neutral e informativa posible las opciones legales de las Entidades para efecto de avanzar en proyectos de digitalización, también es innegable que existen proveedores que son predominantes en la industria. No es una lista limitativa, pero consideramos que es necesario que las Entidades los conozcan. Estos proveedores de servicios en la nube (PSS) cuentan con servicios muy desarrollados a entidades financieras:

- Amazon Web Services (AWS): es el proveedor más grande con el 27% del mercado e infraestructura instalada a nivel mundial.
- Microsoft Azure: proveedor con un dominio muy importante en la industria del software con servicios de integración fáciles de usar.
- Google Cloud Services: actualmente es el líder mundial en motores de búsqueda, que ofrece herramientas basadas en IA y apuesta por estándares abiertos.

14.2 Tipo de Información y Procesos.

La nube tiene aplicaciones varias por lo que no es posible realizar una planeación única para los servicios en la nube, sin embargo, existen áreas definidas donde la misma puede ser de utilidad, entre las que se encuentran:

- Core bancario (proceso completo desde el *front* hasta el *back office*).
- Procesos de crédito.
- Facturación.
- Control y administración de cobranza.
- Administración de fondos.
- Cumplimiento normativo.
- Administración de riesgos.
- Servicios de atención al cliente.
- Detección de operaciones que pudieran estar relacionadas con delitos LD/FT.

14.3 Evaluación de necesidades de la Entidad.

Desarrollar un modelo operativo interno o contratar a un tercero que se especialice en cómputo en la nube es un paso importante. Para ello es necesario entender el tipo de infraestructura que se busca, los requisitos de seguridad mínimos (Sección 8), así como el tipo de aplicación o de Servicio Electrónico que utilizará la tecnología. El modelo de las Entidades debe incluir una forma de medir el retorno de la inversión (ROI) de este cambio en su tecnología. El modelo operativo debe reflejar la manera en que el cómputo en la

nube facilita o crea procesos comerciales o brinda acceso a nuevos mercados, entre otros temas.

Las Entidades necesitan desarrollar una comprensión clara de la manera en que funcionan las aplicaciones actuales y los detalles de transferir su operativa a la nube. La Entidad puede comenzar con una evaluación detallada de los sistemas existentes, las fallas y la rentabilidad de migrar sus sistemas.

Desde nuestro punto de vista hay dos desafíos para las instituciones financieras cuando trabajan en su estrategia de cómputo en la nube:

- Seguridad.
- Regulación.

Por normativa, las Entidades no pueden permitir una filtración de datos (ver Secciones 5, 8 y 9 de la presente Guía Legal). Manejan datos de clientes cuya confidencialidad está protegida por la ley y, en muchas ocasiones, tienen modelos de negocio que no pueden ser objeto de divulgación al representar una ventaja competitiva. A esta fecha, la industria de la nube (al contrario de lo que ocurre con las instituciones financieras) no cuenta con estándares de seguridad tan definida para el tratamiento de los datos personales y financieros. Esto ha sido un gran reto, sobre todo, en el mundo Fintech, donde los procesos de autorización que se han desarrollado en estos últimos dos años han requerido de la intervención e integración de este tipo de tecnologías, generando la necesidad de que existan obligaciones específicas para el mercado mexicano por parte de los Reguladores. Uno de los temas importantes es la localización de los servidores o "residencia de la información" (Ver Sección 16 Prestadores de Servicios Operativos). Las Entidades deben comprender cómo y dónde se almacenan sus datos, si están en servidores compartidos y las medidas de seguridad que rodean a los mismos.

Por otra parte, si bien esta tecnología, tiene muchas ventajas, también presenta riesgos que deben ser analizados al momento de incorporarla. Entre ellos se encuentran:

- Dificultad para realizar la cancelación de datos cuando la Entidad lo considere necesario.

- Persistencia de algunos riesgos cibernéticos en las aplicaciones en la nube.
- Uso de una sola tecnología puede generar dependencia de la misma y ocasionar problemas cuando la misma se vuelva incosteable, riesgosa o anticuada.

14.4 Diagrama de Trabajo.

La implementación de un modelo de cómputo en la nube bajo un esquema SaaS, requiere de un plan de Proyecto que considere, por lo menos, los siguientes aspectos:

- Análisis, en esta etapa el área de sistemas de la Entidad se encarga de analizar los usuarios de los procesos que se piensan llevar a la nube, sistemas, aplicaciones y procesos comerciales, así como las necesidades particulares de la Entidad de los servicios de la nube. Se trata de recopilar de datos. Ello puede incluir: entrevistar a la parte responsable de la infraestructura tecnológica, programadores, analistas y demás personas que tienen a su cargo esa responsabilidad en la Entidad. Luego, se debe analizar la infraestructura tecnológica existente y se registran los dispositivos y aplicaciones relacionados. Sobre la base de los resultados de la recopilación de datos, el análisis se puede continuar utilizando metodologías técnicas para determinar las capacidades y necesidades clave de la Entidad. Es importante establecer en este punto las necesidades genéricas del servicio, si bien los aspectos técnicos pueden acordarse con posterioridad.
- Diseño, en esta fase se realiza una evaluación comparativa entre los posibles proveedores y se lleva a cabo la elección de la plataforma a utilizar, la infraestructura en la nube, los planes financieros, la seguridad y la preparación para adoptar este proyecto. La Entidad realizará la selección de la tecnología en la nube. La selección ocurre en este punto y se refiere a los resultados de la etapa de análisis anterior. En este punto se realiza la planificación de costos con base en la tecnología ubicada en la nube que se ha seleccionado y el diseño del proceso de adopción y migración. Esta etapa es recomendable utilizar un modelo de proyecto piloto o prueba de concepto para determinar la efectividad de la implementación de la computación en la nube. Esta etapa también determina qué aplicaciones experimentarán el proceso de migración a la nueva infraestructura.

- Contratación, requiere que se revisen los supuestos y procesos mencionados en la Sección 15 **(Contratación de Proveedores y Comisionistas)** de la presente Guía Legal, para efecto de requerir todos los temas técnicos y preparar el proceso de autorización de CNBV, según corresponda.
- Adopción, integra las aplicaciones con la plataforma e infraestructura en la nube. La fase de adopción es una fase preparatoria donde, de preferencia, un asesor externo prepara para la infraestructura en la nube. Comienza seleccionando el software y configurando el servidor con las especificaciones de hardware recomendadas y realizando la implementación correspondiente.
- Migración, asegura que la aplicación y la migración de datos se realicen según lo planeado en la etapa de diseño. La fase de migración también se puede llamar como núcleo del proceso de adopción de la computación en la nube. Mover las aplicaciones y procesos de un servidor físico a un servidor virtual plantea retos importante.
- Gestión, se realiza la documentación para asegurar la continuidad del soporte para futuros sistemas. Una vez que se ha realizado el proceso de adopción y migración, comienza esta etapa. Se deben proporcionar accesos de gestión a las partes que estarán a cargo de implementar el programa. Se deben realizar cambios a los Manuales y documentar procesos nuevos y estar en contacto continuo con el proveedor para efecto de entender el alcance y demás elementos del servicio.

Diagrama de trabajo para almacenar información en la nube

Gráfica 13. Diagrama de trabajo para almacenar información en la nube. Fuente: Vite Abogados

14.5 Reguladores.

En este caso la intervención de CNBV es importante, por la naturaleza de los servicios en la nube y los tipos de procesos que normalmente se llevan a cabo hacen que los proveedores de cómputo en la nube se ubiquen dentro del supuesto de Proveedores Relevantes y, por lo tanto, se tenga que dar aviso o solicitar autorización a la CNBV (Ver Sección 15 Contratación de Proveedores y Comisionistas). Sin embargo, debe hacerse un análisis legal cuidadoso antes de determinar si la regulación es aplicable o no a la Entidad y, en su caso, realizar de forma previa una consulta al Regulador para tomar una decisión. Este análisis debe comenzar por lo siguiente:

- Se debe establecer el tipo de información que será objeto del tratamiento en la nube y clasificarla por el tipo de dato (personal o no), así como determinar si la misma está protegida por el secreto financiero.
- Considerar si la información será parte o no de procesos esenciales administrativos u operativos de la Entidad.
- Verificar si la descripción del servicio es un Servicio Excluido.
- Revisar si el manejo y visibilidad de la información será compartida entre el potencial proveedor y la Entidad o si la ésta será la única que esté en control de la misma.
- Analizar si la información es indispensable para completar procesos que inciden directamente en la continuidad del negocio de la Entidad.

14.6 Temas prácticos y recomendaciones.

Para una adecuada implementación del cómputo en la nube, sugerimos atender, entre otras, las siguientes recomendaciones:

- Identificación de Datos. Identificar claramente los datos y los procesos administrativos y operativos que pasarán a la nube, haciendo una distinción entre información financiera (datos personales, sensibles o financieros), datos estratégicos para la Entidad y verificar que no exista transferencias de datos que no sean del conocimiento de la Entidad. Verificar si existen elementos legales

necesarios para dar el carácter de Encargado de datos al proveedor (ver Sección 8 Seguridad y Confidencialidad de la Información).

- Identificar requisitos técnicos y legales. Definir los propios requisitos técnicos y legales es necesario debido a que existen en el mercado existen muchas ofertas en la nube que son "estándar" para todos clientes y no cumplen con una especificación particular, sobre todo si es considerado Proveedor Relevante (ver Sección 15 Contratación de Proveedores y Comisionistas). Es necesario revisar (i) si el tratamiento de la información se hará en México o en el extranjero (pues ello tiene incidencia en el proceso que debe desahogarse ante CNBV), garantía de seguridad y confidencialidad, entre otros, tal como se han expuesto en otras secciones de la presente Guía Legal, (ii) limitaciones prácticas para su uso al interior de la Entidad, (iii) limitaciones técnicas (interoperabilidad con sistemas originales), y (iv) garantía sobre nivel de servicio y continuidad.

- Análisis de riesgos. Realizar un análisis de riesgos completo para definir las medidas de seguridad que se exigirán al proveedor del servicio. Existen metodologías técnicas que un profesional independiente podría aplicar para ello y la selección tanto de la metodología técnica, como del profesional siempre debe ir acompañado de una explicación de las prioridades de la Entidad. El análisis debe contener riesgos de dependencia respecto al proveedor (imposibilidad técnica o legal de cambiar a otro proveedor cuando se requiera o se desee), posibilidad de acceso no autorizado de los datos protegidos por la Entidad, identificación de subcontratistas en la prestación del servicio (que podrían representar un riesgo para la Entidad), temporalidad de la retención de datos de la Entidad, niveles de servicio o garantías de continuidad.

- Claridad sobre el Servicio. Como comentamos, existen diversas variedades de cómputo en la nube: SaaS, PaaS, IaaS, así como maneras diversas de prestar el servicio (público, híbrido, comunitario o privado) por lo que la elección de la más adecuada es un ejercicio esencial. De otro modo, la Entidad podría encontrase en un esquema o entorno que no necesita o que incumple algunos aspectos regulatorios aplicables que en este caso serían los mismos que para Proveedores Relevantes que hemos mencionado en la Sección 16 **(Prestadores de Servicios Operativos)** [75].

[75] Disposiciones Generales SOCAP y Disposiciones Generales SOFIPO.

- Contratación. Una vez identificados los datos, los requisitos técnicos y legales y realizado el análisis de riesgos, el contrato o contratos que documenten la relación entre la Entidad y el proveedor, deben contener, en nuestra opinión los siguientes elementos mínimos:

    - Cumplimiento con las normas y clausulado mínimo exigido por CNBV para estos Contratos Sección 16 (Prestadores de Servicios Operativos).
    - Clausulado relacionado con la protección de datos personales y manejo de información de los clientes.
    - Obligaciones de reportar incidentes de accesos no autorizados o incidentes de seguridad similares.
    - Restricciones o supuestos de subcontratación, así como los supuestos donde deberá notificarlo a la Entidad.
    - Obligación de replicar clausulados mínimos obligatorios en materia regulatoria Sección 16 **(Prestadores de Servicios Operativos)** y en materia de protección de datos en los supuestos donde se permita la subcontratación.
    - Periodo de almacenamiento de datos y obligación de realizar la cancelación respectiva cuando haya pasado cierto límite legal o convencional o cuando el servicio deje de prestarse.
    - Obligación del prestador de servicio de cooperar con la Entidad en el cumplimiento de la regulación aplicable a ésta.
    - Posibilidad de realizar auditoría y/o requerir información sobre la manera en que se están llevando a cabo los procesos en cumplimiento del contrato y de las normas aplicables.
    - Declaraciones sobre las ubicaciones de los servidores donde se procesará la información, así como que se trata de jurisdicciones que otorgan un nivel de protección mínimo a los datos transferidos.
    - Informar en cuanto sea posible a la Entidad sobre cualquier requerimiento judicial o administrativo que pueda afectar materialmente la prestación de los servicios.
    - Obligaciones a cargo del prestador de servicios relacionadas con el cumplimiento de estándares de seguridad mínimos.

- Mencionar la existencia de políticas de seguridad de parte del proveedor de servicios, incluyendo medidas de acceso y mantenimiento de sistemas.
- Mención de las medidas técnicas que garantizarán la disponibilidad, integridad y confidencialidad de los datos (encriptación, manejo de claves de acceso, entre otros).
- Penalidades relacionadas con los niveles de servicio y los supuestos en que serán pagaderas a la Entidad.

- Preparar el Seguimiento. La implementación de un sistema en la nube implicará el cambio en los procesos de manera continua, por lo que debe existir preparación suficiente de parte del equipo interno de la Entidad que operará éstos.

SECCIÓN 15.- CONTRATACIÓN DE PROVEEDORES Y COMISIONISTAS.

Las Entidades pueden contratar con terceros, incluyendo a otras entidades financieras, la prestación de servicios necesarios para su operación, así como comisiones para realizar las operaciones que les son propias de acuerdo con su Nivel de Operaciones de conformidad a lo que establece la normativa[76]. Este tipo de comisionistas y prestadores de servicios (que para efectos de esta Guía Legal hemos denominado Proveedores Relevantes) por la importancia e impacto que tienen dentro de las Entidades deben cumplir con un conjunto de reglas y procesos previo a realizar la contratación adecuada de los mismos.

15.1 Contratos Regulados y no Regulados.

Las reglas para Proveedores Relevantes no serán aplicables cuando las Entidades contraten los servicios que se indican a continuación (Servicios Excluidos):

(i) Los servicios profesionales o de asesoría incluyendo mandatos y comisiones, salvo que estos últimos sean para la realización de las operaciones principales de las Entidades, entre las cuales (y dependiendo de su Nivel de Operaciones) destacan:

[76] Disposiciones Generales SOCAP y Disposiciones Generales SOFIPO.

- Recibir depósitos de dinero a la vista, de ahorro, a plazo, retirables en días preestablecidos y retirables con previo aviso.
- Recibir préstamos y créditos.
- Expedir y operar tarjetas de débito y tarjetas recargables.
- Otorgar su garantía al Fondo de Protección.
- Otorgar préstamos o créditos a sus Socios o clientes.
- Otorgar créditos o préstamos de carácter laboral a sus trabajadores.
- Descontar, dar en garantía o negociar títulos de crédito, y afectar los derechos provenientes de los contratos de financiamiento que realicen con sus Socios clientes.
- Constituir depósitos a la vista o a plazo en instituciones de crédito.
- Realizar inversiones en valores gubernamentales, bancarios y de sociedades de inversión en instrumentos de deuda.
- Recibir o emitir órdenes de pago y transferencias.
- Fungir como receptor de pago de servicios por cuenta de terceros, siempre que lo anterior no implique la aceptación de obligaciones directas o contingentes.
- Realizar la compraventa de divisas en ventanilla por cuenta propia.

(ii) Los servicios auxiliares y complementarios que la Entidad obtenga de las sociedades en las que invierta para que le presten servicios complementarios, auxiliares o inmobiliarios.

(iii) La manufactura, envío a domicilio o distribución de tarjetas de débito, crédito o recargables inactivas.

(iv) El traslado de valores.

(v) La recuperación de cartera

(vi) Mantenimiento de equipos y sistemas de cómputo en red.

(vii) Los servicios relacionados con la administración, tales como limpieza, seguridad, mensajería y correspondencia, almacenamiento y resguardo físico de información y documentación, entre otros.

(viii) El procesamiento de operaciones crediticias en su fase de promoción y evaluación.

(ix) Recepción de pagos de contribuciones federales, estatales, municipales y las correspondientes a la Ciudad de México, en efectivo o con cargo a tarjetas de crédito o débito.

Es preciso tomar en cuenta que tanto en los servicios referidos en las fracciones anteriores, como en aquellos que se refieren a Proveedores Relevantes, las Entidades deberán cuidar en todo momento que las personas que les proporcionen los servicios asuman obligaciones de confidencialidad de la información relativa a las operaciones activas, pasivas y de servicios celebradas con sus Socios o clientes, así como la relativa a estos últimos, en caso de tener acceso a ella.

Asimismo, las citadas Entidades deberán mantener los datos de las personas que les proporcionen tanto Proveedores Relevantes como proveedores ordinarios en un "padrón de prestadores de servicios".

15.2 Reglas comunes de Proveedores Relevantes

Las Entidades, salvo que se trate de Servicios Excluidos, para contratar cualquiera de los servicios o al celebrar cualquiera de las comisiones mercantiles con un Proveedor Relevante, deberán cumplir con los requisitos siguientes:

(i) Tratándose de actividades que impliquen actuar frente a sus Socios o clientes, en todo momento, los terceros que la Entidad contrate deberán actuar a nombre y por cuenta de esta última, por lo que la citada relación deberá documentarse mediante contratos de comisión mercantil.

En ningún caso dichos comisionistas podrán llevar a cabo aprobaciones y aperturas de cuentas de operaciones activas, pasivas y de servicios, salvo que se trate de las operaciones de los Servicios de Comisionistas que se mencionan más adelante.

(ii) Contar con un informe que especifique:

- Procesos operativos o de administración de bases de datos y sistemas informáticos de la Entidad que sean objeto de los servicios o comisiones a contratar.
- Los criterios y procedimientos para seleccionar al tercero. Dichos criterios y procedimientos estarán orientados a evaluar la experiencia, capacidad técnica y recursos humanos del tercero con quien se contrate para prestar el servicio con niveles adecuados de desempeño, confiabilidad y seguridad, así como los efectos que pudieran producirse en una o más operaciones que realice la propia Entidad.

(iii) Contar con planes para evaluar y reportar al Consejo de Administración, al Comité de Auditoría, al Auditor Interno o al Director General de la Entidad, según la importancia del servicio contratado, el desempeño del tercero o comisionista, así como el cumplimiento de la normativa aplicable a dicho servicio.

(iv) Tratándose de servicios de procesamiento de información, la Entidad deberá practicar al menos cada dos años, auditorías que tengan por objeto verificar el grado de cumplimiento de la normatividad conforme a los lineamientos que se establecen en la misma. CNBV puede ordenar la realización de la auditoría con anticipación a dicho periodo, cuando a su juicio existan condiciones de riesgo en materia de operación y seguridad de la información.

(v) El Director o Gerente General, el Comité de Auditoría, así como el Auditor Interno de la Entidad deben definir y vigilar, acorde a su competencia, el cumplimiento de los mecanismos para el adecuado manejo, control y seguridad de la información generada, recibida, transmitida, procesada o almacenada en la ejecución de los servicios o comisiones que se refieran a la utilización de infraestructura tecnológica, de telecomunicaciones o de procesamiento de información, que se realicen parcial o totalmente fuera del territorio nacional.

(vi) Establecer los criterios que permitan a las Entidades, a través de su Director o Gerente General, evaluar la medida en que las contrataciones pudieran afectar cualitativa o

cuantitativamente las operaciones que realice la Entidad, conforme a su objeto, tomando en cuenta para determinar tal circunstancia, lo siguiente:

- La capacidad de la Entidad para, en caso de contingencia, mantener la continuidad operativa y la realización de operaciones y servicios con sus Socios o Clientes.
- La complejidad y tiempo requerido para encontrar un tercero que, en su caso, sustituya al originalmente contratado.
    (a) La limitación en la toma de decisiones que trasciendan en forma significativa en la situación administrativa, financiera, operacional o jurídica de la Entidad.
    (b) La capacidad de la Entidad para mantener controles internos apropiados y oportunidad en el registro contable, así como para cumplir con los requerimientos regulatorios en caso de suspensión del servicio por parte del tercero o comisionista.
    (c) El impacto que la suspensión del servicio tendría en las finanzas, reputación y operaciones de la Entidad.
    (d) La capacidad de la Entidad de participar eficientemente en el sistema de pagos.
    (e) La vulnerabilidad de la información relativa a los Socios.

El Director General de la Entidad es responsable de aprobar las políticas y criterios para seleccionar a los terceros o comisionistas que contrate la Entidad, en términos de lo anterior. Asimismo, el Director General será responsable de la implementación de dichas políticas y criterios.

15.3 Corresponsalías (Comisiones).

Conforme los ha definido la propia CNBV[77], el corresponsal bancario es un tercero que establece relaciones o vínculos de negocio con una institución de crédito (en este caso una Entidad) con objeto de ofrecer, a nombre y por cuenta de ésta, servicios financieros a

[77]CNBV. Modelos de negocio para la inclusión financiera 1. (Internet) Consultado en: https://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Modelos%20de%20Negocio%20para%20la%20IF/1%20Corresponsales%20Bancarios.pdf

sus clientes. Lo anterior, por ejemplo, en el caso de establecimientos comerciales habilitados para prestar servicios financieros ofrecidos por una entidad financiera. Este tipo de esquema se ha convertido, en varios países, en un modelo benéfico debido a que:

- Ofrece una forma de llegar a sectores informales de la economía.
- Es rentable, pues aprovecha las capacidades de un tercero para llegar a nuevos mercados.
- Potencial de aumentar la actividad y número de operaciones de los clientes o Socios.

15.4 Tipos de corresponsales.

En ese sentido, conforme al artículo 17 Bis 36 de las Disposiciones Generales SOCAP y el artículo 265 Bis 36 de las Disposiciones Generales SOFIPO, las Entidades pueden celebrar contratos de comisión mercantil (corresponsalías) con terceros que actúen en todo momento a nombre y por cuenta de aquellas para la realización de las operaciones siguientes:

Tipo de Actividad	Autorización de CNBV[78]	Límite
Pagos de servicios en efectivo, con cargo a tarjetas de crédito o débito.	Sí	
Recepción de pagos de contribuciones federales, estatales, municipales y las correspondientes a la Ciudad de México, en efectivo o con cargo a tarjetas de crédito o débito.	No	
Retiros de efectivo efectuados por el propio Socio o cliente titular de la cuenta respectiva, o por las personas autorizadas en cuentas de depósito o inversión conforme a la ley.	No, sólo un aviso.	1,500 UDIs por cada tipo de inversión y cuenta
Depósitos en efectivo, en cuentas propias o de terceros.	No	Monto diario mínimo equivalente a 4,000 UDIS por cuenta. Monto mensual equivalente al 50% del importe total de las operaciones realizadas en el

[78] Artículo 17 Bis 37 Disposiciones Generales SOCAP y artículo 265 Bis 37 Disposiciones Generales SOFIPO.

Tipo de Actividad	Autorización de CNBV[78]	Límite
		periodo por la Entidad.
Pagos de créditos a favor de la propia Entidad o de otra en efectivo, con cargo a tarjetas de crédito o débito.	Sí	
Orden de pago en las sucursales de las Entidades comitentes, o bien, a través de los propios comisionistas, así como transferencias entre cuentas, incluso a cuentas de otras Entidades o instituciones de crédito.	Sí	
Poner en circulación tarjetas de débito y recargables. En este caso las Entidades deben comprobar fehacientemente que los comisionistas contarán con los controles necesarios para preservar la confidencialidad de la información de sus Socios o clientes.	Sí	
Consultas de saldos y movimientos de cuentas y de tarjetas de crédito, débito y recargables.	Sí	
Realizar la apertura de cuentas de depósito de Bajo Riesgo.	Sí	

Tabla 7. Tipos de Actividad

En todo caso las operaciones referidas únicamente podrán efectuarse en moneda nacional.

Asimismo, existen reglas específicas para la realización de cada tipo de operación a través de comisionistas, mismas que deben ser revisadas previo a la implementación de cada esquema.

15.5 Requisitos de Contratación.

Las Entidades, en aquellos casos en los que sea necesario obtener su autorización conforme a la sección anterior, deberán presentar a la CNBV una solicitud de autorización adjuntando un "Plan Estratégico de Negocios" para llevar a cabo las operaciones correspondientes, con cuando menos veinte días hábiles de anticipación a la fecha en que pretendan contratar las comisiones respectivas.

El Plan Estratégico de Negocios debe contener:

- Documentación que incluya: (i) un informe que especifique los procesos operativos o de administración que llevarán a cabo los comisionistas, (ii) políticas y procedimientos para vigilar el desempeño del tercero o comisionista y el cumplimiento de sus obligaciones contractuales, (iii) planes para evaluar y reportar al Consejo de Administración, al Comité de Auditoría, al Auditor Interno o al Director o Gerente General de la Entidad el desempeño del comisionista y (iv) criterios que permitan a la Entidad a través de su Director General, evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones que realice la Entidad.
- Modelos de contratos de comisión mercantil, que las Entidad utilizaría para establecer las respectivas relaciones jurídicas con su comisionista.
- Descripción de los procesos y sistemas que implementaría la Entidad para la realización de las operaciones.
- Descripción de los Medios Electrónicos que utilizarán las Entidades para garantizar la correcta ejecución de las operaciones y de seguridad de la información de los Socios o Clientes, para lo cual deberán cumplir con los requerimientos técnicos para la operación de Medios Electrónicos que establece la regulación.
- Políticas y procedimientos que implementaría la Entidad, para acreditar la capacidad de los comisionistas.
- Políticas y procedimientos para la administración de los Factores de Autenticación de Socios y operadores que prevengan el uso indebido de los Factores de

Autenticación por parte de sus comisionistas o los empleados de estos. Dichas políticas y procedimientos deberán contemplar un programa de capacitación permanente de los comisionistas, así como las medidas y controles necesarios para asegurar la integridad de los Factores de Autenticación de los Socios o clientes y operadores.

- Medidas que deberá instrumentar la Entidad en materia de:

  (a) Control interno.
  (b) Administración integral de riesgos.
  (c) Seguridad para la prevención de operaciones de lavado de dinero o financiamiento al terrorismo.
  (d) Dotación de efectivo a sus comisionistas en los puntos de atención al público.

- Características de los terceros con los que la Entidad contrataría comisiones mercantiles al amparo de la presente sección, así como la indicación de los volúmenes de operación estimados.
- Programa que describa las distintas etapas de implementación de las operaciones que se realicen a través de los comisionistas.
- Estudio de sustentabilidad y rentabilidad del modelo de negocio que las Entidades llevarán a cabo con los comisionistas.
- Documentación de los controles automatizados para efecto de monitorear los límites de cada tipo de servicio prestado a través de los comisionistas.

Una vez autorizado por la CNBV el Plan Estratégico de Negocios, la Entidad deberá solicitar a la CNBV autorización respecto de las reformas que impliquen cambios sustanciales a los términos en los que realizarían las operaciones con los Socios o Clientes, o bien, cambios que incidan en el volumen de las operaciones realizadas a través de los comisionistas que, en su caso, pretendan efectuar al referido plan con, por lo menos, treinta días naturales de anticipación a la fecha en que se pretenda que surtan efectos.

En el caso de comisionistas contratados para realizar retiros de efectivo por el propio Socio o Cliente titular de la cuenta respectiva, o por las personas autorizadas en cuentas de depósito o inversión conforme a la ley, sólo debe presentarse un aviso suscrito por el

Director General de la Entidad; sin embargo, también debe presentarse el Plan Estratégico de Negocios.

15.6 Informe Anual

Las Entidades deben elaborar un informe anual respecto de la evolución que guarda el plan estratégico de negocios; dicho informe contendrá información cualitativa y cuantitativa respecto de la implementación de lo señalado en la sección anterior, e incluirá un reporte detallado sobre las contingencias que, en su caso, se hubieren presentado respecto de la prestación de servicios de los comisionistas. El informe debe ser entregado a la Comisión, en el transcurso del primer trimestre de cada año.

15.7 Obligaciones Adicionales.

Las Entidades en la implementación de las comisiones mencionadas, deberán ajustarse a lo siguiente[79]:

- Celebrar un contrato de depósito con el comisionista. Al efecto, la Entidad puede otorgar al comisionista, una línea de crédito que permita proveer de fondos a la citada cuenta de depósito, cuando resulte necesario y de acuerdo a las políticas de la propia Entidad. Si bien en ciertos casos, previa aprobación de CNBV, se puede dispensar este requisito.
- La Entidad debe asegurarse de que cada operación tenga correspondencia con los cargos y abonos que se efectúen a las cuentas mencionadas.
- Verificarán que los comisionistas informen por cualquier medio a los Socios o Clientes, que actúan a nombre y por cuenta de la Entidad.
- Adicionalmente, las Entidades deben proporcionar a sus Socios o Clientes, según se trate de una SOCAP o una SOFIPO, un número telefónico al que podrán llamar a fin de conocer los comisionistas con los que la Entidad hubiese contratado. Asimismo, las Entidades deben asegurarse de que sus comisionistas coloquen en sus establecimientos de manera visible, el referido número telefónico.

[79] Artículo 17 Bis 39 Disposiciones Generales SOCAP y artículo 265 Bis 39 Disposiciones Generales SOFIPO.

- Entregarán de manera continua y permanente a los comisionistas, la información que las Entidades deban proporcionar a sus Socios o Clientes, según se trate de una SOCAP o una SOFIPO, por las transacciones realizadas, a efecto de que tales comisionistas, a su vez, la proporcionen a los Socios o Clientes.
- Las Entidades a través de los comisionistas, deberán proporcionar la información suficiente para que sus Socios o Clientes conozcan el procedimiento para presentar aclaraciones o quejas derivadas de operaciones realizadas por medio de los citados comisionistas.
- Implementar sistemas y procedimientos operativos que permitan una gestión adecuada del servicio que presten a través de comisionistas.
- Mantener plenamente identificadas en todo momento, las operaciones que realicen a través de comisionistas de manera independiente de las que realicen a través de sus propias oficinas.

15.8 Clausulado del Contrato de Comisión.

15.8.1 Clausulado Regulatorio

El contrato de los Proveedores Relevantes debe contener, conforme al artículo 17 Bis 35 de las Disposiciones Generales SOCAP y al artículo 265 Bis 35 de las Disposiciones Generales SOFIPO, el presente clausulado:

- La obligación del Proveedor Relevante de recibir visitas domiciliarias por parte del auditor externo de la Entidad, del Comité de Supervisión Auxiliar o de la CNBV o terceros que la propia CNBV designe para ello, a efecto de llevar a cabo la supervisión correspondiente, con el exclusivo propósito de obtener información para constatar que los servicios o comisiones contratadas por la Entidad, le permiten a esta última cumplir con las disposiciones de la ley que le resultan aplicables.
- Aceptar la realización de auditorías por parte de la Entidad, en relación con los servicios o comisiones objeto de dicho contrato, a fin de verificar la observancia de las disposiciones aplicables a las Entidades.
- Entregar a solicitud de la Entidad, al auditor externo de la propia Entidad y a la CNBV o al Comité de Supervisión Auxiliar, libros, sistemas, registros, manuales

y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitirá que se tenga acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la prestación del servicio en cuestión.

- Informar a la Entidad con por lo menos treinta días naturales de anticipación, respecto de cualquier reforma a su objeto social o en su organización interna que pudiera afectar la prestación del servicio objeto de la contratación.
- Guardar confidencialidad respecto de la información relativa a las operaciones activas, pasivas y de servicios que los comisionistas celebren con los Socios, así como la relativa a estos últimos.

En todo caso hay que tener en mente que los requerimientos de información y, en su caso, las observaciones o medidas correctivas que deriven de la supervisión que realice la CNBV, se realizarán directamente a la Entidad. Asimismo, la CNBV podrá, en todo momento, ordenar la realización de las visitas y auditorías señaladas anteriormente precisando los aspectos que unas y otras deberán comprender, quedando obligada la Entidad a rendir a la Comisión un informe al respecto.

15.8.2 Clausulado Específico.

Tratándose de contratos de comisión mercantil cuyo objeto sea la captación de recursos de Socios y otras operaciones fuera de las oficinas de las Entidades, conforme al artículo 17 Bis 41 de las Disposiciones Generales SOCAP y artículo 265 Bis 41 de las Disposiciones Generales SOFIPO, en adición a las cláusulas regulatorias mínimas mencionadas anteriormente, deben contener:

- Las operaciones que el comisionista llevará a cabo por cuenta de la Entidad.
- Los límites individuales y agregados de las operaciones.
- Las cláusulas aplicables a la línea de crédito que la Entidad otorgará al comisionista, de ser aplicable.
- Los procedimientos que la Entidad utilizará para la identificación del comisionista y de los Socios y Clientes, conforme a los estándares de la

regulación, así como los requisitos operativos y técnicos que deberán cumplirse, tanto por la Entidad como por el comisionista.

- Las sanciones y, en su caso, penas convencionales por los incumplimientos al contrato.
- Los requisitos y características que deberán cumplir las partes en la realización de la comisión.
- La obligación por parte de la Entidad de proveer los medios necesarios a fin de dar cumplimiento a lo dispuesto por la LTOSF y por las demás disposiciones legales que les resulten aplicables en la realización de las operaciones objeto de la comisión, así como de asegurarse de que el comisionista efectivamente cumple lo anterior.
- Las siguientes prohibiciones para el comisionista:
  a. Condicionar la realización de la operación a la adquisición de un producto o servicio (ventas atadas).
  b. Publicitarse o promocionarse de cualquier forma a través de la papelería o en el anverso de los comprobantes que proporcionen a los Socios o clientes a nombre de la Entidad de que se trate.
  c. Realizar la operación objeto de la comisión en términos distintos a los pactados con la Entidad correspondiente.
  d. Subcontratar los servicios relacionados a la comisión mercantil.
  e. Cobrar comisiones, por cuenta propia, a los Socios o clientes por la prestación de los servicios objeto de la comisión mercantil, o bien recibir diferenciales de precios o tasas respecto de las operaciones en que intervengan. Lo anterior, sin perjuicio del pago de comisiones que pueda pactarse entre el Socio y la Entidad entre esta última y el comisionista.
  f. Llevar a cabo las operaciones con los Socios a nombre propio.
  g. Pactar en exclusiva con cualquier Entidad incluida la comitente, la realización de las operaciones y actividades consistentes en la recepción de pago de servicios que ofrezca la Entidad, así como el pago de tarjetas de crédito.

- Límites a los montos y transacciones.
- La facultad de la Entidad para suspender operaciones o dar por terminado el respectivo contrato sin responsabilidad, según lo ordene CNBV conforme a la normatividad aplicable.
- Tratándose de apertura de cuentas de Bajo Riesgo la obligación del comisionista para recabar del Socio o cliente la información necesaria a fin de identificar adecuadamente a los clientes o Socios. Para ello deben transmitir en tiempo y forma a la Entidad la información relativa a las mencionadas operaciones para cumplir con los lineamientos en materia de PLD/FT.

Las Entidades pueden contratar con comisionistas para que les presten de manera exclusiva sus servicios, salvo por ciertas excepciones señaladas anteriormente. No obstante, lo anterior, las Entidades no podrán contratar con terceros que, durante los doce meses inmediatos anteriores a la fecha en que surtiera efectos la respectiva comisión, se hubieren desempeñado como comisionistas exclusivos de otra.

15.9 Comisionistas Prohibidos

Las Entidades no podrán celebrar los contratos de comisión mercantil a que se refiere la presente sección con las personas siguientes[80]:

- Entidades financieras, con excepción de aquellas que dentro de las operaciones que tengan autorizadas se encuentre el poder recibir mandatos o comisiones, así como que tengan permitido realizar las operaciones objeto del mandato o comisión de que se trate, incluidas otras Entidades del SACP y bancos.
- Centros cambiarios.
- Instituciones de asistencia privada y demás sociedades o asociaciones que se dediquen al otorgamiento de préstamos con garantía prendaria, incluyendo casas de empeño.

[80] Artículo 17 Bis 42 Disposiciones Generales SOCAP y artículo 265 Bis 42 Disposiciones Generales SOFIPO.

15.10 Obligaciones Diversas

Obligación	Implementación
Las Entidades son responsables por el servicio que sus comisionistas proporcionen a los Socios o clientes, aun cuando la realización de las operaciones correspondientes se lleve a cabo en términos distintos a los pactados, así como por el incumplimiento a la normatividad.	Aplicación de medidas correctivas por la Entidad.
	Inclusión de clausulado especial dentro del contrato.
Suspender parcial o total, temporal o definitiva, la prestación de los servicios o comisiones a través del tercero, cuando a juicio de la CNBV, pueda verse afectada la estabilidad financiera, la continuidad operativa de la Entidad o en protección de los intereses del público, o bien, cuando las Entidades incumplan con las disposiciones	Programa de regularización a ser autorizado por CNBV
Las Entidades deben contar con un padrón que contenga el tipo y detalle de servicios y operaciones contratadas y de los Proveedores de Relevantes. Al respecto, ponemos a su disposición en el Anexo 2 del presente documento un ejemplo de matriz de contratos para llevar un control sobre los contratos con proveedores.	Cumplir de manera detallada con los datos que deben ingresarse conforme a la regulación.
Presentar a la Comisión y el Comité de Supervisión Auxiliar a los noventa días naturales después del cierre del ejercicio, un informe anual que detalle los resultados de las revisiones efectuadas por la Entidad para cerciorarse de que los	Establecer revisiones adecuadas y políticas relacionadas con la revisión de Proveedores Relevantes.

Obligación	Implementación
prestadores de servicios o comisionistas garantizaron la continuidad del servicio con niveles adecuados.	

Tabla 8. Obligaciones Diversas

15.11 Políticas de Desempeño de Proveedores Relevantes

Las Entidades deben contar con políticas y procedimientos para vigilar el desempeño de los Proveedores Relevantes y el cumplimiento de sus obligaciones contractuales, las cuales deben cubrir los siguientes aspectos:

- Las restricciones o condiciones de subcontratación del servicio.
- La confidencialidad y seguridad de la información de los Socios.
- Las obligaciones de la Entidad y del tercero o comisionista, los procedimientos para vigilar su cumplimiento, así como en su caso, las consecuencias legales en el evento de incumplimiento.
- Los mecanismos para la solución de disputas relativas al contrato de prestación de servicios y comisión.
- Los planes de continuidad del negocio, incluyendo los procedimientos de contingencia en caso de desastres.
- El uso y la explotación a favor de la Entidad sobre las bases de datos producto de los servicios y comisiones.
- El establecimiento de lineamientos que aseguren que los Prestadores de servicios reciban periódicamente una adecuada capacitación e información, en relación con los servicios o comisiones contratados.
- El cumplimiento de los lineamientos mínimos de operación y seguridad que se señalan en la regulación si los servicios o comisiones a contratar se refieren a la utilización de infraestructura tecnológica o de telecomunicaciones.

15.12 Políticas de Evaluación de Proveedores Relevantes

Las Entidades, en sus políticas relativas a la contratación de servicios o comisiones, contemplarán como medidas de evaluación respecto de los servicios o comisiones a

que se refiere este capítulo, lo siguiente:

- La capacidad de los Proveedores Relevantes para implementar medidas o planes que permitan mantener la continuidad del servicio con niveles adecuados de desempeño, confiabilidad, capacidad y seguridad.
- La integridad, precisión, seguridad, confidencialidad, resguardo, oportunidad y confiabilidad en el manejo de la información generada con motivo de la prestación de los servicios o comisiones, así como el acceso a dicha información, a fin de que sólo puedan tener acceso a ella, las personas que deban conocerla.
- Los métodos de la Entidad para evaluar el cumplimiento al contrato correspondiente, o bien, la adecuada prestación de los servicios o comisiones.
- Los criterios y procedimientos para calificar periódicamente la calidad del servicio.
- La capacidad de las Entidades de mantener la continuidad en la prestación de los servicios o comisiones.
- La capacidad de las Entidades, en la administración integral de riesgos para identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos que puedan derivarse de la prestación de los servicios o comisiones a que se refiere este capítulo.
- La capacidad del Sistema de control interno para cumplir con las políticas y procedimientos que regulen y controlen la prestación de los servicios o comisiones a que se refiere este capítulo.

El Consejo de Administración deberá designar a un responsable, que podrá ser el Auditor Interno o el Comité de Auditoría, para que dé seguimiento, evalúe y reporte periódicamente a dicho Consejo de Administración, el desempeño del prestador de servicios o comisionista, así como el cumplimiento de las normas aplicables relacionadas con los servicios o las operaciones correspondientes. Para auxiliar al responsable, ponemos a su disposición un cuestionario de contratación con terceros en el Anexo 5 del presente documento.

El Consejo de Administración deberá revisar cuando menos una vez al año, las políticas de selección de los Proveedores Relevantes y aprobar las modificaciones que sean necesarias con base en los resultados de las evaluaciones realizadas por el responsable de dar seguimiento y evaluar el desempeño de aquellos.

15.13 Proceso ante CNBV.

El proceso de notificación o, en su caso, autorización de un contrato de comisión o corresponsalía tiene como base lo expuesto anteriormente y es desarrollado en detalle en las guías correspondientes emitidas por CNBV[81]. De manera genérica, el proceso regulatorio está compuesto de los siguientes elementos:

- Escrito de solicitud: debe presentarse a la CNBV por lo menos 20 días hábiles de anticipación a la fecha en la que se pretenda celebrar el contrato. Será de formato libre y deberá contener, entre otras cosas, lo siguiente:

    1. Información general relativa a la Entidad.
    2. Información y datos del futuro comisionista.
    3. Operaciones materia de la comisión mercantil y sus límites.
    4. Área geográfica materia de los servicios prestados mediante la comisión.
    5. Plan Estratégico de Negocios, con un desglose de la siguiente información y datos mencionados anteriormente en esta sección.
    6. Anexos del escrito de solicitud (soporte documental para acreditar lo manifestado en el escrito).
    7. Puntos petitorios (de manera expresa la solicitud relativa a la autorización).

- Aviso. Documento suscrito por el Director General donde se mencionen las características de la comisión.

15.14 Acercamiento Inicial.

Como se ha comentado en otras partes de esta Guía Legal, la relación con los Reguladores es de vital importancia para las entidades financieras, sobre todo, para el SACP. Las actividades de las Entidades se encuentran bajo supervisión constante y la interacción con la CNBV es constante. En ese sentido, la construcción de un vínculo productivo es un factor

[81] Guía para la Contratación de Servicios y Guía para la Contratación Comisionistas.

importante en el éxito de un modelo de negocio financiero emprendido por una Entidad. Ante todo, antes de acudir ante CNBV para plantear un Proyecto de corresponsalía, sugerimos un planteamiento una vez que se haya avanzado en esbozar los aspectos más generales (tal como se menciona en la sección siguiente), pues es necesario:

- Proporcionar un grado de información suficiente y conciso para que CNBV pueda tener o expresar alguna opinión sobre el Proyecto propuesto.
- Plantear dudas o comentario concretos a CNBV sobre la viabilidad, aspectos legales y tecnológicos del nuevo Proyecto.
- Preparar documentos (presentación preliminar).
- Establecer una vinculación permanente entre la CNBV y la Entidad para efecto de informar sobre los avances y aspectos accesorios del Proyecto.
- Realizar la comunicación a través de una sola persona encargada de establecer contacto con la CNBV: si bien la participación y retroalimentación de varias áreas es necesaria y deseable, hay que considerar que la falta de coordinación puede resultar en que la CNBV no comprenda en su totalidad el Proyecto planteado.

15.15 Plan de Trabajo Diagrama de Trabajo.

1) Realizar un análisis detallado sobre la necesidad de contar con un comisionista, sobre todo atendiendo:

   a) Oportunidades de negocio identificadas de manera objetiva y alcanzable. El uso de un comisionista debe atender a la necesidad de alcanzar lugares donde la Entidad no tiene presencia física y que a la vez ofrezcan un mercado prometedor. Se deben contrastar escenarios posibles, donde los costos logísticos, de transporte, tecnológicos y operativos permitan evaluar la conveniencia de un modelo de corresponsalía. Todo esto implica una planeación puntual para que la Entidad tenga la mayor información posible sobre el mercado y su situación interna. La identificación de riesgos es esencial para poder atender con posterioridad los requerimientos legales expuestos en las secciones anteriores.
   b) Realizar mapas completos del flujo del dinero a través de los comisionistas y de todo el proceso que implicará su participación. Esto para efecto de modificar los Manuales en las partes correspondientes.

c) Establecer los hechos relevantes y comenzar a planear la evaluación de riesgos.

d) Establecer si el comisionista será una herramienta para que la Entidad preste un servicio novedoso o inexistente en ese momento, o si se trata de ampliar la base de un servicio ya existente mediante el ofrecimiento de un nuevo canal de operación. Esto tiene consecuencias importantes, por ejemplo, para determinar si operan algunas limitaciones: montos para cuentas de Bajo riesgo, identificación de clientes, necesidad de una firma electrónica, entre otros.

e) Análisis del tipo de comisión y de servicio que se estará contratando: ¿Se trata de un Servicio Excluido o de alguna actividad que encaja en su totalidad con las que se han descrito en esta sección? La regulación puede no ser exhaustiva y existen áreas grises donde una clarificación de un asesor externo sea lo más conveniente para poder plantear el alcance del Proyecto adecuadamente.

f) Determinar el tipo de interacción y los resultados que se esperan de un comisionista, respondiendo los siguientes temas:

- Capacidad operativa, administrativa, humana o tecnológica que se requiere del comisionista. Determinar si esa capacidad debe ser propia, subcontratada o proveída por la Entidad.
- Tipo de actividades que desarrollará el comisionista para prestar el servicio para efecto de mantener la continuidad en el servicio (además de llevar a cabo la representación de la Entidad frente al público).
- Capacitación requerida por la Entidad y por el comisionista para efecto de operar procesos tecnológicos relacionados con la prestación del servicio.

g) Determinar la inversión aproximada que tendrá la implementación de prestar un servicio a través de un comisionista, evaluando tanto el impacto como el retorno esperado en razón de dicho modelo de negocio.

2) Diagnóstico sobre las capacidades tecnológicas actuales, así como las requeridas para implementar el modelo y la factibilidad de contar con otro tipo de Proveedor Relevante (Sección 15 Contratación de Proveedores y Comisionistas).

3) Nombramiento de Partes Responsables para elaboración de un plan de trabajo, cronograma.

4) Identificación de necesidades legales para la implementación del proyecto:

a) Requisitos de contratación y operación dependiendo del tipo de Servicio Electrónico que, en su caso, se desee implementar.
b) Limitaciones a manejos de montos.
c) Identificación de necesidades y regulación en materia de protección de datos personales (ver Sección 9 Datos Personales y Secreto Financiero).
d) Identificación de requerimientos y limitaciones en materia de disposiciones PLD/FT.
e) Identificación de estructura contractual de la operación: convenios de confidencialidad, borrador de contrato de comisión mercantil, contratos en materia de protección de datos, así como protección y licenciamiento de propiedad intelectual que requiera el Proyecto.
f) Análisis de los supuestos de comisión (cargos) y tasas de interés (en su caso) a la luz de la LTOSF (Ver Sección 5 (Transparencia y Ordenamiento de los Servicios Financieros)).
g) Borrador de los contratos de adhesión que implementarán la prestación del servicio.
h) Evaluación sobre la necesidad de utilizar una Firma Electrónica (ver Sección 12 Implementación de Firma Electrónica).

5) Sesiones de consulta preliminares entre áreas responsables y Partes Responsables donde intervengan:

a) Área de producto o servicios al cliente.
b) Auditoría Interna.
c) Riesgos.
d) Oficial de Cumplimiento.
e) Área legal.
f) Asesor externo.

Todas las sesiones deben estar guiadas por diagramas explicativos de cada proceso identificado para la prestación de los servicios a ser ofrecidos y administrados a través del comisionista.

6) Diagnóstico de los requerimientos operativos y tecnológicos que será necesario atender.

7) Evaluación de Proveedores Relevantes en materia tecnológica para permitir el cumplimiento de los fines de la comisión (ver Sección 15 Contratación de Proveedores y Comisionistas).

8) Presentación del Proyecto al Consejo de Administración por parte del Director General para su aprobación, discusión y modificación. Es recomendable que en esta sesión el propio Consejo de Administración o, en su caso, el Director General nombren a un Administrador del Proyecto que tenga facultades suficientes para verificar el cumplimiento de las metas y los hitos del Proyecto y que cada Parte Responsable nombre a una persona como enlace que se encuentre comprometido con los fines del Proyecto.

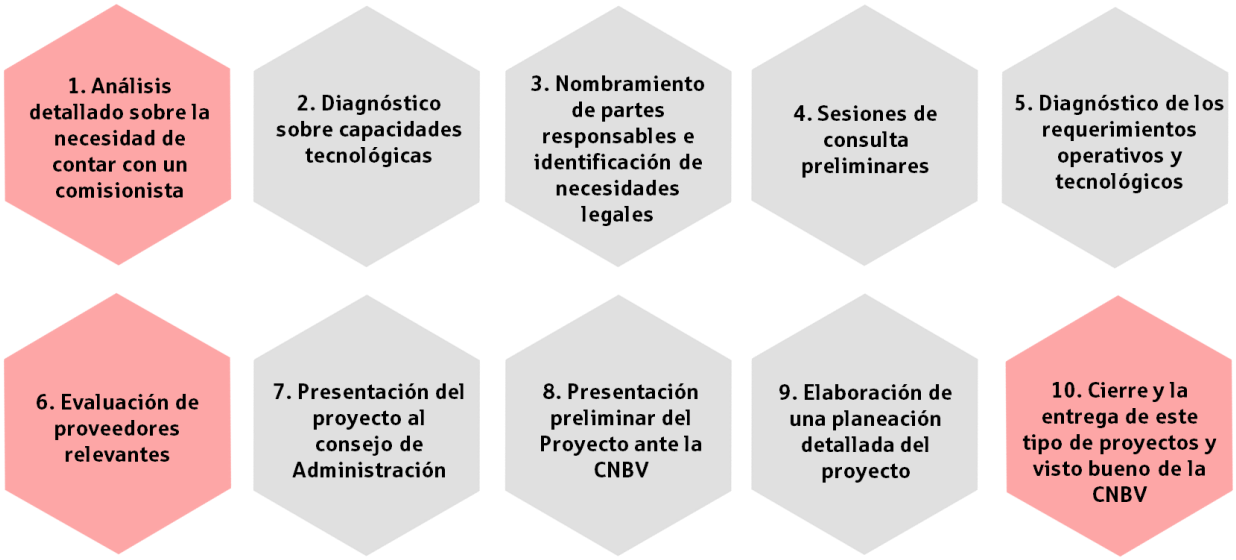
9) Presentación preliminar del Proyecto ante la CNBV mediante el uso de materiales informativos (ver sección inmediatamente anterior).

10) Elaboración de una planeación detallada del Proyecto. Es necesario que el Director General exprese con claridad a las Partes Responsables, incluyendo a las áreas internas, la necesidad de involucrarse y asumir responsabilidad concreta frente al Proyecto. En algunos casos, el proceso ante CNBV y la implementación pueden sufrir retrasos innecesarios cuando las personas al interior de la organización no hacen suyos los objetivos y no lo consideran parte de sus funciones.

11) El cierre y la entrega de este tipo de Proyectos deben estar coordinados y aprobados por todas las áreas y no ocurre sino hasta que CNBV ha dado comentarios al Plan Estratégico de Negocios, al formato de contrato de comisión y a las políticas que deben modificarse para efecto de estar en cumplimiento con los temas operativos, control interno, PLD/FT, productos o servicios (captación, crédito, etc.), transparencia y ordenamiento de los servicios financieros. Esta es una etapa "informal" del proceso donde, si bien no existe una calendarización definida, es posible que varias reuniones e intercambio de información existan previo a la realización del aviso o solicitud de autorización formales.

12) La finalización típicamente coincide con el visto bueno o autorización de parte de CNBV, la presentación del cierre ante el Consejo de Administración y la aprobación d las modificaciones a los Manuales existentes, a las políticas mencionadas en esta sección.

Proceso de evaluación para la contratación de un comisionista



Gráfica 14. Proceso de evaluación para la contratación de un comisionista. Fuente: Vite Abogados

15.16 Temas prácticos y recomendaciones.

México es un país extenso y con poca bancarización. Las corresponsalías son una herramienta útil, sobre todo porque existen zonas donde el modelo de sucursal bancaria no es viable. El manejo de dinero en efectivo continuará siendo durante algún tiempo una necesidad y parte importante de una economía que aún tiene altos índices de informalidad. En Europa ha surgido una Fintech con una solución interesante al problema crónico de falta de infraestructura bancaria, en concreto, los puntos de retiro de efectivo (por ejemplo, cajeros automáticos). Esta Fintech que tiene ya presencia en nuestro país y llamaremos “ST” tiene como objetivo convertir a negocios pequeños como tiendas de conveniencia y restaurantes en puntos de retiro de efectivo sin la necesidad de contar con un cajero electrónico.

En su país de origen ha logrado captar alrededor de 2,500 comercios, convirtiéndose en una red de "cajeros virtuales" con una distribución más amplia que la de los cajeros ordinarios.

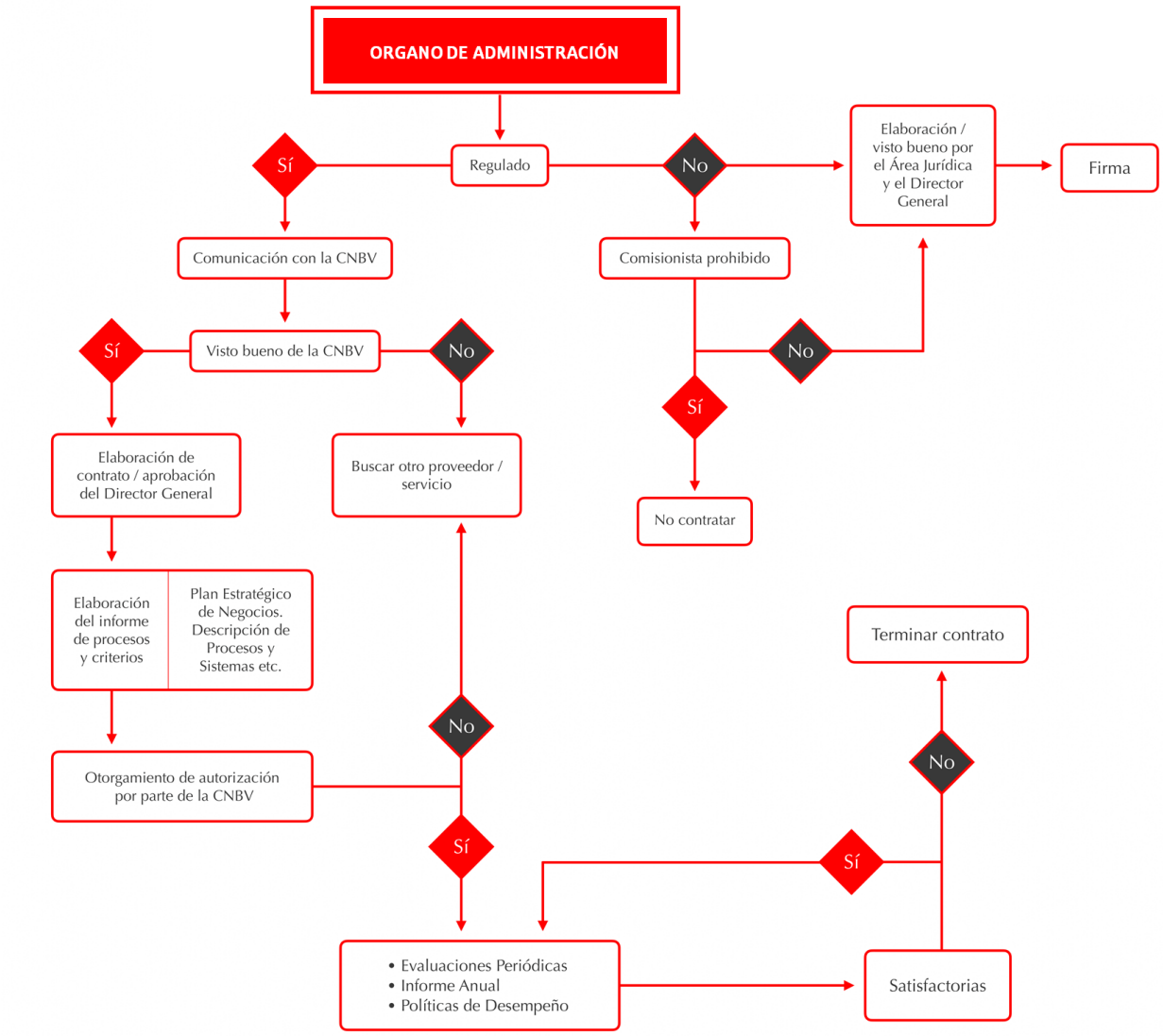
El funcionamiento es el siguiente: una persona con una cuenta de depósito hace la descarga de la aplicación, posteriormente realiza el alta de una cuenta dentro de ST. En el proceso de alta se le solicita que incluya su número de tarjeta. En el momento que el usuario registrado necesite disponer de efectivo se despliega ante él una red de comercios afiliados (los cuales llevaron previamente un proceso de registro y alta con ST para poder operar con este carácter). La aplicación además verifica que existan los fondos disponibles en la cuenta. Posteriormente el usuario obtiene un código de barras o QR que se presenta ante el comercio y entonces se despacha el efectivo.

Estos retiros se ofrecen sin costo alguno. Quienes cubren los costos asociados con el servicio son los bancos. Por su parte, los comercios reciben un porcentaje relacionado con el monto transaccionado.

En algunos casos ST realiza la implementación mediante un acuerdo de "cajeros virtuales", donde a una persona, por ejemplo, una institución bancaria (denominada "Asociado") se le permite que sus clientes o usuarios finales retiren dinero de su cuenta en la red de comercios o tiendas, tal como se mencionó anteriormente. Este acceso incluso permite hacer el retiro en cualquier tienda a nivel mundial. Los honorarios consisten en montos fijos por retiro. El Asociado asume ciertas obligaciones para efecto de realizar la promoción de la aplicación.

En ese sentido, una alianza con entidades Fintech que ofrecen servicios similares, bajo un esquema de comisión podría dar resultados interesantes para el SACP. Al respecto, ver Sección 24 Alianzas en la cual hacemos un análisis más detallado de las posibles estrategias conjuntas que podrían explorarse entre el SACP y el sector Fintech.

DIAGRAMA DE FLUJO PARA CONTRATOS



Gráfica 15. Diagrama de flujo para contratos. Fuente: Vite Abogados

SECCIÓN 16.- PRESTADORES DE SERVICIOS OPERATIVOS.

Las Entidades, para la contratación de Proveedores Relevantes con el objeto de que lleven a cabo un proceso operativo o para la administración de bases de datos y sistemas informáticos relacionados con operaciones que no sean propias de los comisionistas (ver Sección 15 Contratación de Proveedores y Comisionistas), deben sujetarse a ciertas reglas y procedimientos para ello. Dichos Proveedores Relevantes pueden ser prestadores de servicios tecnológicos, terceros especializados, entidades financieras o incluso otras Entidades, siempre que se cumplan con los requisitos de la normatividad y que se describen de manera general en las siguientes secciones. Esta categoría también abarca cierto tipo de comisiones que pueden otorgarse por las Entidades para la realización de procesos administrativos y operativos que no sean Servicios Excluidos.

La subcontratación de recursos, sobre todo tecnológicos, es uno de los temas más importantes en el sector financiero. Existe una fuerte presión de costos, entornos cambiantes y cambios regulatorios que exigen a las Entidades contar con mayor apoyo para poder lograr su objetivo.

La regulación actual para las SACP en muchos aspectos cuenta con elementos que aún no consideran aspectos dinámicos del sector tecnológico y atiende únicamente al cumplimiento de requisitos mínimos para efecto de lograr una contratación exitosa. En experiencia del Asesor Legal, tal como se mencionó en la Sección 14 respecto al cómputo en la nube, los contratos de este tipo deben contener un clausulado mínimo y atender a una administración de riesgos eficiente.

Para dar un enfoque de interés general a este capítulo a cuyo objeto, en más de un aspecto tal como se menciona más adelante, se traslapa con requerimientos iguales o similares a los aplicables a comisionistas (salvo por lo expresamente excluidos en las próximas secciones), queremos centrarnos en el contenido contractual que permita a la Entidad aplicar una administración de riesgos exitosa. La regulación tiene como objetivo preservar la estabilidad y garantizar un estándar mínimo de operación que tienda a mitigar riesgos para el sector financiero como un todo, no obstante, una redacción e implementación correcta de un contra que implique un proceso esencial para las operaciones financieras de las Entidades obedece a cuestiones prácticas y a enfoques particulares.

No tenemos la intención de innovar en cuanto a contenido o alcance de esta sección. La mayoría se basa en la experiencia del Asesor Legal en materia de administración y mitigación de riesgo legal y en la negociación continua de este tipo de contratos para el sector financiero.

16.1 Requisitos de contratación y proceso ante CNBV.

El aviso que debe entregarse ante CNBV, debe precisar el proceso operativo o de administración de bases de datos y sistemas informáticos objeto de los servicios o comisiones de que se trata y entregarse a la Comisión con una anticipación de por lo menos veinte días hábiles a la fecha en que pretendan contratar dichos servicios o comisiones.

La CNBV en protección de los intereses de los Socios o Clientes de las Entidades, antes de la fecha en que se pretenda contratar el servicio o comisión respectivos, tendrá la facultad de requerir a la Entidad que la prestación de dicho servicio no se realice a través del tercero o comisionista señalado en el aviso. Esto, si CNBV considera que los términos y condiciones de contratación del servicio o las políticas y procedimientos de control interno, la infraestructura tecnológica o de comunicaciones materia del servicio, sea previsible que no estarían en posibilidad de cumplir con la normativa aplicable y, en su caso, pueda verse afectada la estabilidad financiera o continuidad operativa de la Entidad, a juicio de la CNBV.

En caso de que la Entidad no reciba dicho requerimiento por escrito por parte de la Comisión en el plazo antes mencionado, se tomará como “afirmativa ficta” (es decir, se tendrá por aprobado el uso de ese Proveedor Relevante) y podrá iniciarse la prestación del servicio o comisión en cuestión. En caso de que la CNBV realice algún requerimiento, el mismo deberá ser satisfecho para efecto de que éste tome una resolución definitiva sobre el proceso.

El aviso debe presentarse en formato libre suscrito por el Director General de la Entidad y deberá contener lo siguiente:

- Informe de procesos operativos. Contar con un informe que especifique los procesos operativos o de administración de bases de datos y sistemas informáticos

de la Entidad que sean objeto de los servicios o comisiones a contratar, así como los criterios y procedimientos para seleccionar al tercero. En caso de que los servicios o comisiones a contratar se refieran a la utilización de infraestructura tecnológica o de telecomunicaciones, el aviso deberá contener un informe técnico que especifique el tipo de operaciones o servicios que habrán de celebrarse utilizando la base tecnológica que le sea proveída por terceros o comisionistas, así como la forma en que se dará cumplimiento a los lineamientos mínimos de operación y seguridad que establece la regulación de las Entidades.

- Criterios de Afectación. Establecer y presentar los criterios que permitan a las Entidades, a través de su Director o Gerente General, evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones que realice la Entidad, conforme a su objeto.

16.2 Autorización de Servicios Prestados fuera de México.

Las Entidades requerirán de la autorización de la Comisión, para la contratación con terceros la prestación de servicios o comisiones que impliquen la realización de un proceso operativo o para la administración de bases de datos, que se proporcionen o ejecuten parcial o totalmente fuera de territorio nacional o por residentes en el extranjero, en todo momento, con independencia de que los procesos de que se trate puedan o no afectar cualitativa o cuantitativamente una o más de las operaciones que realice la Entidad.

Las Entidades deben solicitar la autorización de la Comisión, con cuando menos veinte días hábiles de anticipación a la fecha en que pretendan contratar los servicios o la comisión que corresponda, acompañando para tal efecto la documentación que acredite el cumplimiento de los requisitos señalados en la Sección 15.2 (Reglas Comunes de Proveedores Relevantes) de la presente Guía Legal. Asimismo, debe acreditarse ante CNBV lo siguiente:

(i) Que los terceros o comisionistas con los que se contrate residan en países cuyo derecho interno proporcione protección a los datos de las personas, resguardando su debida confidencialidad, o bien, los países de residencia mantengan suscritos con México acuerdos internacionales en dicha materia o de intercambio de información entre los organismos supervisores, tratándose de entidades financieras;

(ii) Que las Entidades manifiesten a la CNBV que mantendrán en sus oficinas principales en México, al menos la documentación e información relativa a las evaluaciones, resultados de auditorías y reportes de desempeño.

(iii) Que se cuente con la aprobación del Consejo de Administración o, en su caso, del Comité de Auditoría o del Comité de Riesgos, haciendo constar en el acuerdo respectivo los aspectos siguientes:

1. Que al contratar los servicios o comisiones no se pone en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Entidad.
2. Que las prácticas de negocio del tercero o comisionista son consistentes con las de operación de la Entidad.
3. Que no habrá impacto en la estabilidad financiera o continuidad operativa de la Entidad con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizará en la prestación del servicio.
4. Los criterios que permitan a la Entidad, a través de su Director General, evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones de la Entidad.

La solicitud de autorización para la contratación de los servicios o comisiones a que se refiere el presente artículo deberá contener los mismos requisitos mencionados para el aviso. Asimismo, CNBV podría requerir una traducción del contrato al español.

16.3 Reglas comunes con comisionistas.

Existen muchas coincidencias regulatorias en el régimen legal de lo que para esta Guía Legal hemos denominado "Proveedores Relevantes": las comisiones y las prestaciones de servicios tienen en común las reglas descritas en las Secciones 15.2, 15.8, 15.10 y 15.12, entre otras. Asimismo, la planeación e implementación es bastante similar a la expuesta para comisionistas y, en lo aplicable, para los procesos de cómputo en la nube.

16.4 Temas prácticos y recomendaciones.

La contratación de Proveedores Relevantes permite liberar muchas energías al interior de la Entidad para efecto de que sean usadas para otras tareas y conduce a la aceleración del proceso de digitalización, al poner a disposición de las Entidades modelos de servicio ya probados. Todo ello debe contar con una instrumentación legal adecuada para efecto de prevenir incumplimientos y permitir a la Entidad manejar los riesgos del acuerdo de manera más eficiente. Tomando como punto de partida las recomendaciones que hace la Monetary Authority of Singapur (MAS) [82] sobre la contratación de servicios por parte de entidades financieras y nuestra propia experiencia es que hacemos las siguientes recomendaciones al respecto:

- Responsabilidad de la alta dirección. El Consejo de Administración y la Dirección General desempeñan funciones fundamentales para garantizar la adecuada gestión de riesgos. Si bien una Entidad puede delegar algunas de las tareas operativas del día a día al proveedor de servicios, las responsabilidades de mantener supervisión y cumplimiento de los acuerdos de subcontratación, gestión de los riesgos de subcontratación e implementar un marco adecuado de gestión de riesgos de subcontratación, de acuerdo con esta normatividad recaen en el Consejo de Administración, el Director General y los Directivos Relevantes. Estos tres órganos deben asegurarse de que haya procesos adecuados para proporcionar una visión integral de las exposiciones al riesgo incluidas en la subcontratación, e incorporar la evaluación y mitigación de dichos riesgos en un marco de gestión de riesgos de subcontratación y evaluación de proveedores.
- Evaluación de Riesgos. El Consejo de Administración y el Director General deben comprender y evaluar los riesgos derivados de la subcontratación. La Entidad debe establecer un marco para la evaluación de riesgos que debe incluir: (a) identificación del papel de la subcontratación en la estrategia comercial general y objetivos de la Entidad, (b) realizar una revisión integral sobre la naturaleza, alcance y complejidad del acuerdo de subcontratación para identificar y mitigar los riesgos; (c) evaluar la capacidad del proveedor de servicios para dar niveles adecuadas de servicio y cumplir con los estándares regulatorios como si los realizara la propia

[82] MAS. Guidelines on Outsourcing for financial institutions. (Internet) Consultado en: https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

Entidad, (d) analizar el impacto del acuerdo de subcontratación en el riesgo global, perfil de la Entidad, y si hay experiencia interna adecuada y recursos para mitigar los riesgos identificados, y (e) analizar los beneficios de la subcontratación frente a los riesgos que puedan surgir, que van desde el impacto de la interrupción temporal del servicio hasta el de un violación de seguridad y confidencialidad, y terminación inesperada del contrato.

- Evaluación del Proveedor. Previo a la contratación de un Proveedor Relevante, la Entidad debe llevar a cabo un proceso de "*due diligence*" o auditoría en materia de riesgos, la cual debe incluir: aspectos relevantes del proveedor de servicios, incluida su capacidad para proporcionar niveles mínimos de servicio y considerando como si el servicio lo prestara la propia Entidad como entidad regulada. La revisión también debe tener en cuenta:

  (i) La seguridad física y de infraestructura tecnológica del Proveedor Relevante.

  (ii) Los controles que tiene el Proveedor Relevante en la prestación de los servicios, la reputación comercial y su solidez financiera, incluidos sus estándares éticos y profesionales con los que guía.

  (iii) Experiencia y capacidad para implementar y prestar los servicios a ser contratados.

  (iv) Solidez financiera y recursos (la auditoría debe ser similar a una evaluación crediticia de la viabilidad del proveedor de servicios basada en revisiones de la estrategia y los objetivos comerciales, estados financieros auditados, la solidez del compromiso de los principales patrocinadores de capital y la capacidad de prestar servicio compromisos incluso en condiciones adversas).

  (v) Existencia dentro del Proveedor Relevante de: gobierno corporativo adecuado, buena reputación en la industria y existencia de litigios pendientes o potenciales (esto puede revisarse en algunos servicios independientes que rastrean la existencia de este tipo de controversias).

  (vi) Verificación de seguridad y controles internos del Proveedor Relevante, incluyendo un marco de gestión del riesgo tecnológico y la existencia de planes de continuidad del negocio.

  (vii) Existencia de pólizas de seguro suficientes para lidiar con daños a terceros o a la propia Entidad contratante.

(viii) Se recomienda hacer vistas a las oficias o instalaciones del Proveedor Relevante y, en lo posible, llevar a cabo una investigación propia del comportamiento en el mercado del Proveedor Relevante. Las visitas deben ser realizadas por personas que posean los conocimientos y habilidades necesarias para realizar la evaluación.

(ix) Asegurarse que los empleados del Proveedor Relevante que realicen cualquier parte del acuerdo de subcontratación hayan sido evaluados para cumplir con las políticas de contratación de la Entidad para el rol que están desempeñando, de acuerdo con los criterios aplicables a sus propios empleados, entre otros: (a) si han sido objeto de algún procedimiento de carácter disciplinario o penal, y (b) si han sido condenados por algún delito (patrimoniales en particular), entre otros.

Lo anterior, sin perjuicio de verificar los aspectos regulatorios supervisados por CNBV conforme a la normatividad aplicable y brevemente expuesto en este capítulo.

El proceso y alcance de la revisión, puede variar según la naturaleza y el alcance del riesgo del contrato y el impacto para la Entidad en caso de una interrupción del servicio o una violación de la seguridad y la confidencialidad (por ejemplo, una auditoría reducida puede ser suficiente cuando se trate de partes relacionadas o de proveedores más sólidos o grandes de la industria). De cualquier modo, la Entidad debe asegurarse de que la información utilizada para la revisión sea la más actual y completa.

- Contrato. Los acuerdos que se reflejen en cada contrato con un Proveedor Relevante, además de contener las cláusulas regulatorias mínimas que marca la normativa, deben ser objeto de una revisión cuidadosa por un experto legal para efecto de asegurar que cada uno de los acuerdos pueda ser exigido y constituyen obligaciones válidas en contra del Proveedor Relevante, sobre todo, en un escenario de litigio. Asimismo, su contenido debe reflejar, por lo menos, los siguientes aspectos:

  (i) Deben abordarse los riesgos identificados en la evaluación del Proveedor Relevante, ya sea mediante la inserción de cláusulas indemnizatorias en caso de que ocurran ciertos escenarios como la inclusión de declaración suficientes.

(ii) Incluir mecanismos de renegociación y renovación que permitan a la Entidad mantener control sobre los plazos y términos de la prestación del servicio, así como el otorgar facultades suficientes a la Entidad para tomar medidas adecuadas en caso de incumplimiento a los niveles o aspectos del servicio, cambios en la regulación o incumplimiento de la regulación por causa del contrato.

(iii) Establecer normas de desempeño, operativas, de control interno y de gestión de riesgos, así como las respectivas consecuencias de cada incumplimiento, procurando no recurrir a formulaciones generales. Esto incluye hacer una conexión lógica con cada uno de los anexos del contrato a clausulado y consecuencias concretas: existe una costumbre extendida de mandar secciones importantes del contenido contractual a documentos secundarios, lo cual es eficiente, pero debe estar debidamente controlado para efecto de no dejar sin efecto el clausulado concreto del contrato principal en casos de incumplimiento o demandas.

(iv) Inserción de cláusulas de confidencialidad y seguridad de la información: sobre todo teniendo en consideración temas de secreto financiero y datos personales. Ello debe reflejar un análisis previo de la Entidad sobre la capacidad con la que cuenta para disponer de esa información para poder recibir el servicio que se pretende contratar.

(v) Gestión de la continuidad del negocio: negociar y reflejar estándares mínimos de operación continua, aminorar y especificar cuestiones relacionadas, por ejemplo, con caso fortuito y fuerza mayor. En algunos casos se pueden establecer catálogos mínimos de situaciones donde dicho supuesto no será aplicable: el “caso fortuito” o la “fuerza mayor” son excluyentes de responsabilidad pues son situaciones que, por causas ajenas al obligado, le impiden de manera total o parcial, cumplir con sus obligaciones. Lo anterior es problemático por la manera en que dichos términos están definidos en la normativa contractual. Esto requiere entender, por parte del asesor legal, la naturaleza y alcance del servicio para modificar la aplicabilidad de esta regla.

(vi) Procesos de seguimiento y control del desempeño del Prestador de Servicios durante la vigencia del contrato.

(vii) Derechos de auditoría e inspección a favor de la Entidad, para efecto de corroborar el funcionamiento de los servicios y entender temas relevantes sobre el estado operativo, financiero o legal del Proveedor Relevante.

(viii) Notificación de acontecimientos adversos: para efecto de hacer saber a la Entidad si existe un evento que podría poner en peligro el funcionamiento continuo y adecuado de la Entidad. Asimismo, el Proveedor Relevante debe asumir la obligación de tomar medidas de mitigación en caso de que ocurran dichos eventos.

(ix) Resolución de controversias: especificar el proceso de resolución, los eventos de incumplimiento y las indemnizaciones, recursos y acciones disponibles para las partes en cada supuesto. La Entidad debe poner énfasis en que sus derechos contractuales puedan ejercerse en caso de incumplimiento por parte del Proveedor Relevante.

(x) Los supuestos y consecuencias de la terminación por incumplimiento (incluyendo cualesquier supuestos establecidos en anexos y documentos auxiliares del contrato) y la salida anticipada en caso de que así convenga a los intereses de la Entidad.

(xi) Se sugiere que la Entidad tenga derecho a rescindir el contrato en caso de incumplimiento o en circunstancias en las que: (i) el Proveedor Relevante sufra un cambio de control (cambio de accionistas principales); (ii) el Proveedor Relevante se declare insolvente o entre en liquidación; (iii) el Proveedor Relevante haya sido víctima o causado incidentes que afecten la seguridad o la confidencialidad de la información procesada por él y (iv) exista un deterioro demostrable en la capacidad del Proveedor Relevante para realizar el servicio contratado.

(xii) El período mínimo o máximo para solicitar la terminación debe especificarse en el contrato. Asimismo, deben insertarse disposiciones que garanticen una transición sin problemas cuando el acuerdo se rescinda o se modifique. Tales disposiciones pueden facilitar la transferibilidad de los servicios contratados a un tercero.

(xiii) Acuerdos sobre la capacidad de realizar la subcontratación, incluyendo capacidad de monitorear y controlar los convenios de subcontratación, así como las reglas y limitaciones de la subcontratación. Es recomendable incluir cláusulas que hagan que el Proveedor Relevante sea contractualmente responsable por el desempeño y las prácticas de gestión de riesgos del subcontratista y por el cumplimiento por parte de éste de las disposiciones normativas aplicables.

- Confidencialidad y Seguridad. La Entidad debe dar prioridad a la identificación y especificación de requisitos de confidencialidad y seguridad en el contrato a celebrarse con el Proveedor Relevante. Se sugiere adoptar las siguientes medidas para proteger la confidencialidad y seguridad de la información:

(i) Establecer las responsabilidades de ambas partes contratantes para garantizar la idoneidad y eficacia de las políticas y prácticas de seguridad de la Entidad (incluyendo aquellos aspectos regulatorios que deben integrarse, tal como se ha expresado en otras secciones de esta Guía Legal), incluidas las circunstancias bajo las cuales cada parte tiene derecho a cambiar los requisitos de seguridad. El acuerdo de subcontratación también debe abordar:

- La responsabilidad del Proveedor Relevante en caso de violación de la seguridad o la confidencialidad de la información perteneciente a la Entidad o sus Socios o Clientes, así como la obligación del Proveedor Relevante de informar sobre estos incidentes de seguridad.

- La información de los clientes de la Entidad (dependiendo del tipo de contrato) debe ser utilizada por el Proveedor Relevante y su personal estrictamente para los propósitos del servicio.

- Revisar y monitorear las prácticas de seguridad y los procesos de control del Proveedor Relevante de manera regular, incluyendo la realización de auditorías o entrega de informes periódicos sobre confidencialidad, adecuación de la seguridad y cumplimiento normativo, entre otros temas.

- Continuidad del Negocio. La Entidad debe asegurarse de que la continuidad del negocio no se vea afectada por la contratación del Proveedor Relevante. Al evaluar el impacto de la contratación la Entidad debe no sólo revisar su Manual de Riesgos, sino que debe realizar un análisis relacionado con riesgos de seguridad de la información que hasta este punto quizás no habían sido tomados en consideración. Este estudio de riesgos debe considerar las medidas que garanticen una mitigación adecuada de cualesquier indicadores o situaciones potencialmente riesgosas. El principal escenario de desastre debe tomar en cuenta el grado de interdependencia creado entre el Proveedor y la Entidad (supuestos de terminación anticipada o interrupción del servicio o incluso imposibilidad del Proveedor Relevante de cumplir con sus obligaciones por cualquier razón). Para ello es necesario establecer:

  (i) Asegurarse que el Proveedor Relevante cuenta con un "Plan de Continuidad del Negocio" (PCN) satisfactorio conforme al tipo de servicio que está ofreciendo. El contrato debe incluir requisitos del PCN del Proveedor Relevante, específicamente "tiempo objetivo de recuperación" (RTO), punto objetivo de recuperación (RPO) y esquema de reanudación de operaciones.

  (ii) De ser posible participar en pruebas conjuntas de escenarios catastróficos para efecto de examinar la efectividad del PCN.

  (iii) Incluir en el contrato la obligación del Proveedor Relevante de probar de manera regular la efectividad de su PCN, así como el deber de notificar cualquier situación adversa derivada de dichas pruebas.

- Gestión y Control del Contrato. Para efecto de implementar medidas adecuadas para monitorear y controlar los contratos con Proveedores Relevantes, se sugiere a las Entidades:

  (i) Mantener un registro de todos los contratos celebrados con Proveedores Relevantes, de preferencia a través de un sistema accesible para su revisión por parte de las Partes Responsables de implementarlo (desde la alta dirección hasta las personas encargadas de administrar dicho contrato).

  (ii) Establecer grupos multidisciplinarios de gestión del contrato, incluyendo personas con responsabilidad en materia de control interno, administración de riesgo, área legal y de cumplimiento, así como las de negocio financieras, para verificar que el contrato cumpla con las especificaciones deseadas.

  (iii) Establecer políticas y procedimientos para monitorear la prestación de servicios y la confidencialidad y seguridad de la información, con el fin de evaluar el cumplimiento continuo de los niveles de servicio acordados y la viabilidad de las operaciones de la Entidad.

  (iv) Revisiones periódicas, al menos una vez al año, del desempeño del Proveedor Relevante.

- Importancia del Contrato. La Entidad debe evaluar la importancia de un contrato en el contexto de su plan de negocios y de su operación a través de ciertos criterios de "materialidad". En otras palabras, se trata de realizar un juicio cualitativo sobre distintos factores para efecto de evaluar riesgos potenciales y establecer medidas apropiadas para su cumplimiento:

  (i) Importancia de la actividad empresarial que se subcontratará (por ejemplo, en términos de contribución a los ingresos de la Entidad);

  (ii) El impacto potencial de la subcontratación sobre los resultados, la solvencia, la liquidez, el capital y el perfil de riesgo de la Entidad;

(iii) El impacto en la reputación (y la marca) de la Entidad para efecto de lograr los objetivos, estrategia y planes comerciales, en caso de que el Proveedor Relevante no cumpla con el servicio o se encuentre con una violación de la confidencialidad o seguridad a su cargo.

(iv) El impacto del contrato con los clientes de la institución, en caso de que el Proveedor Relevante no lo realice o se encuentre con una violación de la confidencialidad o la seguridad;

(v) El impacto en las contrapartes de la Entidad, por ejemplo, incumplimientos cruzados potenciales, es decir los incumplimientos en que podría caer la Entidad si el Proveedor Relevante no puede presar los servicios;

(vi) Costo de la subcontratación como proporción de los costos operativos totales de la Entidad;

(vii) Costo del contrato en caso de incumplimiento, es decir los costos que deberá asumir la Entidad en caso de que la Entidad lo realice internamente o busque un servicio similar de otro proveedor. Lo anterior en el contexto de los costos operativos totales de la Entidad.

(viii) Capacidad y (costos) de llevar e implementar controles internos apropiados y cumplir con los requisitos normativos en caso de que el Proveedor Relevante enfrente problemas operativos.

(ix) La contratación de todas o sustancialmente todas las funciones de control interno o de gestión de riesgos, incluyendo las funciones de cumplimiento, la auditoría interna, la contabilidad, entre otras, se consideran áreas de “alto impacto” que requieren de un cuidado especial para su implementación.

SECCIÓN 17.- USO DE BIOMÉTRICOS.

Como se ha mencionado en secciones anteriores, los Proyectos de digitalización deben obedecer a necesidades previamente identificadas (y calculadas) de cada Entidad. El uso de "biométricos" no es la excepción.

En el caso de las instituciones de banca múltiple, hubo una reforma importante en la materia donde incluso se hace obligatorio el solicitar los mismos a sus usuarios y clientes para efecto de abrir cuentas bancarias y utilizar otros servicios. Por lo que respecta al SACP no ha existido una reforma similar, sin embargo, su uso se encuentra reconocido, si bien de manera limitada, en la regulación.

Actualmente, el uso de biométricos es prevalente en el uso de teléfonos celulares, los cuales ya están perfectamente habilitados para efecto de utilizarlos al dar acceso y uso de varias aplicaciones.

17.1 Definición.

Un "biométrico[83]" es cualquier característica física o humana que puede ser usada para realizar la identificación digital y darle acceso a un sistema, un dispositivo electrónico o datos. Los ejemplos más claros de biométricos son: huellas digitales, voz o incluso patrones de movimiento (por ejemplo, el trazo de rasgos, o la manera de apretar botones o teclas). En concreto, cada biométrico se considera como una característica única e irrepetible de su titular y se puede utilizar en combinación con otros factores para asegurar que la identificación de la persona es exacta.

Los datos biométricos "físicos" utilizan características tangibles para acreditar la identidad del usuario. Las tecnologías más comunes para generar y usar estos biométricos son escaneos de huellas dactilares, reconocimiento facial, escaneos de retina y recolección de ADN.

Los ciclos de "uso" de los biométrico físicos, son similares:

[83] GIONES-VALLS, Aina. La gestión de la identidad digital: una nueva habilidad información digital (Internet). Consultado en: http://bid.ub.edu/24/giones2.htm

(i) Inscripción, donde se captura la imagen o el registro del rasgo físico.

(ii) Almacenamiento, que implica el resguardo de los datos del biométrico en un sistema informático.

(iii) Comparación, el proceso a través del cual un sistema compara un rasgo o elemento con una información almacenada para determinar si hay una coincidencia.

Existe un segundo tipo de biométrico que está comenzando a ser habitual que son los referidos al "comportamiento", los cuáles analizan comportamientos como pulsaciones de teclas, escritura a mano o navegación de una página web para verificar la identidad del usuario. Consiste en rastrear comportamientos inconscientes de una persona durante el curso de una actividad para crear un perfil único que sea teóricamente imposible de reproducir por un tercero. Esto requiere de programas especializados o, en el caso de los datos recopilados, teléfonos celulares, a través de sensores que ya existen en el dispositivo. Esos datos son analizados por tecnología (por ejemplo, inteligencia artificial) que identifica los patrones correspondientes y crea una "huella" única para el usuario.

Los biométricos, en ese sentido, son un factor de seguridad que impide el fraude en las transacciones financieras y previene una afectación negativa a los usuarios de las entidades que ofrecen estos servicios. No obstante, el uso de esta tecnología para evitar fraudes tiene riesgos: la recopilación y almacenamiento de estos datos es delicado, pues se trata de datos que son únicos e inmutables. A diferencia de lo que puede pasar con un NIP o una contraseña, en este caso una divulgación o transferencia no autorizada tiene consecuencias permanentes para el usuario.

Como veremos, si bien la regulación del SACP sí prevé el uso de biométricos para realizar parte del proceso de identificación, no existe una regulación completa y comprensiva para las Entidades.

17.2 Evaluación de Utilidad.

Los biométricos son apoyos para reducir la probabilidad de que una persona no autorizada acceda a un servicio prestado por una entidad financiera.

Un Proyecto dirigido a realizar la identificación mediante datos biométricos requiere mucho tiempo y es costosa: requiere de la implantación de procesos para registrar un individuo, realizar la captura del biométrico, almacenarlo y vincular el biométrico a la cuenta del Usuario del servicio financiero.

La calidad de los datos biométricos obtenidos de las personas físicas depende en gran media de la habilidad de la persona que realiza el registro del cliente y de la calidad del sistema usado.

Un escenario ideal es el uso de una tecnología que permita realizar una implementación de bajo costo, un proceso de recolección e identificación sencillo para el cliente y un nivel de seguridad adecuado.

La Entidad, previo a la implementación de un sistema de identificación y uso de biométricos para los servicios financieros que ofrece, debe realizar una evaluación de riesgos que considere lo siguiente:

- Establecer el tipo de dato biométrico que se desea utilizar. Los tipos de biométricos más usados son los datos faciales y huella digital. Esto debe verse en el contexto de las limitaciones y requisitos legales mencionados anteriormente.
- Considerar la seguridad requerida para efecto de almacenar adecuadamente los datos del Usuario, así como los estándares necesarios para evitar falsificaciones por terceros, por ejemplo, un sistema que no confunda una fotografía en dos dimensiones con la representación en tercera dimensión de un rostro humano o incluso entre gente muy parecida. Esto incluye medidas de seguridad físicas (en el caso de que el almacenamiento se lleve a cabo por la Entidad) y de ciberseguridad.
- Considerar riesgos “no adversariales”, es decir, errores o factores humanos que pueden implicar un riesgo.
- Considerar la responsabilidad y el grado de riesgo legal que implica para la Entidad el manejo de información sensible (datos sensibles), así como las consecuencias del uso indebido de los mismos (ver Sección 9 - Datos Personales y Secreto Financiero).
- Gastos y riesgos relacionados con Proveedores Relevantes para efecto de servirse de biométricos en sus procesos.

- Consultar con sus Clientes, Socios o Usuarios su percepción sobre el uso y transferencia de sus datos biométricos, así como establecer si los dispositivos electrónicos que se utilizarán para la captación requieren de la compra y puesta a disposición de hardware especializado o si basta con el uso de tecnología cotidiana, como teléfono celular o sitios web.
- Evaluar y medir la prevalencia de fraudes o intentos de fraude hacia o dentro de la Entidad y comparar la incidencia de los mismos en el contexto de una posible implementación.

17.3 Regulación.

En México no existe una legislación específica para la recolección, uso y tratamiento en general de "datos biométricos". A diferencia de lo que ha estado ocurriendo en la Unión Europea y en Estados Unidos de América, las cuales imponen obligaciones y lineamientos en relación con[84]:

- Obligación para los responsables de biométricos de establecer y publicar guías o políticas para el tratamiento de dichos datos, así como los parámetros técnicos y legales que se usarán para destruir esa información.
- Implementación de consentimientos expresos para efecto de realizar el tratamiento de los biométricos.
- Aplicación de sanciones severas y específicas para violaciones a los deberes de guarda y custodia de datos biométricos.

Nuestra legislación en materia de protección de datos personales (ver Sección 9 Datos Personales y Secreto Financiero) cubre dentro de su definición de datos personales a los biométricos, si bien no existe un régimen diferenciado de los mismos. En ese sentido, las Entidades, en un primer de análisis legal tendrían que considerar, en primer término, el tipo de dato biométrico que desean implementar, así como la manera en que implementarán el ciclo de tratamiento del mismo (ver Sección 17 Uso de Biométricos) y

[84] Thales Group. Digital identity and security. (Internet) Consultado en: https://www.thalesgroup.com/en/markets/digital-identity-andsecurity/government/inspired/biometrics

tomar las medidas necesarias para modificar las políticas internas en materia de datos personales y los avisos de privacidad, en su caso.

Por su parte, las Disposiciones PLD/FT de las Entidades establecen que, en el caso de que la Entidad opte y esté autorizada para realizar la identificación no presencial de potenciales Socios o clientes (ver Sección 6 Prevención de Lavado de Dinero y Financiamiento al Terrorismo) debe cumplir además con lo siguiente en el caso de biométricos:

- Las Entidades deben requerir que el solicitante se tome una fotografía a color de su rostro, utilizando dispositivos con cámaras de resolución de, al menos, 4 mega pixeles, imágenes a color de 24 bits, cuya toma únicamente se realice en línea a través de la propia herramienta tecnológica puesta a disposición por las Entidades[85].
- Una vez que reciban los datos del potencial cliente o Socio deberán comparar las fotografías de la credencial para votar y del rostro del cliente o Socio de forma presencial[86], a fin de hacer el reconocimiento biométrico facial entre estas, asegurándose de que ambas coinciden conforme al nivel de fiabilidad establecido por el responsable de riesgos o su equivalente o, en caso de no contar con este, por el Comité de Auditoría o el Consejo de Administración.
- La CNBV puede aprobar mecanismos de identificación no presencial de los posibles Clientes distintos a los señalados expresamente en las Disposiciones PLD/FT, lo cual podría incluir el uso de biométricos adicionales al de la imagen del rostro. Para ello, sería necesario que la Entidad en cuestión acredite que la tecnología a ser utilizada, a juicio de la CNBV sea fiable para identificar a la persona física de que se trate; si bien en todo caso se deben cumplir con los demás requisitos de identificación establecidos por la norma. En consecuencia, el uso de biométricos no puede constituir la única fuente de verificación de la personalidad del potencial Socio o Cliente.

[85] Las Disposiciones PLD/FT no especifican si la aplicación debe verificar que el dispositivo que se utiliza para tomar la fotografía tenga la capacidad de tomar fotografías con dichas especificaciones o si, por el contrario, se debe aceptar la fotografía y posteriormente validarla. Al respecto, es nuestro criterio que por practicidad se acepten las fotografías y posteriormente se acepten o se descarten; sin embargo, esto está sujeto a los criterios de la CNBV, por lo que nosotros sugerimos consultar a dicha autoridad previo a tomar esta decisión.

[86] Existen maneras de realizar la verificación automática, pues el Instituto Nacional Electoral: La verificación de datos de diversos trámites, puede llevarse a cabo gracias a los convenios firmados por dicha institución con más de 50 organizaciones, entre las que destacan bancos, cajas populares, partidos políticos e instituciones públicas. Este servicio de verificación ayuda a prevenir la usurpación de identidad y así brindar seguridad al proceso, reduciendo el riesgo de fraudes.

- La tecnología utilizada para la identificación a distancia, incluyendo la utilizada para la validación de los biométricos, debe ser aprobada por el responsable de riesgos o su equivalente o, en caso de no contar con este, por el Comité de Auditoría o el órgano de administración.
- Las Entidades deben contar con los medios necesarios para la transmisión y resguardo de la información, datos y archivos generados en los procedimientos de contratación a distancia (lo cual incluye el uso de biométricos), que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación, así como su adecuada conservación y localización. Las Entidades podrán utilizar mejoras tecnológicas que ayuden a compensar la nitidez de las imágenes, aprobadas por su responsable de riesgos o su equivalente o, en caso de no contar con este, por el Comité de Auditoría o el órgano de administración, cuando se muestren los documentos de identificación y se realice el reconocimiento facial del solicitante.
- En todo caso para efecto de solicitar la autorización de CNBV con el objeto de implementar procesos de contratación a distancia, la Entidad debe proporcionar, entre otros documentos, evidencia de que los reconocimientos de identificación de rostro que se utilicen tengan el nivel de fiabilidad determinado por el responsable de riesgos o su equivalente o, en caso de no contar con este, por el Comité de auditoría o el órgano de administración.
- Los procedimientos mencionados anteriormente no serán aplicables cuando la Entidad haya implementado y cumplido con los requerimientos aplicables a la prestación de Servicios Electrónicos.

Por lo que respecta al uso de biométricos en el contexto de la prestación de Servicios Electrónicos, a riesgo de duplicar lo ya mencionado en la Sección 9 (Datos Personales y Secreto Financiero), para efectos de claridad es necesario recordar:

- Conforme a la regulación de la Banca Electrónica de las Entidades, éstas están obligadas a aplicar un conjunto de técnicas y procedimientos utilizados para verificar la identidad de (a) un Usuario y su facultad para realizar operaciones a través de Servicios Electrónicos, y (b) una Entidad y su facultad para recibir instrucciones a través de Servicios Electrónicos. Esto es lo que se conoce como “Autenticación”.

- Para efecto de llevar a cabo los procesos de Autenticación las Entidades deben usar "Factores de Autenticación", los cuales son mecanismos tangibles o intangibles, basados en las características físicas del Usuario, en dispositivos o información que solo el Usuario, posea o conozca. Estos mecanismos pueden ser:

  a) Información que el Usuario conozca y que la Entidad valide a través de cuestionarios practicados por operadores de atención telefónica.
  b) Información que solamente el Usuario conozca (contraseñas, NIP).
  c) Información contenida, recibida o generada en medios o dispositivos respecto de los cuales el Usuario tenga posesión.
  d) Información del Usuario derivada de sus características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, siempre que dicha información no pueda ser duplicada y utilizada posteriormente.

- En el uso de los Factores de Autenticación las Entidades deben ajustarse a las reglas establecidas en la Sección 9 (Datos Personales y Secreto Financiero).
- Los Factores de Autenticación Categoría 4 son los que se refieren a datos de biométricos y se definen como la información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras.
- La Entidad que utilice los Factores de Autenticación Categoría 4, debe aplicar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario.
- Se puede considerar dentro de esta categoría a la firma autógrafa de Usuarios plasmada en los comprobantes generados por las Terminales Punto de Venta o bien la plasmada en dispositivos ópticos en ciertos casos.
- Los casos de uso, es decir, los supuestos en los cuales se pueden utilizar estos biométricos o Factores de Autenticación Categoría 4 se encuentran establecidos en la regulación (ver Sección 10 Banca Electrónica). En la mayoría de dichos casos el uso de biométricos (Factores de Autenticación Categoría 4) es optativo, pues se permite el uso de Factores de Autenticación Nivel 3.

17.4 Evaluación de Prestadores de Servicios.

La decisión de implementar sistemas de seguridad a través de datos biométricos de los Socios o Clientes debe basarse en un estudio cuidadoso del uso de este tipo de datos en el contexto de las estrategias de seguridad, prevención de fraude y modelo de negocio de la Entidad. Es necesario que la Entidad busque un experto en estos temas para efecto de entender a profundidad los principios operativos básicos de las soluciones biométricas existentes en el mercado, así como sus puntos fuertes y sus debilidades. Asimismo, los aspectos legales sobre su uso, esbozados en esta sección también deben tenerse en cuenta para una potencial implementación.

Como también se mencionó antes, no todos los biométricos son iguales: las tecnologías de biométricos se pueden clasificar de acuerdo con la fuente de datos de entrada en la que se basan para autenticación e identificación. Algunas de las partes del cuerpo más comunes que son escaneadas por los sistemas biométricos son manos, cara, ojos y, en algunos casos, la voz. En este momento, el uso de otros biométricos en los servicios financieros aún estaría algo lejos de integrarse: pruebas de ADN, patrones de venas o de movimientos, por ejemplo.

Cada tipo de biométrico descrito cuenta con ventajas y desventajas, por ejemplo, las huellas digitales, son relativamente fáciles de obtener y leer, si bien no están exentas de posibles falsificaciones o errores de lectura. Otras como el reconocimiento facial son relativamente fáciles de obtener, pero pueden ser poco confiables para autenticar a una persona debido a cambios en la luz, modificaciones en vello facial u otras características similares y los algoritmos para implementarla suelen ser más complejos. El escaneo de retina está libre de los errores o desventajas anteriores, pero su utilización es más costosa.

El uso de biométricos, si bien lo hemos enfocado a los temas de identificación y acceso a un Servicio Electrónico, también pueden tener otros usos dentro de la Entidad, por ejemplo:

- Acceso lógico: controlar el acceso a datos o información (red aplicaciones de seguridad).
- Acceso físico: controlar el acceso a recursos tangibles.

- Verificación de identidad: establecer la identidad de un individuo o comparar su identidad con otros datos.
- Los aspectos que deben cuidarse y revisar de algún proveedor de tecnología biométrica son los siguientes:
- El posible proveedor de servicios en materia de biométricos debe garantizar ciertos estándares de seguridad y niveles de servicio.
- El tema de almacenamiento siempre debe estar en la discusión con un posible proveedor, pues ello está relacionado con la caracterización del mismo como Proveedor Relevante (Sección 15 de esta Guía Legal).
- Determinar si la Entidad debe realizar otras contrataciones adicionales o comprar equipo de cómputo para poder realizar las funciones que involucren la recolección, almacenamiento y uso de datos biométricos.
- Revisión de las políticas de seguridad y privacidad del posible proveedor, con especial énfasis en el cumplimiento de los aspectos presentados en la Sección 8, entre otros.

En términos generales, las reglas para Proveedores Relevantes mencionados en la Sección 15 de la presente Guía Legal serían aplicables.

17.5 Acercamiento Inicial.

El uso de cada tecnología biométrica tiene su propia problemática y requiere de una aproximación específica; no obstante, las acciones y temas genéricos de implementación y funcionamiento son similares. Toda implementación debe tener claridad sobre las implicaciones del "ciclo de los biométricos" para evaluar adecuadamente los riesgos, costos, necesidad de proveedores y adaptabilidad del sistema a las necesidades propias de la Entidad.

- Recolección de los datos. Este es el primer contacto del usuario con el sistema biométrico. Es necesario contar con un dispositivo de entrada para el correcto funcionamiento de esta tecnología. La calidad de dicha recolección es de suma importancia para las futuras autenticaciones del usuario en cuestión. Prever que existan grupos que no puedan proporcionar el dato requerido y establecer alternativas: casos específicos de personas con capacidades diferentes. Preparar

información y materiales de divulgación que apoyen a los usuarios en la recolección y aspectos relevantes de los biométricos. La recolección debe realizarse por personal capacitado para garantizar la calidad de la toma.

- Procesamiento de las muestras. Las muestras de datos biométricos se procesan después de la toma de los mismos. El número de muestras biométricas necesarias para el procesamiento posterior se basa en la tecnología utilizada para su obtención: a veces, una sola muestra es suficiente, pero a menudo múltiples son requeridas. Las características biométricas pueden requerir técnicas de almacenamiento específico.
- Almacenamiento. Después de procesar las primeras muestras biométricas y extraer las características, debe realizarse el almacenamiento de la información. Los accesos y la titularidad de la base de datos son muy relevante para determinar si se requiere un Proveedor Relevante y, en consecuencia, llevar a cabo la tramitación correspondiente ante CNBV (ver Sección 15 Contratación de Proveedores y Comisionistas).
- Comparación. Los datos biométricos recolectados, para efecto de poder ser utilizados para fines de autenticación deben ser comparados de manera constante. Esto está referido a la capacidad de respuesta del sistema y la continuidad del mismo.
- Autenticación. La parte final del proceso es la decisión de autenticar a una persona o de negar el acceso al sistema. El acceso final depende de los parámetros de seguridad y la comparación entre el biométrico almacenado y el biométrico ofrecido para validación. Existen márgenes de error (como en cualquier tecnología), pero es necesario que ellos se encuentren dentro de los límites inferiores para evitar altas incidencias de falsos rechazos.
- Conocimiento de las etapas y procesos del servicio. Si bien existen tecnologías propias de un Proveedor Relevante, así como secretos industriales que no serán objeto de relevación a la Entidad, es necesario entender cada módulo y cada proceso que prestará dicho tercero conforme a las etapas anteriores.

Con esos puntos en mente podrá trazarse una ruta crítica y establecer los elementos que serán necesarios de un Proveedor Relevante y las adaptaciones tecnológicas y operativas que la Entidad requerirá para efecto de tener una implementación exitosa.

Finalmente hay que recordar que ni las Disposiciones PLD/FT, ni las reglas emitidas por CNBV en materia de banca electrónica permiten (en consonancia con las mejores prácticas en la materia) el uso de un biométrico de manera aislada o única para completar la autenticación. En ese sentido, su uso siempre va acompañado de otros requisitos y tecnologías que validen de manera más completa la identidad de los Usuarios, por ejemplo, el uso de contraseñas.

17.6 Plan de Trabajo y Diagrama.

1) Realizar un análisis detallado sobre la necesidad de implementar datos biométricos, sobre todo atendiendo:

   a) Limitaciones legales y casos de uso conforme a lo mencionado anteriormente: protección de datos personales, prevención de lavado de dinero y Banca Electrónica.

   b) Determinar la función que tendrán los datos biométricos dentro del plan de negocio de la Entidad:

      (i) Establecer si el uso de biométrico será requerido para temas de identificación o enrolamiento únicamente o si se será con el objeto de lograr validación para acceder a servicios contratados.

      (ii) Contextualizarlos con un producto o servicio específico dentro de la Entidad. Indicar si su función será complementaria con algún nuevo producto o servicio.

   c) Planear la evaluación de riesgos en relación con el uso de biométricos: establecer su incidencia en cuanto a prevención de fraudes, exposición a nuevos riesgos de carácter cibernéticos, entre otros, sin perjuicio de lo que sea necesario entregar a CNBV en caso de que deba contratarse a un Proveedor Relevante.

   d) Realizar el análisis del o los Proveedores Relevantes, considerando los aspectos mencionados en las Secciones 15 y 16 para determinar los aspectos contractuales

y regulatorios de la contratación, así como un diagnóstico de las capacidades tecnológicas de la Entidad.

e) Realizar un mapa de los procesos y casos de uso para la Entidad de los biométricos considerando las fases de recolección, procesamiento, almacenamiento y validación y evaluar las tecnologías que serán necesarias para realizar satisfactoriamente cada uno de los pasos mencionados.

2) Nombramiento de Partes Responsables para elaboración de un plan de trabajo, cronograma.

3) Sesiones de consulta preliminares entre áreas responsables y Partes Responsables para determinar los cambios legales, operativos y administrativos que serán requeridos para implementar adecuadamente los biométricos.

4) Evaluación de Proveedores Relevantes en materia tecnológica para permitir la implementación adecuada de los biométricos (ver Sección 15 Contratación de Proveedores y Comisionistas).

5) Presentación del Proyecto al Consejo de Administración por parte del Director General para su aprobación, discusión y modificación. Es recomendable que en esta sesión el propio Consejo de Administración o, en su caso, el Director General nombren a un Administrador del Proyecto que tenga facultades suficientes para verificar el cumplimiento de las metas y los hitos del Proyecto y que cada Parte Responsable nombre a una persona como enlace que se encuentre comprometido con los fines del Proyecto.

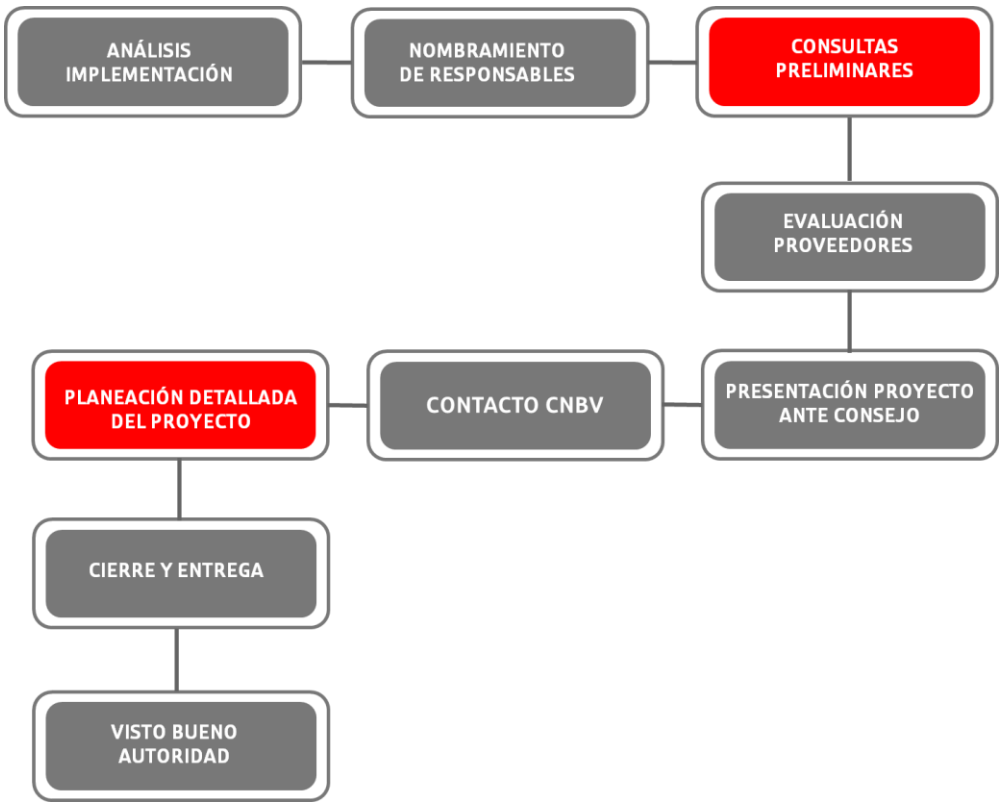
6) Presentación preliminar del Proyecto ante la CNBV mediante el uso de materiales informativos donde se detalle (i) el caso de uso concreto del dato biométrico dentro de la Entidad, (ii) el diagnóstico preliminar de riesgos, (iii) las necesidades y cambios tecnológicos y operativos que implicará la implementación de los biométricos, (iv) la manera en que la Entidad llevará a cabo todo el "ciclo" de vida o implementación de los biométricos.

7) Planeación detallada del Proyecto. Es necesario que el Director General exprese con claridad a las Partes Responsables, incluyendo a las áreas internas, la necesidad de involucrarse y asumir responsabilidad concreta frente al Proyecto.

8) El cierre y la entrega de este tipo de Proyectos deben estar coordinados y aprobados por todas las áreas y no ocurre sino hasta que CNBV haya otorgado las autorizaciones correspondientes (por ejemplo, para el Proveedor Relevante o llevar a cabo la identificación a distancia conforme a las disposiciones PLD/FT). Asimismo, deben estar alineados los temas de cumplimiento, operativos, control interno y prevención de lavado de dinero

9) La finalización típicamente coincide con el visto bueno o autorización de parte de CNBV, la presentación del cierre ante el Consejo de Administración y la aprobación d las modificaciones a los Manuales existentes en lo aplicable.

Plan de trabajo para implementar el uso de biométricos



Gráfica 16. Plan de trabajo para implementar el uso de biométricos. Fuente: Vite Abogados

17.7 Regulador.

El acercamiento con CNBV es importante, previo al uso de factores biométricos de autenticación debido a que en la mayoría de los supuestos donde deben ser usados son la identificación de los Usuarios. En ese sentido la aproximación, como se ha referido en otras secciones, debe ser lo suficientemente informada y consensuada entre las áreas relevantes para permitir a los funcionarios hacerse una idea clara de las implementaciones que se desea llevar a cabo en la Entidad (ver Sección 17 Uso de Biométricos).

17.8 Temas prácticos y recomendaciones.

La regla general (por razones de costos, tiempos) es que la implementación se realice a través de un Proveedor Relevante. En ese sentido las consideraciones sobre temas prácticos de contratación descritas en la Sección 16 (Prestadores de Servicios Operativos) de la presente Guía Legal serían aplicables. No obstante, por la especificidad de la materia, sugerimos que el contrato respectivo contenga un clausulado que abarque los siguientes aspectos:

- Indicar y establecer parámetros y umbrales de rendimiento de los sistemas en materia de almacenamiento, recolección, comparación y autenticación. No existe un rendimiento al cien por ciento o perfecto de este tipo de sistemas (por factores humanos o tecnológicos), por lo que el establecimiento de umbrales mínimos de servicio y actividad es vital para lograr una relación productiva con el Proveedor Relevante.
- En el caso de los dispositivos para la toma o almacenamiento de los biométricos, establecer las obligaciones de cuidado que tendrá el Proveedor de Servicios para asegurar que el equipo reciba el mantenimiento adecuado.
- Obligar al Proveedor Relevante a establecer medidas adecuadas de seguridad para el almacenamiento de la información biométrica obtenida de los Socios o clientes.
- Establecer, en términos de la legislación de datos, las obligaciones y deberes que como “Encargado” debe asumir, en su caso, para al tratamiento de los biométricos.
- Asimismo, en materia de protección de datos personales, las Entidades deben ser muy cuidadosas en los siguientes aspectos:

- Avisos de Privacidad: Ajustar los términos del tratamiento de la información a ser obtenida de los clientes de la Entidad. Es necesario ser específico en cuanto los biométricos que se obtendrán y, sobre todo, los fines para los cuales serán utilizados. Los datos deben ser utilizados únicamente para los fines de autenticación e identificación correspondientes
- Políticas de privacidad: Las políticas de privacidad deben corresponder a las modificaciones mencionadas para reflejar el tratamiento aplicable a los biométricos. Asimismo, las medidas de resguardo, seguridad (propias o del Proveedor Relevante) deben quedar debidamente documentadas (sobre todo si se trata de tecnología de cómputo en la nube).

SECCIÓN 18.- MEDIOS DE DISPOSICIÓN.

Los medios de disposición más comunes son las tarjetas de crédito y las tarjetas de débito. Si bien su regulación es similar y su implementación y uso no es exclusiva de las Entidades (como se verá más adelante), ambas guardan diferencias importantes y sus casos de uso son distintos. Hay otros Medios de Disposición, unos antiguos y otros novedosos que están surgiendo con el desarrollo de los teléfonos inteligentes y la progresiva digitalización de los servicios financieros (por ejemplo, la creación de tarjetas virtuales), pero para efecto de esta Guía Legal y por la importancia que guardan nos referiremos únicamente a las tarjetas ("Tarjetas") en sus dos variantes[87]:

- Tarjeta de Débito. La tarjeta de débito permite a los Usuarios realizar pagos directamente desde sus cuentas de depósito utilizando redes de pago. Es decir, el producto o servicio que subyace es necesariamente una cuenta de depósito únicamente si bien sus funcionalidades son similares a las de la tarjeta de crédito, así como los casos de uso: compras en línea, pagos en Terminales Puntos de Venta, entre otros. Elimina el uso de efectivo y cheques. No existe un sobregiro y no se está pidiendo prestado al emisor de la tarjeta para poder utilizarla. Esta está sujeta a requisitos y reglas específicas que se mencionan a detalle en la Sección 18.1 de esta Guía Legal.
- Tarjeta de Crédito. Se trata de un Medio de Disposición que tiene funciones de pago y que tiene como "servicio subyacente" una línea de crédito y las mismas consideraciones (salvo por la existencia de un crédito) de las tarjetas de débito son aplicables a estas. Un caso que es particular es la disposición de efectivo a través de cajeros automáticos o mediante transferencia (si bien algunas tarjetas de crédito lo permiten, pero a costos muy altos). Estos Medios de Disposición permiten gastar más de lo que realmente se tiene debido a su naturaleza crediticia.

Los pagos con tarjeta permiten adquirir productos y servicios de manera instantánea. Actualmente todos los negocios, con el incremento de la digitalización de la economía, dependen de estos Medios de Disposición para funcionar.

[87] Las Entidades pueden expedir tarjetas de débito desde el Nivel I de operaciones. Sin embargo, sólo Entidades con Nivel IV pueden otorgar tarjetas de crédito con base en contratos de apertura de crédito en cuenta corriente.

Los dos Medios de Disposición indicados (salvo por algunas innovaciones que no se tratarán en esta Guía Legal) se presentan como pedazos de plástico utilizados para la adquisición de bienes y servicios. Usualmente ostenta el logo de Visa o Mastercard, la indicación de la entidad emisora, dieciséis dígitos, fecha de expiración, un número de seguridad (CVV) en el reverso, el nombre del titular (en algunos casos), así como otros distintos propios de la marca y del servicio que se está adquiriendo.

18.1 Redes de Medios de Disposición.

La Ley define a los Medios de Disposición como: las tarjetas de débito asociadas a depósitos de dinero a la vista; a las tarjetas de crédito emitidas al amparo de un contrato de apertura de crédito; a los cheques; a las órdenes de transferencia de fondos, incluyendo el servicio conocido como domiciliación; cualquier dispositivo, tarjeta, o interfaz que permita la realización de pagos, transferencias de recursos o disposición de efectivo cuyas operaciones se procesen por medio de las Redes de Medios de Disposición, así como aquellos otros que la CNBV y el Banco de México, de manera conjunta, reconozcan como tales mediante disposiciones de carácter general.

Para comprender a cabalidad dicha definición es necesario tener en cuenta las siguientes definiciones:

- Redes de Medios de Disposición: son la serie de acuerdos, protocolos, instrumentos, interfaces, procedimientos, reglas, programas, sistemas, infraestructura y demás elementos relacionados con el uso de Medios de Disposición.
- Participantes en Redes: es toda persona que de manera habitual preste servicios relacionados con las Redes de Medios de Disposición.
- Adquirente: es el Participante en Redes que de conformidad con el contrato que haya celebrado con una Cámara de Compensación[88] para pagos con tarjetas, provea servicios de pagos a receptores de pagos o a Agregadores, en las Redes de

[88] **Cámara de Compensación:** es la entidad central o mecanismo de procesamiento centralizado, a través del cual se intercambian instrucciones de pago u otras obligaciones financieras, relacionadas con cualquier Medio de Disposición.

Pagos con Tarjetas y, en su caso, provea la infraestructura de TPV[89] conectadas a estas últimas redes; por ejemplo, un Banco[90].

- Emisor: es el Participante en Redes que expide tarjetas y que, a través de la Cámara de Compensación para pagos con tarjeta recibe las solicitudes de autorización de pago que le dirige el Adquirente y genera las respectivas autorizaciones de pago, rechazos de pagos, devoluciones y ajustes, con el objeto de ser enviados al receptor de pagos a través de la cámara y al Adquirente que corresponda.
- Titular de Marca: es el Participante en Redes que sea titular de una marca susceptible de utilizarse en tarjetas y que otorga bajo un contrato, licencias para su uso a Emisores en la emisión de Tarjetas, y a Adquirentes en la prestación de servicios relacionados con ellas. Un ejemplo de Titular de Marca es VISA y MASTERCARD.
- Agregador: es el Participante en Redes que sea titular de una marca susceptible de utilizarse en tarjetas y que otorga bajo un contrato, licencias para su uso a Emisores en la emisión de tarjetas, y a Adquirentes en la prestación de servicios relacionados con ellas. A modo de ejemplo, enunciamos empresas como Clip y Sr. Pago.
- Empresa Especializada: es el Participante en la Redes que prestan servicios solo a los Participantes en la Red de pagos con tarjeta que sean necesarios para que dichos sujetos puedan llevar a cabo las respectivas actividades.
- Receptor de Pagos: es la persona física o moral que, con motivo de la celebración de un contrato de prestación de servicios con un Adquirente o Agregador, acepta pagos con tarjeta por medio de Terminal Punto de Venta u otros dispositivos conectados a la red de pagos con tarjetas que el Adquirente o Agregador ponga a su disposición, y es quien a su vez inicia la solicitud de autorización a través del Adquirente o Agregador y recibe la aceptación o rechazo de esta, a través del mismo Adquirente o Agregador.

En la práctica esto se conoce como sistema de cuatro partes: se trata de la colaboración de los Participantes en Redes con el objeto de llevar a cabo operaciones de pago mediante

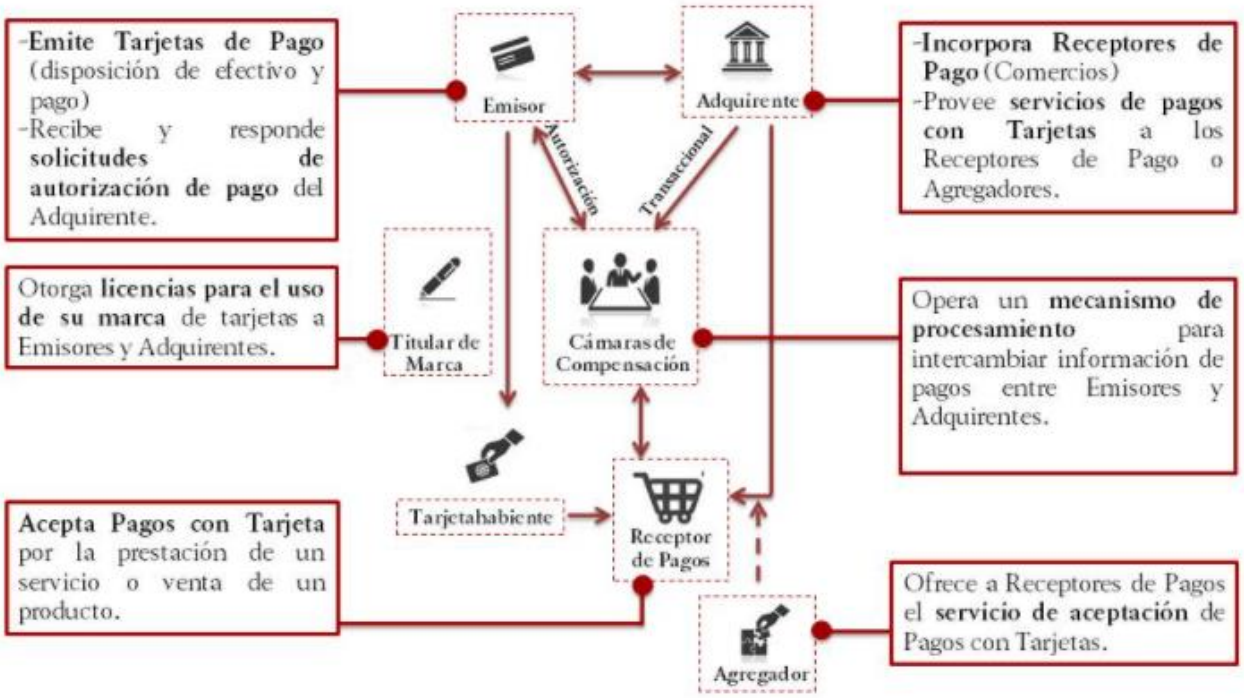
[89] TPV, Terminal Punto de Venta.

[90] Para ver los Adquirentes relevantes ver este link: https://www.cnbv.gob.mx/Paginas/BusquedaEntidades.aspx

los Medios de Disposición. De manera resumida el funcionamiento podría esquematizarse de la siguiente manera:

- Primero se encuentra al "Emisor" de la Tarjeta. La función de un Emisor (que en este caso podría ser una Entidad) es respaldar al Usuario mediante la apertura de una cuenta bancaria y su correspondiente Tarjeta de Débito o través del otorgamiento de crédito y la emisión de una tarjeta de crédito. El Emisor necesita un proveedor de tecnología que pueda conectarse con las Redes de Medios de Disposición. Esta tecnología, como lo hemos mencionado anteriormente, puede ser propia o proveída por un tercero (un Proveedor Relevante).
- Luego está el "Receptor de Pagos": es la persona que lleva a cabo la aceptación del pago realizado a través de Tarjetas. Se le refiere también como el "comerciante", el cual, si tiene una ubicación física, necesita una máquina que pueda leer la Tarjeta proporcionada por un cliente: una Terminal Punto de Venta (TPV). En caso de los Receptores de Pago que operan negocios en línea, estas TPV pueden ser un software.
- El Titular de la Marca otorga una licencia para el uso de su marca dentro o como parte de las tarjetas a Emisores y, en su caso, a los Adquirentes.
- El usuario de la Tarjeta la presentará con algún Receptor de Pagos. Éste recibe los pagos con Tarjeta a cambio de la prestación de un servicio o venta de un producto.
- La presentación de la Tarjeta en una TPV en posesión de un Receptor de Pago no es suficiente. Se necesita un enlace entre la Tarjeta y las Redes de Medios de Disposición, el cual provee la Cámara de Compensación. Ésta pone en marcha un mecanismo de procesamiento para intercambiar información entre Emisores y Adquirentes, en la cual el Emisor recibe y responde solicitudes de autorización de pago por parte del Adquirente. Ejemplos de lo anterior incluyen a Visa y Mastercard. Las Cámaras de Compensación establecen las reglas y estándares de comunicaciones que los Adquirentes y Emisores deben cumplir.
- Finalmente, pero no de menor importancia, todo lo anterior asume que existe una conexión de internet que puede soportar las transacciones mencionadas anteriormente.

Funcionamiento de las Redes de Medios de Disposición



Gráfica 17. Funcionamiento de las Redes de Medios de Disposición. Fuente: CNBV

Se debe puntualizar, a riesgo de ser redundante con lo expuesto en secciones anteriores, que el proceso descrito es distinto tratándose de Tarjeta de crédito o de débito en lo siguiente:

- En las Tarjetas de crédito, el Emisor se obliga a pagar por cuenta del tarjetahabiente los bienes, servicios y, en su caso, el efectivo que proporcionen los establecimientos a los tarjetahabientes;

- En las Tarjetas de Débito, el Emisor sólo comprueba la disponibilidad de efectivo en la cuenta subyacente en la Tarjeta para autorizar el pago de los bienes, servicios o efectivo.

18.2 Reguladores

Las autoridades que intervienen en la supervisión de los Participantes en Redes (y por lo tanto en todo el ciclo de uso de las Tarjetas) son la CNBV, Banxico y Condusef.

- CNBV: a este organismo le corresponde la supervisión de los Participantes en Redes, dicha supervisión se realiza respecto a los términos y condiciones en las que los Participantes en Redes presten servicios relacionados con las Redes de Medios de Disposición, así como las Cuotas de Intercambio[91], Tasas de Descuento[92] y Comisiones[93] que se cobren directa o indirectamente por estos servicios. Lo anterior, con el fin de fomentar la competencia en la prestación de servicios relacionados con los Medios de Disposición, proteger los intereses de los usuarios finales de dichos servicios, promover el libre acceso de los Participantes en Redes a la infraestructura de las Redes de Medios de Disposición y evitar la existencia de términos discriminatorios en las reglas de dichas redes.
- Banco de México está facultado para regular el funcionamiento y la operación de las Cámaras de Compensación de Medios de Disposición, así como los cargos que éstas efectúen por la realización de sus operaciones.
- Condusef: a esta autoridad le corresponde emitir y aplicar la normatividad de las Entidad (por ejemplo, cuando actúan en su carácter de Emisoras) cumplir la publicidad relativa a las características de las operaciones activas, pasivas y de servicios, así como la supervisión de los Participantes en Redes en relación con la prestación de servicios a los usuarios de los Medios de Disposición.
- Conforme al artículo 4 Bis 3 de la LTOSF, los Participantes en Redes deben guiar la prestación de sus servicios conforme a los siguientes principios:
- Competencia, es decir, se debe buscar un balance entre las Cuotas de Intercambio, Comisiones o cobros de cualquier naturaleza relacionados con las Redes de Medios de Disposición, tanto para los usuarios de los Medios de Disposición como de los establecimientos donde se utilicen los Medios de Disposición.
- Libre Acceso, es decir, las Redes de Medios de Disposición deben permitir el acceso a su infraestructura, en condiciones equitativas y transparentes, a todos los Participantes en Redes.
- No Discriminación, es decir, los Participantes en Redes, propietarios de infraestructura relacionada con Redes de Medios de Disposición y demás entidades

[91] **Cuotas de Intercambio**: monto fijo o porcentaje sobre el monto del Pago con Tarjeta que se pagan entre sí Adquirentes y Emisores por los Pagos con Tarjeta, sin importar su denominación o desagregación.

[92] **Tasa de Descuento**: cualquier cobro fijo, variable en función al monto o combinación de estos que efectúa el Adquirente a los Receptores de Pagos, por cada operación de Pago con Tarjeta.

[93] **Comisión:** a cualquier cargo, independientemente de su denominación o modalidad diferente al Interés, que una Entidad cobre a un Cliente.

que tengan injerencia en éstos deberán llevar a cabo sus actividades y permitir las actividades de terceros de forma no discriminatoria, fomentando la interconexión de las diferentes Redes de Medios de Disposición entre sí y el acceso de terceros a las mismas, cuando su naturaleza lo permita.

- Protección de los intereses de los Usuarios, mediante acciones tendientes a procurar:

  (i) La transparencia en el cobro de Comisiones, cuotas o cobros de cualquier clase por cada operación.

  (ii) Que no existan cobros múltiples, directos o indirectos, o por diversas personas por la misma operación o concepto.

  (iii) Que el nivel de cualesquier Cuota de Intercambio o Comisiones sea adecuado para el fomento del uso de Medios de Disposición y no sea discriminatorio.

  (iv) Que el nivel de cualesquier Cuota, incluyendo las de Intercambio, no establezca formalmente o en la práctica "pisos" o "mínimos" inadecuados en el cobro a los comercios o clientes.

18.3 Características de las Tarjetas.

18.3.1 Tarjetas de Débito.

Las Entidades, en la contratación de las operaciones pasivas, pueden emitir Tarjetas de Débito en las formas que ellas determinen, siempre y cuando en ellas se muestre claramente la denominación de la Entidad o cualquier otra expresión, simbología, emblema o logotipo que las identifique.

Las Tarjetas de Débito permiten:

- Disponer de efectivo en las sucursales de la Sociedad emisora, en cajeros automáticos, a través de comisionistas bancarios, así como en negocios afiliados.

- Pagar bienes, servicios, créditos, impuestos, así como para realizar otros pagos que las Entidades permitan a sus Socios.

En los contratos que suscriban con negocios afiliados, las Entidades tendrán la obligación de permitir a los establecimientos optar por aceptar como medio de pago de los bienes y servicios que ofrecen solo Tarjetas de Débito, solo Tarjetas de Crédito, o bien, Tarjetas de Débito y Tarjetas de Crédito, indistintamente.

18.3.2 Tarjetas de Crédito.

Las Tarjetas de Crédito siempre deben expedirse a nombre de una persona física y deben contener los requisitos mínimos contemplados en la normatividad de Banxico[94], entre los cuales se encuentran los siguientes: (i) la mención de ser tarjeta de crédito; (ii) denominación social de la Entidad emisora; (iii) número seriado de la tarjeta de crédito; (iv) nombre del tarjetahabiente y espacio para su firma autógrafa; (v) mención de que su uso sujeta al titular al contrato correspondiente; (vi) mención de ser intransferible; y (vii) fecha de vencimiento.

Además de los requisitos anteriores, tratándose de Tarjetas de Crédito que se emitan con circuito integrado o chip deberán observar los estándares de seguridad, nacionales e internacionales, a los que hacen referencia las reglas de tarjetas de crédito emitidas por Banxico[95], así como cumplir con los procesos establecidos en dichos estándares.

Las personas morales pueden celebrar contratos de apertura de cuenta que se relacionen con Tarjetas de Crédito, sin embargo, éstas siempre se expedirán a nombre de las personas físicas que aquéllas designen.

Las reglas relacionadas con las comisiones y la forma de realizar los cobros relacionados con Tarjetas de Crédito se encuentran en la normativa emitida por Banco de México. En todo caso, las Entidades deberán efectuar cargos en la cuenta por el importe de los pagos de bienes, servicios, contribuciones y disposiciones conforme a las reglas de Banco de México que establecen los supuestos donde deben utilizarse al menos dos elementos independientes para autenticar dichas operaciones.

[94] Circular 34/2010

[95] Circular 34/2010.

Todos los cargos por pagos o disposición de efectivo efectuados en moneda extranjera con la tarjeta de crédito deberán asentarse en la cuenta, invariablemente, en moneda nacional.

Las Entidades sólo podrán emitir y entregar tarjetas de crédito: (i) con previa solicitud del cliente o Socio; (ii) mediante la suscripción de un contrato; (iii) con previa estimación de la viabilidad de pago por parte de los solicitantes; y (iv) con motivo de la sustitución de una tarjeta anterior (para el caso de un Cliente ya existente).

En la entrega de las tarjetas de crédito, las Tarjetas de Crédito siempre deberán entregarse desactivadas y para su activación los Tarjetahabientes deberán solicitarlo expresamente a través de los mecanismos que las Entidades emisoras dispongan para ello, ya sea en alguna de sus sucursales, o bien, a través de un comisionista, mediante el cotejo de la firma autógrafa del propio tarjetahabiente con respecto a alguna identificación de las indicadas en las disposiciones secundarias. Además, la Emisora deberá entregar al tarjetahabiente el NIP que le corresponda, en forma separada de la tarjeta de crédito.

Tratándose de créditos, préstamos o financiamiento revolventes asociados con Medios de Disposición, las Entidades deben:

- Documentar por escrito las operaciones en los formularios que contengan las solicitudes.
- Constar que se dio a conocer al cliente el contenido del contrato.
- Deben constar los datos de inscripción del Contrato de Adhesión en el registro conducente.
- Cuando se envíe el Medio de Disposición, debe enviarse junto con el Contrato de Adhesión y su carátula.

De igual forma, las disposiciones secundarias en materia de transparencia establecen los requisitos mínimos que deben contener los estados de cuenta y los comprobantes de operación de Medios de Disposición.

Existen reglas especiales de publicidad tratándose de Medios de Disposición. Las disposiciones secundarias en materia de transparencia[96] establecen que, tratándose de operaciones de apertura de crédito en cuenta corriente vinculada a una tarjeta de crédito y depósitos a la vista asociados a tarjeta de débito, las Entidades deben utilizar folletos informativos que incluyan, entre otros requisitos:

- Descripción general del producto, servicio u operación;
- Costos y Comisiones; y
- Riesgos.

Existen reglas que tienen que tomar en consideración las Entidades para las tasas de interés en créditos revolventes asociados a una Tarjeta de Crédito, entre estas se debe pactar una sola tasa de interés ordinaria máxima y, en su caso, una sola tasa de interés moratoria máxima. Adicionalmente, las Entidades podrán otorgar tasas de interés promocionales, las cuales en todo caso deberán ser inferiores a la tasa de interés ordinaria máxima, siempre y cuando sus términos y condiciones estén claramente estipulados.

La tasa de interés ordinaria que reflejen los estados de cuenta puede variar sin necesidad de notificación o aviso alguno al cliente, en los siguientes supuestos: (ii) cuando los cambios a la tasa de interés ordinaria sean inherentes a las variaciones en el nivel de la tasa de referencia; y (ii) en caso de que por su vigencia o por comportamiento crediticio del cliente conforme a lo pactado en el contrato, expire una tasa de interés promocional. En cualquier circunstancia, sólo podrá cobrarse intereses sobre los saldos diarios insolutos comprendidos dentro del período de cálculo de intereses del estado de cuenta de que se trate.

18.4 Contracargos en Tarjeta de Crédito.

La Emisora, en el caso de cargos no reconocidos a Tarjetas de Crédito, estará obligada a abonar, en la respectiva cuenta, a más tardar el segundo día hábil siguiente a la recepción de dicho aviso, el monto equivalente a aquellos cargos a esa cuenta que sean objeto del

[96] Disposiciones de carácter general aplicables a las Redes de Medios de Disposición.

aviso de robo o extravío (siempre que dicho aviso se dé conforme a lo establecido en las disposiciones aplicables[97]) y siempre y cuando:

- Los referidos cargos correspondan a operaciones realizadas durante las cuarenta y ocho horas previas a la presentación del aviso de robo o extravío; y

- El aviso de robo y extravío relativo a la reclamación por cargos que el Tarjetahabiente no reconozca como propios, este se haya presentado a la Emisora dentro de un plazo de noventa días naturales posteriores a la fecha en que se realizó el cargo no reconocido. Salvo las excepciones establecidas en las disposiciones.

La Emisora puede determinar libremente el importe del pago mínimo de la tarjeta de crédito, siempre y cuando se cumpla con la normatividad establecida por Banco de México.

18.5 Acercamiento Inicial y Evaluación de Prestadores de Servicios.

Existen aspectos técnicos y operativos importantes donde es necesario involucrar, no sólo al área legal, sino a las áreas operativas, informáticas y de control interno previo a plantear un Proyecto relacionado con la emisión de las Tarjetas. No se trata de que éstas cumplan únicamente con los requisitos mencionados: la operativa, por lo menos para una Entidad sin mucha experiencia al respecto, puede resultar compleja. Como vimos antes, existen muchos elementos y piezas sueltas en los procesos de Redes de Medios de Pago. Toda línea de acciones que inicia desde que alguien solicita una Tarjeta, la desliza en una terminal, se autoriza la transacción, se compensa y se liquidan las cantidades, así como la administración (atención al cliente, supervisión del servicio subyacente, entre otras), es un trabajo que suele cambiar aspectos muy importantes de una Entidad. Obtener la mayor información posible de la manera en que interviene cada participante, los elementos técnicos del viaje de la información en cada paso y la validación y entendimiento amplio de cada proceso son esenciales para entender: qué se debe cambiar dentro de la Entidad y el tipo de Proveedores Relevantes que debe analizarse y contratarse.

[97] Circular 34/2010.

18.6 Diagrama y Plan de Trabajo.

La organización de un esquema de negocio donde se involucre la emisión de Tarjetas debe comenzar con un análisis de las demandas reales de los Socios o clientes. Una vez realizado lo anterior, será necesario determinar los siguientes aspectos:

- Esquema o marca que se desea utilizar para las tarjetas: las más populares en el mercado son VISA y MasterCard, debido a que su aceptación es prácticamente mundial. Esto, dependiendo del esquema de implementación, tiene como consecuencia contar con una licencia o ser miembro de los esquemas de dichas compañías. Éstas tienen varios tipos de licencias, entre las más importantes están la completa o la patrocinada. La membresía total significa que la Entidad tendrá una responsabilidad financiera completa. Por parte, el esquema patrocinado significa que la Entidad encontrará algún miembro de pleno derecho existente dentro de los esquemas del Titular de Marca que será financieramente responsable por la Entidad. El proceso para obtener una licencia lleva tiempo (seis u ocho meses). En la mayoría de los casos, si los volúmenes u operaciones son pequeños, la única opción para comenzar es la membresía patrocinada. Para seleccionar entre VISA o MasterCard es necesario consultar preferencias en el mercado mexicano y, desde luego, los términos y condiciones concretos de cada licencia. En etapas más avanzadas puede pensarse en contar con las dos.

- El siguiente tema es la operación y funcionalidad de las Tarjetas. Asimismo, se necesita contar con una opción para producir Tarjetas y procesar las transacciones relacionadas con ellas. Una transacción corresponde a una serie de mensajes en línea con el propósito principal de verificar la disponibilidad de fondos del titular de una tarjeta y poder completar el pago. Estos mensajes se basan principalmente en versiones de implementación de estándares específicos. La Entidad también debe considerar los ajustes contables y operativos que la administración de Tarjetas conlleva, por ejemplo, crear programas que permitan monitorear y ajustar saldos de las cuentas de los Usuarios. Aquí puede intervenir un tercero que provea los servicios necesarios para efecto de cumplir con esas tareas; incluso existen soluciones completas que también realizan la gestión completa de los datos, los puntos de venta, cajeros, entre otros. Existen varios esquemas que se pueden adoptar para cumplir con lo anterior:

(i) Subcontratar los servicios en su totalidad, de manera que la Entidad reciba solo reportes e información de las transacciones periódicas de tiempo en tiempo para poder ajustar saldos y cuadrar los temas financieros, contables y regulatorios relacionados con la Tarjeta. Esta opción permite que la inversión en infraestructura tecnológica sea relativamente barata, pero existe el riesgo de que el ajuste de los saldos no pueda hacerse de manera rápida o adecuada o que el cliente, al usar otros canales, abuse de la tarjeta sin restricciones.

(ii) Subcontratar partes específicas de los procesos relacionados con la Tarjeta, en el entendido de que existirá una vinculación automática y en línea para la aceptación o rechazo de los montos de las transacciones, así como información que permita determinar si la transacción es segura. Este esquema podría limitar la capacidad de la Entidad de realizar la administración directa de las Tarjetas y ofrecer de manera inmediata soluciones a los Usuarios.

(iii) Vinculación directa con el Titular de Marca y crear una infraestructura tecnológica propia. Esto implicaría la adquisición de programas que permitan realizar la administración de las Tarjetas y realizar una integración completa con los sistemas de la Entidad, lo cual podría resultar largo de implementar y generar costos importantes. Este esquema permite que la Entidad tendrá un soporte para un sistema propio que mantendrá al sistema actualizado. Desde luego existen muchas variantes en la práctica de cómo hacer la integración y manejar las Tarjetas de manera integral desde una infraestructura compartida. Lo anterior, puede implicar cambios importantes a nivel operativo y de riesgos.

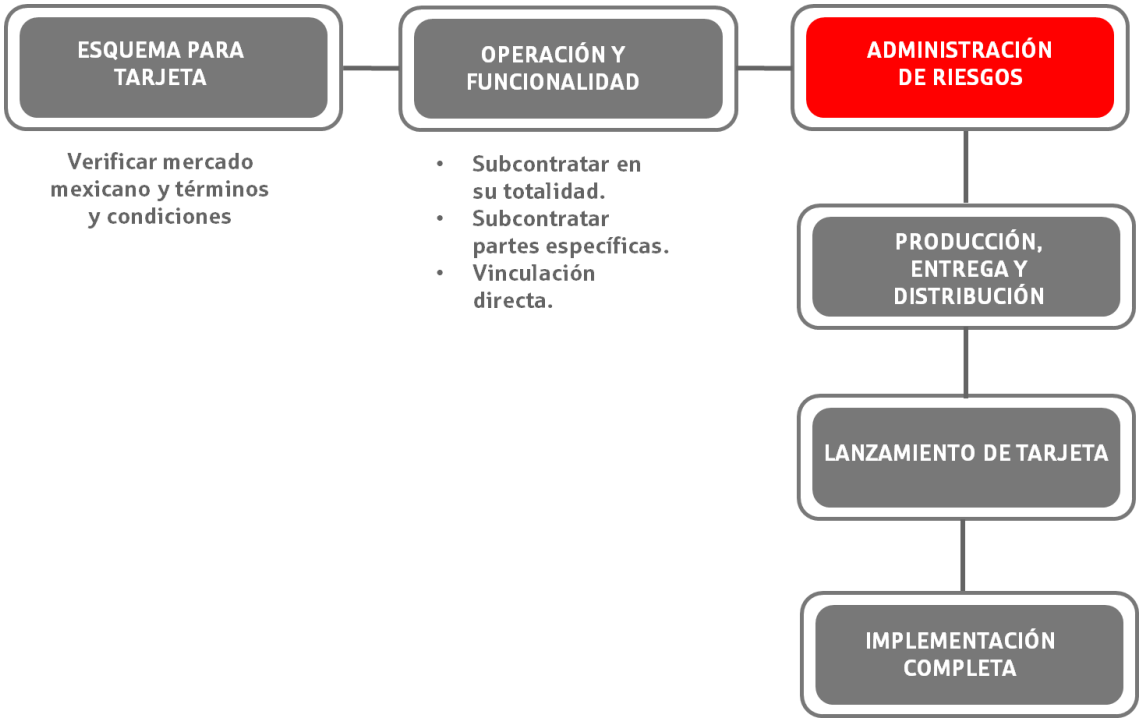
- Realizar ajustes en la manera de administrar los riesgos de fraude relacionados con la Tarjeta. Establecer parámetros que sean acordes con las medidas de seguridad que ya se encuentran integradas a las mismas. Generar políticas sobre ello. Asimismo, es posible que se requiera contratar un programa que permita administrar estos aspectos relacionados con la Tarjeta.

- Los aspectos de producción, entrega y distribución de las Tarjetas deben ser también considerados y ser parte de una planeación integral del Proyecto. Sobre todo, en el entendido de que los Medios de Disposición mencionados en esta sección son Tarjetas de plástico (en el futuro cercano quizás las tarjetas virtuales generadas en aplicaciones móviles podrían prevalecer). La producción incluye aspectos específicos como la personalización de las Tarjetas (nombre de titular, número, entre otros datos que deben almacenarse en el chip y la banda magnética). Existen soluciones completas para todo ello. No es común que el Emisor se encargue por sí mismo de estas tareas: existen especificaciones (no sólo desde el punto de vista legal sino estándares internacionales) que deben ser consideradas para garantizar la seguridad y adecuación de esos Medios de Disposición. Asimismo, deben incluirse elementos como marcas propias y chips. También debe atenderse: elementos técnicos y especificaciones del chip (parámetros de los mismos), generación y resguardo de los NIP (generación propia o tercerizada).

- No quisiéramos redundar en lo que hemos expuesto en secciones anteriores respecto a la Planeación de un Proyecto, pero el lanzamiento de una Tarjeta también implica su asociación a un servicio existente (débito o crédito) y, por lo tanto, genera cambios dentro de la Entidad: canales de distribución y publicidad, procedimientos de identificación y aprobación (de crédito), generación de reportes regulatorios y evaluaciones de riesgos, ajustes en la operativa y en los procesos de administración de la Entidad, cambios o ajustes en la atención al cliente y cambio en los Manuales de la Entidad.

- Una vez que se ha obtenido la licencia de un Titular de Marca y, en su caso, las autorizaciones corporativas y regulatorias para realizar las contrataciones de Proveedores Relevantes que manejen los procesos relacionados con las Tarjetas han sido resuelta es necesario ir de la mano con dichos Titulares para lograr una implementación completa enfocada, no sólo en el Medio de Disposición sino en el procesamiento de las transacciones. Es común que los Titulares de Marca establezcan esquemas operativos que permitan realizar el manejo de la Tarjeta, lo cual conlleva capacitar al personal de la Entidad. Esto es un procedimiento de certificación.

Plan de trabajo para la implementación de medios de disposición en las Entidades



Gráfica 18. Plan de trabajo para la implementación de medios de disposición en las Entidades. Fuente: Vite Abogados

18.7 Temas prácticos y recomendaciones.

Existen en el mercado soluciones "completas" para la emisión de Tarjetas que se encargan de realizar gran parte de los procesos que mencionamos en la sección anterior que, en ocasiones, ofrecen incluso el sublicenciamiento de las marcas (VISA, MasterCard). Sin embargo, al considerarlas la Entidad debe tomar en cuenta los siguientes aspectos en la negociación de los contratos respectivos:

- Verificar los aspectos relacionados con el cumplimiento de estándares en la industria para los procesos de fabricación y embozado (personalización) de las tarjetas.
- Establecer de manera clara cuál será la responsabilidad de este Proveedor en la administración de las transacciones. Es común que se atribuya la responsabilidad

al Titular de la Marca, el cual sin ser parte de este contrato queda fuera de cualquier acción por parte de la Entidad. Se sugiere indicar con claridad cuáles serán los pasos y procesos que desarrollará el Proveedor Relevante por sí mismo y cuáles el Titular de la Marca o un tercero.

- Verificar que el Proveedor Relevante conoce la regulación aplicable a la Entidad y que cumplirá con las características aplicables a las mismas que se describen en secciones anteriores.
- Verificar que el contrato de adquirencia con el Banco Adquirente contenga todas las cláusulas relevantes. Al respecto, ponemos a su disposición en el Anexo 4 del presente documento las cláusulas más relevantes que debe contener el mencionado contrato.
- Indicar los procesos y responsabilidades en el caso de que ocurran los Contracargos, así como la manera de comunicarlo a la Entidad para llevar a cabo un seguimiento adecuado del servicio subyacente (crédito o débito).
- Delimitar las responsabilidades de cada parte del contrato en el caso de que exista un uso inadecuado o fraudulento de las Tarjetas.
- Garantía y niveles de servicio adecuados, vinculando cada uno a supuestos de incumplimiento específicos, así como a penalidades o consecuencias legales que sirvan de disuasión a incumplimientos futuros.
- Establecer esquemas de atención y ayuda a la Entidad para efecto de resolver cualquier tema o contratiempo relacionado con las Tarjetas.
- Identificar a los subcontratistas del Proveedor Relevante, así como el ámbito de su responsabilidad en todo el proceso y, de ser posible, tratar de involucrarlos en el propio contrato.
- Incluir estándares de continuidad y de servicio.
- Incluir, en su caso, el clausulado regulatorio mínimo, y atender los temas de protección de datos personales que pudieran estar involucrados en el esquema[98].

[98] Las cláusulas que deben incluirse en el contrato serían las aplicables para Proveedores Relevantes, entre las que se encuentran:
a) Recibir visitas domiciliarias por parte del auditor externo de la Sofipo, del Comité de Supervisión o de la Comisión o terceros que la propia CNBV designe, a efecto de llevar a cabo la supervisión correspondiente, con el exclusivo propósito de obtener información para constatar que los servicios o comisiones contratados por la Sofipo, le permiten a esta última cumplir con las disposiciones de la Ley que le resultan aplicables. Para que se realicen las visitas referidas, las Sofipo podrán designar un representante.
b) Aceptar la realización de auditorías por parte de la Sofipo, en relación con los servicios o comisiones objeto de dicho contrato, a fin de verificar la observancia de las disposiciones aplicables a las Sofipo.
c) Entregar a solicitud de la Sofipo, al auditor externo de la propia sociedad y a la Comisión o al Comité de Supervisión, libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate.

- Establecer rangos máximos en cuanto a los costos de procesamiento y no dejar la puerta abierta al cobro de cuotas u honorarios no especificados que pudieran generarse por procesamiento de transacciones (por ejemplo, del Titular de la Marca).
- Tiempos de respuesta específicos por parte del Proveedor para el desahogo de cada parte del proceso y administración de la Tarjeta, según se acuerde.

Asimismo, permitirá que se tenga acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la prestación del servicio en cuestión.
d) Informar a la Sofipo con por lo menos treinta días naturales de anticipación, respecto de cualquier reforma a su objeto social o en su organización interna que pudiera afectar la prestación del servicio objeto de la contratación.
e) En su caso, guardar confidencialidad respecto de la información relativa a las operaciones activas, pasivas y de servicios que los comisionistas celebren con los Clientes, así como la relativa a estos últimos
Los requerimientos de información y, en su caso, las observaciones o medidas correctivas que deriven de la supervisión que realice la CNBV en términos de las disposiciones aplicables, se realizarán directamente a la Sofipo. Asimismo, la CNBV podrá, en todo momento, ordenar la realización de las visitas y auditorías señaladas en los incisos a) y b) anteriores, precisando los aspectos que unas y otras deberán comprender, quedando obligada la propia sociedad a rendir a la CNBV un informe al respecto.

El clausulado es prácticamente idéntico para las Cajas de Ahorro.

SECCIÓN 19.- SISTEMAS DE PAGOS.

Un "Sistema de Pagos" es un conjunto de instrumentos, procedimientos bancarios y, por lo general, sistemas interbancarios de órdenes de transferencia de fondos o de liquidación de órdenes de transferencias aceptadas que aseguran la circulación del dinero.

Para llevar a cabo la compensación o liquidación de ordenes de transferencia, un Sistema de Pagos debe reunir, principalmente, los siguientes requisitos:

- Que participen, directa o indirectamente, al menos tres sociedades autorizadas para actuar como instituciones financieras y
- Que el monto promedio mensual de las obligaciones de pago que acepte el procedimiento de que se trate para su compensación o liquidación en un año calendario, sea igual o mayor al equivalente a cien mil millones de unidades de inversión.

Las operaciones que se celebran a través de los sistemas de pagos en México están sujetas a la Ley de Sistemas de Pagos, así como a la legislación financiera que en cada caso resulte aplicable. En todos los casos, estas reglas son de carácter federal.

Uno de los Sistemas de Pagos más importantes es el Sistema de Pagos Electrónicos Interbancarios (SPEI). En palabras del propio Banco de México, SPEI[99]:

- Constituye la infraestructura de pagos del Banco de México que permite a sus participantes enviar y recibir pagos entre sí para poder brindar a sus clientes finales el servicio de transferencias electrónicas en tiempo real.
- Puede conceptualizarse como una tubería central a la que se conectan los participantes, sobre la cual, de manera eficiente y segura se cargan y abonan las cuentas de los participantes con el Banco de México para poder liquidar las operaciones entre participantes, ya sea que hayan sido enviadas por cuenta propia o por cuenta de sus clientes.

[99] Banco de México. (2018) ¿Qué es y cómo funciona el SPEI? Consultado en: https://www.banxico.org.mx/spei/d/%7B44351472-054C-58EB-611D-153B1029C2A8%7D.pdf

- Para realizar esa conexión con el SPEI los participantes realizan desarrollos propios o contratan a terceros para que les brinden ese servicio

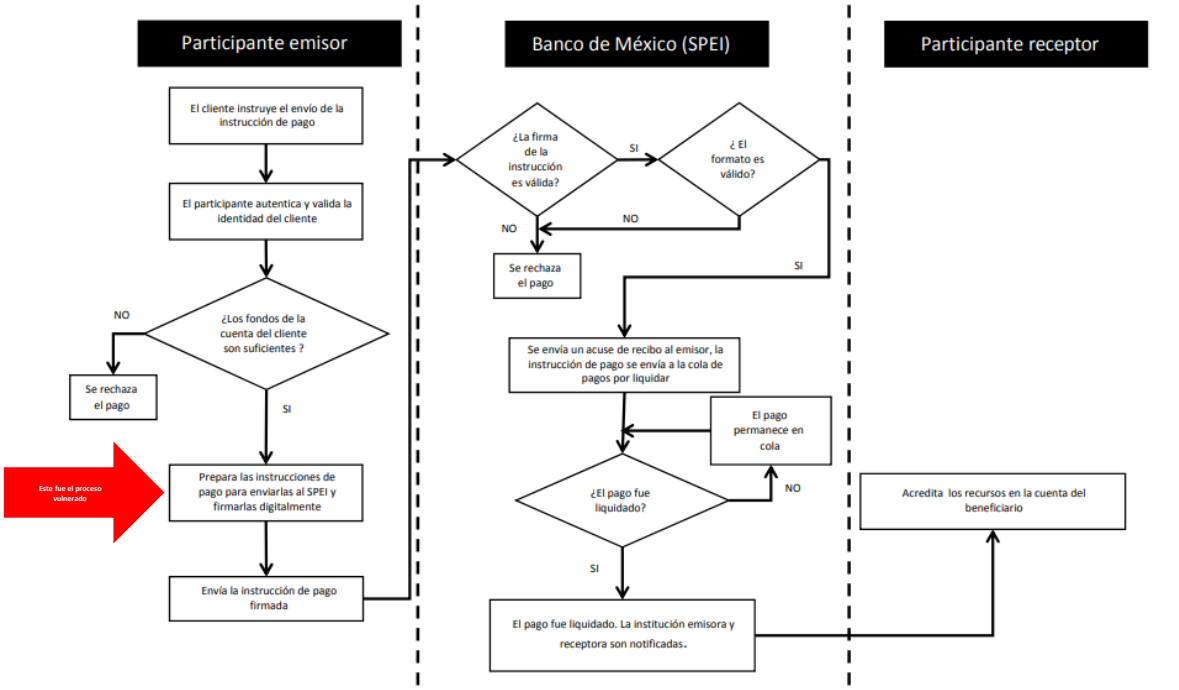
El funcionamiento del SPEI, descrito también por el propio Banco de México[100], es el siguiente:

- El cliente final (cuentahabiente) instruye desde su banca electrónica o aplicación móvil a su institución participante los pagos que desea realizar. Esto se hace siguiendo controles de seguridad como contraseñas, elementos dinámicos (tokens) y pruebas de posesión de dispositivos (como mensajes a teléfonos móviles pre registrados), entre otros.
- El participante valida los elementos de seguridad de la instrucción y guarda evidencia de que realizó esta validación.
- El participante prepara las instrucciones de sus clientes, les incluye elementos de seguridad adicionales (sujeto a la Circular 14/2017), sobre los cuales únicamente ellos tienen el control, y los envían al SPEI de Banco de México.
- El Banco de México verifica las firmas electrónicas de los participantes, que dan certeza de la integridad de la instrucción de pago, y procede a su procesamiento y posterior liquidación al participante receptor del pago.
- Se informa a los participantes involucrados en la transferencia de recursos de la liquidación y el participante receptor del pago acredita los fondos en la cuenta de su cliente y envía al Banco de México la información para generar el Comprobante Electrónico de Pago (CEP).

De manera esquemática puede resumirse de la siguiente manera:

[100] *Op. Cit.* Banco de México. (2018)

Diagrama de funcionamiento del SPEI



Gráfica 19. Diagrama de funcionamiento del SPEI. Fuente: Banco de México. [101]

19.1 Ingreso a los Sistemas de Pagos.

El movimiento electrónico de dinero juega un papel muy importante en la economía mexicana. El sector de pagos y su desarrollo tienen un impacto muy profundo en la progresiva bancarización de los sectores informales de nuestro país. La interacción realizada con base en dinero “inmaterial” a través de internet es un instrumento de inclusión financiera que aún debe desarrollarse con mayor profundidad en México.

Banco de México, como el organismo constitucionalmente autónomo encargado de garantizar el buen funcionamiento de los sistemas de pagos (entre otras tareas), se ha dado también a la tarea de apoyar la inclusión financiera a través de éstos.

Como lo menciona un estudio del CEMLA[101], el uso de los sistemas electrónicos de pagos tiene los siguientes beneficios inmediatos y tangibles en una economía:

- Reducción de costos transaccionales y menor fricción en la transferencia de recursos.
- Reducción de la importancia de factores geográficos en la posibilidad de bancarización debido a la prevalencia de medios electrónicos.
- Reducción de los riesgos asociados con el manejo de dinero en entornos de inseguridad, así como facilidad en el manejo de las finanzas propias.
- El uso masivo de instrumentos electrónicos de pago pone las bases para usos más sofisticados y complejos de los sistemas de pagos y produce un efecto positivo en la competencia por mejores herramientas.

Para que una persona en su carácter de usuario puede realizar transferencias a través de SPEI es necesario:

- Tener una cuenta abierta en una entidad financiera con servicio de banca por internet o el servicio de banca móvil.
- El servicio de transmisión o pagos mediante SPEI se solicita directamente con la entidad financiera donde está abierta la cuenta.
- La entidad financiera debe ser un "participante" del SPEI (Participante de SPEI), pues no todas las instituciones que forman parte del sistema financiero mexicano están automáticamente autorizadas para hacer uso de dicho sistema.
- Conocer la Clave Bancaria Estandarizada (CLABE) de la cuenta (18 dígitos), el número de tarjeta de débito (16 dígitos) o el número del teléfono celular (10 dígitos) asociado a la cuenta de la persona o empresa a la cual se le hará la transmisión.
- Cumplir con los demás requisitos en materia de Banca Electrónica que sean aplicables a la Entidad de que se trate.

[101] CEMLA. The Role Payments Systems (Internet) Consultado en: https://www.cemla.org/PDF/forodepagos-TheRolePaymentSystems.pdf

19.2 Acceso a SPEI.

Como lo comentamos anteriormente, el SPEI permite al público en general realizar transferencias de cantidades monetarias mediante "Ordenes de Transferencia" (es decir, la instrucción incondicional emitida por un Participante SPEI a través de un Sistema de Pagos, a otro Participante SPEI, para que ponga a disposición del beneficiario designado en dicha instrucción, una cantidad determinada en moneda nacional en este caso), liquidadas por medio del propio sistema con posterioridad a su envío.

El SPEI es considerado un "sistema de pagos híbrido[102]" que procesa órdenes de transferencia prácticamente en tiempo real: la frecuencia con la que el SPEI liquida pagos depende de los procesos que tenga que ejecutar. En promedio, este sistema liquida los pagos en 1.9 segundos y los resultados se liquidan inmediatamente en las cuentas de efectivo de los participantes en el SPEI.

El SPEI usa un protocolo de comunicación abierto y propietario, es decir, el protocolo fue específicamente diseñado para el SPEI y no depende de una arquitectura, lenguaje de programación o sistema operativo determinado. Este sistema ha sido desarrollado y operado por el Banco de México y su seguridad se basa en mensajes firmados digitalmente, por lo que los participantes usan los certificados digitales y las claves de personas autorizadas. Estas operaciones se realizan a través de un ambiente o red privada y protegida y el uso de un dispositivo de seguridad ya sea un token o una tarjeta de seguridad[103].

El SPEI realiza diversas validaciones a los pagos que se procesan en el sistema. Cuando recibe una orden de transferencia, el SPEI verifica el tamaño y la estructura del mensaje, y la validez de la firma electrónica. Si la firma del banco emisor es válida y la estructura del pago es correcto, los pagos recibidos están listos para entrar al proceso de liquidación. El

[102] La diferencia entre los sistemas de liquidación bruta en tiempo real (LBTR) y los sistemas de liquidación neta diferida, LND (o a una hora determinada), radica en la forma y la hora de la liquidación, y no en la forma en que los mensajes de pago se procesan o transmiten. Los sistemas LND pueden procesar órdenes de pago en tiempo real, pero liquidan en lotes y en términos netos a horas predeterminadas, ya sea durante el día operativo o, más comúnmente, al final del día. Por otro lado, los sistemas de LBTR liquidan los pagos en cuanto son aceptados por el sistema, operación por operación. Los sistemas híbridos: combinan la pronta liquidación final lograda en sistemas de liquidación bruta en tiempo real con la eficiencia del manejo de la liquidez de los sistemas con liquidación neta diferida.

[103] Banxico. Sistema de Pagos Electrónicos (Internet) Consultado en: https://www.banxico.org.mx/servicios/sistema-pagos-electronicos-in.html

Banco de México genera avisos de liquidación, los firma y los envía a los participantes beneficiarios, quienes deberán abonar los recursos a las cuentas de los clientes receptores[104].

Pueden actuar como Participantes del SPEI:

- Entidades sujetas a la regulación en el ámbito federal, en materia financiera, así como a la supervisión del Banco de México, la CNBV, la Comisión Nacional de Seguros y Fianzas o la Comisión Nacional del Sistema de Ahorro para el Retiro;
- Las dependencias o entidades de la Administración Pública Federal;
- El Banco de México, en su carácter de fiduciario en los fideicomisos respectivos,
- Cualquier institución distinta a una entidad financiera regulada, que opere un sistema internacional de liquidación de operaciones cambiarias que incluyan al peso como una de las divisas participantes.

Además de lo anterior, para ser admitidos como Participantes del SPEI, los interesados deben cumplir con los requisitos, términos y condiciones establecidos en las presentes en la Circular 13/2017 y llevar a cabo un proceso específico para ello.

Los futuros Participantes de SPEI deben acreditar, previo a su ingreso, requisitos técnicos, de seguridad informática y de gestión del riesgo operacional. Los requisitos de acceso de todos los Participantes de SPEI son esencialmente los mismos, por lo que existe un trato equitativo para el ingreso al sistema.

Dentro de los requerimientos de acceso a SPEI, se encuentran los siguientes:

- Solicitud de Admisión. Presentar una solicitud de admisión por escrito señalando expresamente su voluntad de sujetarse incondicionalmente a las disposiciones de Banco de México aplicables y a las normas internas.
- Informes Técnicos. La solicitud se acompaña de una serie de informes técnicos, tales como: (i) informe de cumplimiento que indique que el interesado cumple con

[104] *Ibidem.*

los requisitos previstos en la normativa emitida por el Banco de México[105]; (ii) informe de cumplimiento que indique cómo se da cumplimiento a cada requisito; y (iii) informe de cumplimiento en el que se indique el nivel de cumplimiento de los requisitos, así como cualquier otro riesgo identificado.

En relación con el informe de cumplimiento mencionado en el inciso (i) anterior, hacemos de su conocimiento que el Banco de México solicita que los Participantes cumplan los siguientes requisitos, entre otros, para poder actuar como tales: (i) requisitos de seguridad informática, tales como políticas y procedimientos documentados que se obligue a seguir la Entidad en materia de seguridad informática, un área designada responsable de la seguridad informática, políticas que se obligue a seguir la Entidad para un manejo seguro de la información electrónica que contenga procedimientos de desechamiento o dada de baja de los componentes. Para restringir el acceso a los puertos físicos, para el resguardo de la información, para detectar la alteración o falsificación de la información, entre otros; (ii) requisitos de gestión del riesgo operacional, tales como una metodología para la administración del riesgo operacional relacionada con la operación con el SPEI, una metodología de análisis de impactos al negocio, procedimientos de contratación y capacitación del personal para asegurar que el personal relacionado con el SPEI cuente con las habilidades y conocimientos suficientes para operarlo, medidas de mitigación de los riesgos, procedimientos de recuperación y restauración de la operación con el SPEI ante la materialización de alguno de los riesgos, una política de continuidad, entre otros; (iii) requisitos de protección a los clientes de quien suscribe la solicitud de admisión, tales como sistemas y medidas de control que aseguren que el procesamiento de las órdenes de transferencia de los clientes será completamente automatizado, que el interesado podrá ofrecer la posibilidad de realizar órdenes de transferencia a nombre y por cuenta de sus clientes emisores en un esquema no automatizado exclusivamente en situaciones de contingencia, entre otros; y (iv) requisitos en materia de riesgos adicionales para la administración como participante, los cuales se refieren predominantemente a requisitos para evitar la comisión del delito de lavado de dinero o financiamiento al terrorismo.

Además, debe acompañarse de la documentación, información, dictámenes y certificaciones que acrediten que cumple con los requisitos técnicos, operativos y de gestión de riesgos necesarios para el buen funcionamiento del sistema de pagos previstos

[105] Disposiciones 57ª, 58ª y 62ª de la Circular 14/2017.

en las normas internas del Banco de México. En particular, debe estar claro que el interesado observa los requisitos de seguridad informática, de gestión del riesgo operacional, de protección de clientes emisores, de interoperabilidad y de gestión de riesgos adicionales relacionados con el uso del SPEI para la realización de actividades ilícitas

Cabe señalar que Banco de México podrá requerir documentación e información adicional que estime necesaria para evaluar la procedencia de otorgar la autorización solicitada.

- Convenios con Banco de México. Se deben celebrar los siguientes convenios con Banco de México:

  (i) Convenio suscrito por el representante legal del interesado en términos del clausulado que Banco de México ponga a su disposición una vez que lo solicite.

  (ii) Convenio de colaboración para la protección de clientes emisores.

- Políticas de Seguridad. Elaborar una política y procedimientos en que el futuro Participante de SPEI: (i) se obligue a seguir en materia de seguridad informática con los requisitos establecidos en las disposiciones del Banco de México; (ii) se obligue a seguir en materia de pruebas de confianza e integridad que deba aplicar a aquellos miembros de su personal, así como a terceros que provean servicios en materia de tecnologías de la información y comunicación, que tengan acceso a información y sistemas relevantes en la operación con el SPEI; (iii) se obligue a seguir los requisitos establecidos en las disposiciones del Banco de México para la administración de riesgos; y (iv) apliquen y establezcan medidas de mitigación de los riesgos establecidas en las disposiciones del Banco de México.
- Requisitos de Contratación con Terceros. Además de la solicitud de autorización, se deben cumplir con requisitos especiales en caso de que se vaya a contratar con un tercero:

  (iii) En caso de que se contrate con terceros la interfase que les permita conectarse con el SPEI o algún otro servicio esencial para el procesamiento de órdenes de transferencia, se debe presentar una solicitud de

autorización al Banco de México por conducto de la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos. Junto con la solicitud, deberán proporcionar: (i) el proyecto de contrato que pretenda celebrar con el tercero, (ii) aprobación de sus consejos de administración, (iii) documentos que acrediten la experiencia, calidad técnica y suficiencia de recursos del tercero, entre otros.

(iv) En caso de que el interesado quiera contratar con terceros que presten el servicio total o parcialmente fuera de territorio nacional, deberán proporcionar, además de lo indicado en el numeral anterior, lo siguiente: (i) acreditar que los terceros residan en países cuyo derecho proteja los datos de las personas; (ii) prever el instrumento donde conste la aprobación de los consejos de administración; (iii) contar con esquemas de soporte técnico que permitan solucionar problemas e incidencias con independencia de las diferencias de husos horarios y días hábiles, entre otras.

(v) Además de lo anterior, el interesado deberá obtener autorización previa y por escrito de Banco de México para efectuar cualquier modificación al contrato que hayan celebrado con el tercero e informarle sobre cualquier reforma al objeto social del tercero o modificaciones a la organización interna que puedan afectar la prestación del servicio.

- Políticas en materia PLD/FT. Establecer políticas en materia PLD/FT para efecto de: (i) identificar a las personas que solicitan las disposiciones aplicables del Banco de México y (ii) contar con políticas y procedimientos documentados en materia de prevención de recursos de procedencia ilícita que incluyan, al menos, las actividades que realizarán para identificar las cuentas que establecen las disposiciones del Banco de México.

19.3 CoDi.

La plataforma de Cobro Digital (CoDi) ha sido desarrollada y operada por Banco de México para facilitar las transacciones de pago y cobro a través de transferencias electrónicas, de forma rápida y segura a través de teléfonos móviles en un esquema que opera veinticuatro horas los trescientos sesenta y cinco días del año. En palabras de Banco de México: "*Su*

objetivo es realizar pagos electrónicos mediante un esquema en el que el pago es solicitado, por quien sería el receptor de los fondos, desde un dispositivo móvil o desde internet y el emisor del pago lo autoriza desde su propio dispositivo. De esta forma, se busca que la plataforma CoDi proporcione un medio de pago seguro y eficiente a los pequeños comercios, a los comercios electrónicos, a los proveedores de servicios y al público en general para realizar cobros con las ventajas de seguridad y eficiencia de las transferencias electrónicas[106]".

CoDi usa la tecnología de los códigos QR, NFC e Internet:

- QR: (de respuesta rápida) consiste en un código bidimensional, a través del cual se almacenan datos en patrones de puntos dentro de un cuadrado para después ser leídos y mostrados desde una aplicación (app) en un teléfono celular.
- NFC: (comunicación de campo cercano) se basa en la transmisión de datos e información mediante la aproximación de dos dispositivos móviles entre sí.
- Mensajes vía internet: permiten enviar a través de este medio las solicitudes de pago directamente al dispositivo móvil del usuario de manera similar a las producidas por aplicaciones de mensajería instantánea.

CoDi no cuenta con una regulación específica: su implementación se encuentra como extensión y modificación a la regulación existente de SPEI, por lo que cualquier análisis legal debe considerarlo como tal. Entre los "usuarios" potenciales del SPEI se encuentran:

- Participantes de SPEI, es decir entidades reguladas que hayan realizado el proceso de acceso descrito anteriormente en esta sección y que estén facultadas para realizar y operar transacciones a través de SPEI.
- Tercero Desarrollador, es decir, un interesado en desarrollar aplicaciones móviles, aplicativos para comercios electrónicos o programas informáticos con la funcionalidad de cobro mediante CoDi (exclusivamente debido a que los Participantes de SPEI son las únicas entidades que pueden poner a disposición del público la funcionalidad de pago del CoDi). Dicha tecnología deberá ser registrada

[106] Banco de México. Exposición de Motivos.

y certificada por el Banco de México. Los desarrollos registrados y certificados podrán ser comercializados o puestos a disposición del público en general. Los terceros desarrolladores solo podrán desarrollar software con funcionalidad de cobro, ya que los Participantes de SPEI son las únicas entidades que pueden poner a disposición del público en general la funcionalidad de pago en CoDi.

- Comercio Desarrollador, pueden ser comercios que desarrollan aplicaciones móviles, funcionalidad o programas que interactúan con puntos de venta para poder realizar cobros con CoDi. De manera similar al Tercero Desarrollador, deben obtener cierta documentación técnica, así como registrar y certificar el desarrollo a través de los procesos que Banco de México ha establecido para ello. No todos los comercios que deseen participar en CoDi requieren del desarrollo de un programa.

Desde nuestro punto de vista, lo que podría resultar relevante (y jurídicamente posible) para las Entidades es fungir como Participantes de SPEI y, de manera adicional, proporcionar el servicio de CoDi a sus Socios o Clientes.

19.4 Acercamiento Inicial.

La inclusión de las Entidades como Participantes de SPEI requiere una planeación cuidadosa e implica un uso importante de recursos. Al mismo tiempo, el acceso a este sistema de pago puede representar un avance muy importante en las Entidades, pues podría permitir ampliar la oferta de servicios, reducir la dependencia de servicios tercerizados y hacer más atractiva su oferta de servicios.

Acceso a SPEI puede otorgar una ventaja competitiva de las Entidades frente en el sector, sin embargo, SPEI es sólo una herramienta. La manera de desarrollar las capacidades que ofrece dicho servicio requiere de un desarrollo particular: no se trata solamente de tener acceso al mismo, sino de desarrollar herramientas que permitan al Socio o Usuario utilizar un servicio atractivo y eficiente. En este caso la planeación también pasa por los temas ya referidos de Banca Electrónica y PLD/FT, así como los temas tecnológicos y operativos que inciden en una nueva oferta de servicios.

En ese sentido las Entidades deben planear un acceso a SPEI considerando un marco de tiempo aproximado, así como un presupuesto que esté a su alcance. Asimismo, el desglose de cada fase debe ser hecho con mucho cuidado considerando:

- Los requerimientos de acceso a SPEI.
- El tipo de servicio que se pretende implementar gracias al acceso a SPEI.
- La inclusión o no de elementos relacionados con CoDi.
- Requerimientos aplicables a las Entidades en materia de Banca Electrónica, PLD/FT.
- El éxito de un proyecto se mide solamente si puede lograrse que:
- Cada fase se ejecuta en tiempo.
- Se desarrolla dentro de un presupuesto definido.
- Se alcanzan los objetivos iniciales.
- Existe aceptación y utilización efectiva de los beneficiarios o usuarios del proyecto (es decir, existe satisfacción del cliente interno o externo).
- Para efecto de lograr lo anterior, es necesario que la Entidad comience planteándose lo siguiente:
- Analizar la necesidad de convertirse en participante del SPEI: para ello se necesita el apoyo de un experto legal y un experto de sistemas para efecto de recorrer cada uno de los requerimientos de la normatividad expedida por Banco de México[107] y asignar preliminarmente tiempos y costos a cada uno de dichos requisitos. Las metas de negocios y las eficiencias que se quieran alcanzar con SPEI son un factor determinante para el éxito del Proyecto.
- Diagnosticar las actuales capacidades tecnológicas y financieras de la Entidad frente a los requerimientos de SPEI. Considerar no sólo los aspectos relacionados con la autorización para actuar como Participante de SPEI, sino las actividades que corresponde realizar en el día a día a la Entidad como tal.
- Involucrar al Consejo de Administración en la planeación y en el establecimiento de las metas, mediante la preparación de presentaciones con información de las ventajas, riesgos y presupuesto estimado del Proyecto.

[107] Circular 14/2017.

- Realizar una ruta crítica preliminar que permita a la Entidad comprender cuáles serían los pasos.
- En el caso de que existan dudas específicas, realizar un acercamiento preliminar con Banco de México para efecto de resolver dudas puntuales. Es decir, los Reguladores no fungen ni deben ser considerados como asesores de la Entidad. Las decisiones de negocios, técnicas y legales deben ser (y son) responsabilidad de las Entidades y sus asesores. Sin embargo, existen aspectos de implementación que ellos, en nuestra experiencia, están abiertos a responder a cuestiones que pueden surgir en la interpretación de su propia regulación.
- Realizar dos tipos de consultas: clientes externos y clientes internos. Es decir, en esta etapa es necesario dirigirse a los Socios o Clientes de la Entidad para entender la manera en que manejan las transferencias y manejo de fondos de manera cotidiana, así como recabar información sobre temas de inclusión financiera en el marco del SACP. Asimismo, las áreas legales, control interno, Auditoría Interna y sistemas deben ser consultados sobre los procesos que podrían afectarlos con vistas a una incorporación a SPEI.
- Planear las adaptaciones de personal que será necesario realizar para mantener un adecuado funcionamiento de la Entidad como Participante de SPEI.
- Mantener claridad sobre la necesidad de realizar adaptaciones en el camino: existirán temas que será necesario cambiar a medida que avanza el proyecto, por lo que ello deberá preverse también en la asignación presupuestal al Proyecto

19.5 Diagrama y Plan de Trabajo.

Una planeación a nivel regulación, debe considerar los siguientes aspectos a nivel legal. En cuanto a la metodología, sugerimos realizar una planeación con los niveles indicados en la Sección 2 para una proyección y diseño considerando los requisitos aplicables:

Gráfica 20. Plan de trabajo para la conexión al SPEI de las Entidades. Fuente: Vite Abogados

Es importante también tomar en cuenta que se puede requerir la participación de Proveedores Relevantes que presten sus capacidades tecnológicas para efecto de cumplir con los requerimientos normativos de acceso.

19.6 Temas prácticos y recomendaciones.

Es importante que en la planeación del nuevo producto o servicio que involucrará SPEI se consideren los siguientes riesgos para realizar la evaluación correspondiente:

- Riesgo de liquidez. Posibilidad de que un participante no liquide una obligación por su valor total en la fecha correspondiente. Este evento no implica que este participante sea insolvente, ya que puede liquidar su obligación en una fecha posterior.
- Riesgo de crédito. Posibilidad de que un participante no liquide una obligación por su valor total.
- Riesgo de principal. Posibilidad de que un participante que es contraparte en una transacción de valores o divisas cumpla con la parte a que está obligada y no reciba la contraprestación. En un evento así, el participante puede perder el valor total de una operación.

- Riesgo legal. Posibilidad de pérdida debido a la aplicación inesperada de una ley o regulación, o por causa de un contrato cuyo cumplimiento no se puede exigir legalmente.
- Riesgo operativo. Posibilidad de que deficiencias en los sistemas de información o en los controles internos resulten en pérdidas inesperadas.
- Riesgo sistémico. Posibilidad de que el incumplimiento de las obligaciones por parte de un participante en un sistema de transferencia (o en general en los mercados financieros) sean causa de que otros participantes o instituciones financieras no sean capaces a su vez de cumplir con sus obligaciones. Tal incumplimiento puede causar problemas graves de liquidez o de crédito, lo que podría amenazar la estabilidad de los mercados financieros.

19.7 Modelo novedoso y Acceso a SPEI

El acceso a SPEI (y a su extensión o modalidad CoDi) requiere un esfuerzo considerable. A reserva de que cada Entidad estudie esta posibilidad a detalle en conjunto con sus reguladores, pensamos que es posible abordarse mediante la figura del "Modelo Novedoso" previsto de la Ley Fintech. Para esto es necesario recordar que las Entidades están autorizadas para realizar inversiones permanentes en otras sociedades, siempre y cuando les presten servicios auxiliares o complementarios.

Una idea podría ser la constitución de un vehículo especial (una sociedad mercantil) controlado por un conjunto de Entidades con el objeto de adoptar un Modelo Novedoso con acceso a SPEI para prestar servicios a los accionistas de dicho vehículo. Este tipo de planteamiento (colectivizar un servicio) para prestar un servicio a varias entidades financieras no es nuevo: ahí está el ejemplo de las Sociedades de Información Crediticia, en las cuales existe inversión por parte de varias entidades financieras con el objeto de contar con un servicio colectivo.

Desde luego, esto tiene varios retos en distintos niveles legales:

- Consultas con los Reguladores para efecto de verificar que (i) en opinión de Banco de México un Modelo Novedoso tiene la posibilidad de actuar como un Participante

de SPEI, (ii) el punto de vista de CNBV y de SHCP sobre si la sociedad (bajo un esquema de coinversión) efectivamente configura un supuesto de servicio auxiliar o complementario (es decir si las Entidades tienen capacidad para invertir en esta sociedad) y (iii) acreditar la existencia de elementos novedosos o innovadores que ameriten otorgar este tipo de autorizaciones.

- Crear esquemas y arreglos corporativos que garanticen un equilibrio entre los potenciales socios o accionistas para evitar futuros conflictos (preparación de estatutos sociales y convenios entre accionistas) así como, en su caso, valuar posibles aportaciones en especie (por ejemplo, Entidades que decidieran aportar conocimientos técnicos o personal en lugar de aportaciones en efectivo).
- Establecer un modelo de negocio viable que permita que eventualmente, el Modelo Novedoso, adopte su forma definitiva (como se explica más adelante) y realizar una planeación adecuada para obtener la autorización correspondiente.

Los Modelos Novedosos (también conocidos como *Sandboxes* a nivel internacional) son un espacio de experimentación, que permite a empresas ofrecer servicios financieros a un número acotado de clientes, usando herramientas o medios tecnológicos innovadores, con el fin de probarlos antes de ofrecerlos al público en general de forma masiva. La Ley Fintech los define como aquellas sociedades que para la prestación de servicios financieros utilicen herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento del otorgamiento de una autorización para operar como tal por parte de las comisiones reguladoras.

Los elementos principales de los Modelos Novedosos son los siguientes:[108]

- Experimentación, funcionan como un entorno de prueba.
- Duración limitada, en ningún caso pueden utilizarse para mantener a las empresas indefinidamente en el Sandbox. Se trata de “experimentos” temporales.

[108] Banco Interamericano de Desarrollo. Sandbox Regulatorio en América Latina y el Caribe para el ecosistema FinTech y el sistema financiero.

- Ofrecen soluciones casuísticas, se estructuran en torno a principios básicos que se adaptan a muy diversos modelos de negocio y permiten un enfoque individualizado, basado en los riesgos de cada propuesta.
- Excepcionales, dado que operan en un entorno experimental sujeto a riesgo, en la práctica se aplican de forma limitada.

Tratándose de entidades financieras (como sería el caso de los participantes del SACP), solo es posible adoptar este esquema a través modelos que requieran excepciones a la regulación secundaria a la que están sujetas para poder probar el modelo. No obstante, en este caso planteado, no sería propiamente la Entidad la que estaría sujeta a las reglas de Modelo Novedoso sino el vehículo controlado por varias entidades, por lo que consideramos que le serían aplicables los requerimientos para Modelos Novedosos para entidades no reguladas (excluyendo para estos efectos la normativa del capítulo "De los Modelos Novedosos en Entidades Reguladas" de la Ley Fintech). En todo caso esto podría ser un área gris que valdría la pena explorar con los Reguladores.

En este supuesto y asumiendo que en análisis anterior sea correcto a juicio de los Reguladores y que la regulación aplicable sea el del capítulo "De la Autorización de Modelos Novedosos", hay que tomar en cuenta lo siguiente:

- Aspectos a Evaluarse. Para el otorgamiento de la autorización temporal, el Banco de México deberá revisar, entre otros aspectos, el cumplimiento de los criterios y condiciones siguientes:

  (i) Que la propuesta sea conceptualmente novedosa;

  (ii) El producto para ofrecerse o el servicio a prestarse al público debe probarse en un medio controlado (limitado y con restricciones);

  (iii) La forma en que se pretenda desarrollar la actividad reservada debe representar un beneficio al cliente del producto o servicio de que se trate con respecto a lo existente en el mercado;

(iv) El proyecto se debe encontrar en una etapa en la que el inicio de operaciones pueda ser inmediato (lo cual implica que el periodo de planeación y la inversión iniciales deben realizarse de manera previa);

(v) El proyecto debe poder ser probado con un número limitado de clientes, y

(vi) Los demás que, en su caso, determinen las Autoridades Financieras competentes mediante disposiciones de carácter general.

- Duración de la Autorización. La autorización deberá tener una duración acorde a los servicios que se pretenden prestar y no podrá ser mayor a dos años, prorrogable por un año siempre que la sociedad autorizada para operar el Modelo Novedoso se encuentre en trámites para alcanzar "su forma final" como se menciona a continuación.
- Salida. La sociedad que se autorice como Modelo Novedoso debe llevar a cabo las acciones necesarias para obtener la autorización, registro o concesión definitivos durante el plazo de la autorización temporal, conforme a las leyes financieras que regulen dichos actos. Es decir, el Modelo Novedoso debe tender a realizar actividades como una entidad regulada al final de la vigencia de la autorización. Cuando no realice dichas acciones, deberá llevar a cabo el procedimiento de salida, es decir, terminar con las operaciones que se encontraba realizando. En el caso propuesto sería necesario analizar la forma final adecuada para este tipo de Modelo Novedoso.
- Requisitos Genéricos. En la solicitud de autorización temporal del Modelo Novedoso, las sociedades deberán incluir lo siguiente:

(i) El proyecto de estatutos sociales con domicilio en México y estableciendo las actividades que se pretenden llevar a cabo;

(ii) La descripción del Modelo Novedoso, la totalidad de las operaciones o actividades que pretenda realizar a través de este Modelo y el detalle de cada una de ellas, justificando la necesidad de operar con dicho Modelo Novedoso;

(iii) Las políticas de análisis de riesgo, incluyendo aquellas políticas a seguir en materia de seguridad en la Infraestructura Tecnológica y de seguridad de la información;

(iv) Las disposiciones jurídicas que regulan la actividad reservada que consideran que obstaculizan el desarrollo de los productos o servicios a través del Modelo Novedoso;

(v) Los beneficios potenciales para los Clientes del servicio o producto de que se trate con respecto a lo existente en el mercado;

(vi) El mercado objetivo o número máximo de Clientes a los que se les ofrecería el producto o servicio de que se trate, especificando en su caso, la ubicación geográfica respectiva y el monto máximo de recursos que podrán recibir de cada cliente, así como el monto máximo total que podrán recibir durante la vigencia de su autorización temporal;

(vii) La forma en que habrán de resarcir los daños y perjuicios que, en su caso, genere a sus clientes por la prestación de los servicios que otorgue durante el periodo en desarrollo, lo cual deberá pactarse en los contratos que para tal efecto celebren;

(viii) La forma en que pretende informar y recabar el consentimiento de sus clientes respecto a que celebrarán operaciones con sociedades autorizadas para operar con Modelos Novedosos, así como los riesgos a que se encuentran sujetos por ello;

(ix) La forma, método y plazos en que habrán de cumplir con los requisitos para obtener la autorización, registro o concesión definitivos conforme a las leyes financieras que regulan el servicio a prestar;

(x) El procedimiento de salida a llevar a cabo en caso de que las autoridades financieras no le otorguen la autorización, registro o concesión definitivos o concluya la vigencia de la autorización temporal o de su prórroga, según corresponda, y

(xi) La demás documentación e información que las autoridades financieras competentes requieran al efecto.

- Autorización Corporativa. La presentación de la solicitud de autorización debe ser aprobada por el órgano de administración de la sociedad que pretenda obtener la autorización.

En este caso la autoridad encargada de supervisar el Modelo Novedoso propuesto sería Banco de México, quien a través de la Circular 5/2019, menciona que "El Banco de México, considerando que tanto las instituciones de tecnología financiera, entidades financieras y sujetos supervisados por autoridades financieras como las empresas distintas a estas, podrían diseñar nuevos modelos de negocio y desarrollar implementaciones innovadoras que tengan el potencial de generar procesos más eficientes en los servicios de compensación, ruteo y liquidación, y que estos a su vez puedan representar menores costos para los usuarios finales, siempre y cuando cuenten con las medidas de control de riesgos adecuadas".

Estas actividades objeto del Modelo Novedoso en comento se definen de la siguiente manera:

- Ruteo: la transmisión de solicitudes de autorización de operación, autorizaciones de operación, rechazos de operación, devoluciones o ajustes de operaciones que realizan las Cámaras de Compensación de los participantes por la que se realiza el intercambio entre ellos.
- Compensación: proceso para determinar al cierre de un periodo establecido el saldo deudor o acreedor que corresponda a cada uno de los participantes de la Cámara de Compensación o a otras cámaras de compensación a las que transmita y de las que reciba autorizaciones de operaciones, devoluciones, ajustes y otras obligaciones financieras y que a su vez dichos saldos resulten del intercambio de obligaciones entre esos participantes y las cámaras de compensación y que tengan como efecto que estos asuman el carácter de acreedores y deudores recíprocos.
- Liquidación: al acto en virtud del cual los participantes dan por cumplida la obligación correspondiente que resulte de la compensación.

Los solicitantes que pretendan operar algún Modelo Novedoso relacionado con los servicios anteriores, deberán presentar su solicitud de autorización ante la Gerencia de Autorizaciones y Consultas de Banca Central del Banco de México, la cual tiene que ir acompañada, además de los requerimientos genéricos ya mencionados (además de otra documentación auxiliar), deberá describirse el Modelo Novedoso la cual deberá precisar, entre otros:

- Descripción detallada de los beneficios potenciales para los clientes.
- Periodo por el que se solicita la autorización (considerando los límites ya mencionados).
- Descripción detallada de los procesos del servicio.
- Obligaciones con los clientes.
- Límites con los que pretende operar.
- Características de la infraestructura tecnológica.
- Esquema de seguridad informática.

La sociedad una vez autorizada, deberá solicitar la inscripción el registro correspondiente y cumplir con los requisitos del mismo. Además, deberá presentar cada seis meses un reporte que contenga información relativa a las operaciones realizadas y a los clientes con los que cuenta, así como a las situaciones de riesgo que se hayan presentado. Lo anterior, se ve reflejado de manera resumida en el siguiente diagrama:

Solicitud de autorización para ser participante del SPEI

Gráfica 21. Solicitud de autorización para ser participante del SPEI. Fuente: Vite Abogados

SECCIÓN 20.- AUTOMATIZACIÓN DE PROCESOS.

Existen muchas tecnologías que pueden utilizarse para automatizar procesos. Para esta sección y dado que ya hemos hablado muy brevemente de la RPA (Automatización Robótica de Procesos o *Robotic Process Automation*) nuestro enfoque se centrará en ella, si bien la intención es que el siguiente panorama y recomendaciones sean aplicables a cualquier intento por automatizar un proceso dentro de una Entidad a través de un software. La automatización de un proceso es un paso adicional en los procesos de digitalización: una vez que se han establecido estrategias digitales en una Entidad, entonces el camino para automatizarlas es el más natural para eliminar las duplicidades de funciones, ahorrar tiempo al personal y dedicar recursos valiosos a otras tareas.

La automatización, en experiencia de algunas personas a las que el Asesor Legal ha apoyado en Proyectos similares, generalmente responde a las siguientes necesidades:

- Recortar costos operativos y de mantenimiento.
- Enfocar al personal de la Entidad en actividades de mayor complejidad y de mayor valor agregado.
- Retrasos continuos o perceptibles en el cumplimiento de obligaciones (regulatorias o contables).

Una vez detectada la necesidad de automatizar los procesos, es conveniente planear para la implementación de RPA o automatización. En el caso de Entidades con poca experiencia en dichos procesos se recomienda empezar por temas básicos y con implementaciones pausadas.

20.1 Selección de Procesos.

La selección de los procesos que pueden ser objetos de automatización son un tema que puede depender de diversos factores al interior de la Entidad, pero de manera general, existen características comunes en todas las empresas. Dichos procesos son:

- Repetitivos: los programas informáticos son mejores para replicar procesos repetitivos y con pocos cambios en su ejecución continuada. Por sí mismos, los programas de software no son muy buenos para ponderar opciones en entornos

desconocidos o que requieren experiencias de diverso tipo para efecto de llegar a una solución. Es decir, actividades de alta dirección, por ejemplo, no son buenos candidatos para la automatización.

- Basado en datos: se trata de procesos de que administran, generan y usan datos en formato electrónico y cuyo análisis de manera manual no es eficiente. Implica que son datos e información sujetos de información y manejo global y estadístico.
- Regulación formal: los procesos que se pueden describir mediante una serie de reglas o pasos predeterminados son más fáciles de traducir en un código, de tal manera que el programa que provea la automatización puede entender.
- Aspectos Regulatorios. Existe una gran cantidad de procesos relacionados con la recolección y uso de información para efecto de cumplir con la regulación aplicable a las Entidades. La automatización permite llevar un control más exacto del estado de cumplimiento regulatorio de la Entidad.
- Precisión. Existen tareas para las cuales los humanos no son muy buenos, especialmente aquellas que implican la realización de un número considerable de actividades repetitivas que implican variar datos conforme ciertos patrones. La cantidad de errores humanos en estos procesos puede reducirse gracias a la automatización.
- Continuidad. En algunos casos, debido a la obligación de conservar la continuidad del negocio, hay procesos que deben correr veinticuatro horas los siete días de la semana. El desgaste humano y cuestiones de índole laboral y de costos hacen que esto sea complicado de lograr. Las máquinas no tienen estas restricciones.

20.2 Identificación de Áreas Relevantes.

Las Partes Responsables más importantes para llevar a buen puerto un proyecto de automatización son las siguientes:

- Dirección General: será el responsable de obtener el apoyo del Consejo de Administración, así como organizar los esfuerzos para la implementación del Proyecto. La supervisión de su parte es esencial.

- Área de Sistemas: se trata del equipo más importante y quien deberá jugar un papel central en la selección del futuro proveedor. Debe hacer explícita su experiencia o inexperiencia en procesos de automatización ya existentes, así como advertir de los problemas que él prevé en la posible implementación. Su opinión sobre la disponibilidad de tecnologías maduras y accesibles es esencial. Asimismo, él podrá dar su opinión de los impactos que tendrá tanto la prueba de concepto como la implementación definitiva del Proyecto.
- Auditoría Interna: el cumplimiento de los objetivos de sistema de control interno debe cuidarse en todo momento. Si el nuevo proceso no es capaz de adoptar normas mínimas que aseguren el cumplimiento de las reglas de control interno, es poco probable que el Proyecto sea viable para la Entidad.
- Área Legal: esta área, ya sea interna o a través de un asesor externo, debe realizar actividades de (i) identificación de aspectos regulatorios en el proceso que se pretende automatizar (datos personales, PLD/FT y sistema de control interno, entre otros), así como la necesidad de realizar cambios a los Manuales de la Entidad, (ii) caracterización del futuro proveedor tecnológico como Proveedor Relevante o no con base en las tareas que va a realizar (por ejemplo, si es o no un Servicio Excluido), y (iii) la documentación legal que formalice la relación con el futuro proveedor, así como asegurarse de que existen aprobaciones corporativas (de ser el caso).
- Área de Administración de Riesgos: que evalúe si existe o cuáles son los riesgos que la automatización traerá a la Entidad y den su punto de vista en la evaluación del costo beneficio que tendrá el Proyecto.
- Áreas contables y de negocios: para efecto de valuar el costo beneficio del Proyecto y establecer el impacto que tendrá la automatización del proceso en el modelo de negocio de la Entidad.

Dependiendo del tipo de automatización será necesario involucrar a otras áreas, por ejemplo, al Oficial de Cumplimiento si se trata de procesos PLD/FT o áreas de cobranza si se trata de automatizar procesos de administración de cartera, entre otros ejemplos.

El enfoque del "Cliente Interno" o persona que sería usuaria o beneficiaria de los procesos de automatización es muy importante: entender la manera en que cambiará su proceso de

trabajo, la capacitación que se requerirá, así como el apoyo externo que requiere una implementación exitosa deben consensuarse con él.

20.3 Tipos de Proveedores.

No todos los proveedores involucrados en un proceso de automatización deben ser Proveedores Relevantes en el sentido en que los hemos definido en las Secciones 15 (Contratación de Proveedores y Comisionistas) y 16 (Prestadores de Servicios Operativos) de la presente Guía Legal. En este caso, el área legal o el asesor externo debe realizar una evaluación considerando:

- Si el proveedor tendrá acceso a información de Socios o Usuarios de las Entidades.
- La importancia del proceso para la administración y operación de la Entidad.
- La manera en que se llevará a cabo la administración de las bases de datos que, en su caso, se requerirá para manejar el proceso.
- La dependencia que generará el proceso para la Entidad y las consecuencias que tendría en la continuidad del negocio un incumplimiento del proveedor a los niveles de Servicio.

Incluso si el asesor determina que estamos en presencia de un Servicio Excluido, es decir uno que no requiere de la intervención de CNBV para su contratación, se recomienda siempre consultar a dicho Regulador para efecto de verificar dicha interpretación.

20.4 Acercamiento Inicial.

El acercamiento inicial, una vez que se hayan determinado los posibles procesos sujetos a posible automatización, debe pasar por las siguientes etapas:

- Investigación sobre las opciones de tecnología de automatización disponibles para ser implementadas en México, incluyendo RPA e IA. Entender si existen entidades financieras que hayan realizado implementaciones similares con éxito. Esto incluye la búsqueda y recolección de información de proveedores, herramientas tecnológicas y aspectos técnicos de una implementación.
- Realizar entrevistas con posibles proveedores de tecnología y, en lo posible, realizar pruebas piloto o de conceptos de una posible implementación. Documentar de manera adecuada las ventajas y desventajas de la tecnología propuesta y establecer parámetros presupuestarios de implementación. El criterio de selección de proveedores debe ser: costos bajos y posibilidad de realizar pruebas piloto dentro de la Entidad.
- Verificar con las Partes Responsables de la Entidad los aspectos necesarios para llevar a cabo la prueba piloto, incluyendo aspectos de ciberseguridad, garantías y mantenimiento del proveedor a la tecnología. La colaboración con el posible proveedor es esencial, pues de este modo se conoce su disponibilidad y capacidad para prestar el servicio.
- Una prueba piloto no quiere decir que ésta deba realizarse a la ligera: hay arreglos en materia legal que deben acordarse con el posible proveedor (convenios de confidencialidad, contratos de prestación de servicios), así como con las áreas internas (evaluación de la viabilidad legal y alcances de la prueba piloto, así como arreglos en materia de ciberseguridad al interior de la Entidad).
- Una vez seleccionado el o los proveedores se comienzan a negociar los términos y condiciones de la posible colaboración, así como la interacción con el equipo de la Entidad para establecer los siguientes pasos.
- Considerar que el equipo de la Entidad que manejará los nuevos procesos automatizados necesitará la debida capacitación y asistencia para efecto de implementar el Proyecto, por lo que incluso ello debe estar debidamente

documentado en el contrato que se celebra con los proveedores o en un documento similar.

- Compartir con la Dirección General y el Consejo de Administración las metas, objetivos y procesos relacionados con los procesos automatizados. La claridad en la comunicación con la administración es necesario para asegurar su apoyo, tanto a nivel jerárquico y organizativo como presupuestal. Mostrar que las ventajas en el mediano y el largo plazo serán mayores que las desventajas y que el ahorro de dinero y recursos de la Entidad serán mayores que las desventajas
- La naturaleza de un programa piloto es precisamente la de una prueba. La Entidad debe considerar como una posibilidad real (y en muchos casos necesaria) el abandonar el Proyecto o el proveedor preseleccionados, así como replantear las necesidades propias. Lo importante es que la Entidad se sienta suficientemente informada sobre la decisión que va a tomar. En ocasiones, el incentivo del proveedor es tratar de implementar u ofrecer procesos que no necesariamente se alineen con los objetivos de la Entidad.

20.5 Diagrama y Plan de Trabajo.

Desde nuestro punto de vista, el plan de trabajo y los pasos necesarios para efecto de poder implementar una tecnología que automatice algunos procesos de la Entidad debe considerar:

- Los aspectos mencionados en la sección anterior para efecto de realizar una aproximación inicial exitosa, estimando:

  (i) Una selección de procesos automatizables con base en uno o más de los criterios propuestos en las secciones anteriores, involucrando tanto a los propietarios de los procesos como a las futuras Partes Responsables de implementar el Proyecto.

  (ii) La recolección de suficiente información sobre tecnologías disponibles (incluyendo RPA e IA).

(iii) Involucramiento de la Dirección General y el Consejo de Administración en la evaluación preliminar del Proyecto.

(iv) Preselección rigurosa de los futuros proveedores y establecimiento de las bases de pruebas piloto.

(v) Preparación de documentación legal para la prueba piloto, visto bueno de las Partes Responsables y verificación de aspectos regulatorios y de ciberseguridad para realizar dicha prueba.

- En paralelo a lo anterior, debe realizarse una evaluación financiera o de costo beneficio de la posible automatización:

(i) Identificar si es un proceso normal y común en las empresas o si se trata de un proceso propio de la Entidad como entidad financiera o debido a su modelo de negocio.

(ii) Establecer si el proceso requiere un número constante de reglas y pasos para ejecutarse, en específico, si no requiere de constante supervisión o creatividad para su finalización.

(iii) Indicar si el proceso varía muy poco en su ejecución a lo largo del tiempo.

(iv) Establecer el tiempo que lleva realizar el proceso y quiénes son los encargados de realizarlo, así como el número de empleados involucrados.

(v) De manera anualizada indicar las horas que lleva realizar el proceso.

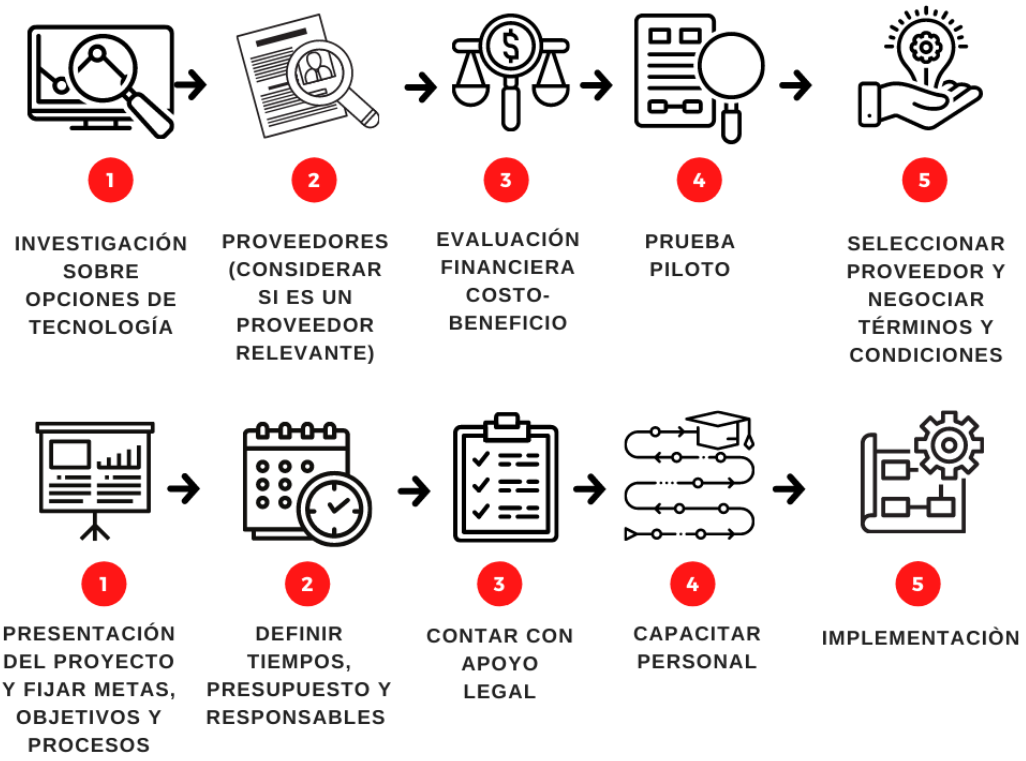
(vi) Entrevistar a los ejecutores del proceso e indagar si consideran el proceso repetitivo o aburrido.

(vii) Revisar si la realización continua del proceso puede conllevar a errores humanos.

- Preparar una presentación sobre el futuro Proyecto indicando los aspectos mencionados anteriormente para su aprobación por parte del Consejo de Administración. Ellos son los que también, en su caso, pueden autorizar el posible presupuesto y garantiza que habrá el apoyo suficiente para completarlo.
- Realizar una planeación del Proyecto conforme a lo descrito en la Sección 2 (Aspectos Generales de la Administración de Aspectos Esenciales), identificado tiempos, presupuesto y responsabilidades de cada una de las áreas responsables. Un punto que debe contemplarse es la realización de la prueba piloto, la cual debe también administrase como un "mini Proyecto" por sí mismo. Esta fase de planeación debe considerar (i) el modelo o impacto de negocio para la automatización, así (ii) los recursos tecnológicos que será necesario contratar o comprar o preparar para efecto de comenzar con la prueba piloto y la implementación final.
- Determinar, con apoyo del asesor legal interno o externo, el impacto que tendrá la automatización en el Sistema de Control Interno y los Manuales de la Entidad, así como la necesidad, en su caso, de obtener autorizaciones corporativas o regulatorias (CNBV) para efecto de implementar y finalizar el Proyecto.
- En el caso de que se determine que el proveedor será un Proveedor Relevante, la planeación deberá incluir los pasos necesarios para solventar el proceso ante CNBV conforme a las Secciones 14 (Almacenamiento en la Nube) y 15 (Contratación de Proveedores y Comisionistas) . Esto también deberá considerar los aspectos relacionados con la negociación y clausulado mínimo que debe tener el contrato, así como la entrega de información del Proveedor Relevante.

Es preciso hacer notar que no existe un modelo estándar de planeación para implementar el RPA o automatización. Es necesario tomar en cuenta que dentro de esta categoría estamos englobando varios tipos de situaciones, consideramos prudente que se tome mucho tiempo en los temas mencionados en el "Acercamiento Inicial".

Plan de trabajo para la automatización de procesos



Gráfica 22. Plan de trabajo para la automatización de procesos. Fuente: Vite Abogados

20.6 Temas prácticos y recomendaciones.

A riesgo de parecer redundantes, a continuación, presentamos algunas recomendaciones relacionadas con la implementación de Proyectos como los tratados en esta sección:

- Una aproximación cuidadosa empieza por pasos pequeños: la información sobre tecnologías disponibles y la realización de pruebas piloto son muy importantes, si bien éstas deben hacerse en entornos muy controlados para evitar incumplimientos a la regulación o exponer la Entidad a riesgos cibernéticos.
- Buscar opciones varias de proveedores de sistemas automatizados: la búsqueda intensiva debe ser hecha con criterios de eficiencia y no necesariamente con el objeto de buscar el proveedor menos costoso.

- Los cambios en la Infraestructura Tecnológica no se limitan necesariamente a los servicios del Proveedor Relevante, sino que puede implicar gastos adicionales, contrataciones de nuevo personal y capacitación permanente.
- El liderazgo de proyectos de automatización no debe recaer necesariamente en el área legal: el gran componente tecnológico y de negocios que tiene puede requerir que sea otra Parte Responsable la que dirija los esfuerzos. Esto debe evaluarse para asegurar que quien esté al mando del Proyecto comprenda todos los aspectos relacionados con el mismo.
- Los aspectos que deben clarificarse con el proveedor de servicios, previo a cerrar y firmar los contratos respectivos son los siguientes:

(i) Experiencia previa en la implementación de proyectos de automatización y ejemplos concretos del tipo de proyecto y compartir los criterios que se usaron para ello.

(ii) Entender el modelo de soporte que será prestado.

(iii) Modelo de honorarios y costos (por ejemplo, por hora, por volumen, etc.).

(iv) Entender cuáles serían los hitos y entregables del proveedor en favor de la Entidad.

(v) Los supuestos y consecuencias de realizar cambios a la implementación, su modelo de costos en este supuesto, así como su experiencia en estos casos.

(vi) Las necesidades de adaptación de la Entidad para efecto de poder utilizar el servicio (es decir, si se requiere personal que sepa programar o llevar a cabo una tarea específica).

(vii) Entender cuál será el apoyo del proveedor para realizar las pruebas, desarrollo y producción de las aplicaciones o ambientes de los programas.

(viii) Verificar si habrá capacitación suficiente para la Entidad para efecto de poder operar el modelo de manera continua.

(ix) Identificar los estándares de ciberseguridad que subyacen a las aplicaciones y demás infraestructura que será prestada por el proveedor.

(x) Entender los accesos a la información y a los procesos operativos de la Entidad.

- Documentar los procesos a automatizarse, las expectativas y metas de Proyecto es importante para que exista un repositorio común donde las Partes Responsables puedan verificar avances, resolver dudas y entender si se están cumpliendo las expectativas originales.

SECCIÓN 21.- USO DE DATOS (BIG DATA).

El término "Big Data" hace referencia a la capacidad de procesamiento de una cantidad alta de datos masivos, los cuales, en principio, no pueden ser procesados ni analizados por la tecnología convencional o metodologías simples. La obtención de información relevante requiere de nuevas herramientas. Mediante el Big Data es posible analizar tendencias, predecir comportamientos e incluso sacar conclusiones de temas concretos que de otra manera quedarían ocultos.

En las últimas décadas, la capacidad de generar y almacenar datos se ha incrementado de manera exponencial. Simultáneamente, la capacidad de procesamiento a gran escala también ha aumentado. Las Entidades, como instituciones financieras, manejan también una cantidad importante de datos: las actividades que realizan sus Clientes o Socios a través de cada transacción es una huella que puede ser objeto de análisis. Para entender el comportamiento de sus Socios o clientes, es recomendable que las Entidades puedan acceder a sus propios datos y analizarlos, de modo que puedan hacer frente a las demandas del mercado[109] [110].

El acceso al Big Data se ha vuelto un proceso más sencillo y por lo tanto más popular, que no en todos los casos requiere de inversiones considerables o de la realización de procesos excesivamente complicados. Lo anterior es debido a que los costos para almacenar información son cada vez más baratos, lo que permite almacenar y gestionar mayores volúmenes de información y a que las técnicas y programas para realizar "minería" de esos datos son ya herramienta de acceso común. Tal como lo hemos explicado en secciones anteriores, existen grados de implementación de cada Proyecto según las necesidades de cada Entidad. Los datos pueden clasificarse en:

[109] The Data Deluge. The Economist [Internet]. 25 de febrero del 2010 [consultado el 1 de agosto del 2018]. Recuperado de: https://www.economist.com/leaders/2010/02/25/the-data-deluge.

[110] D.A. Reed, J. (2015) Dongarra Exascale Computing and Big Data. Communications of the ACM New York, NY, USA: ACM, 58 (7), pp. 56-68

- Estructurados. Se trata de datos ordenados u organizados en formatos predeterminados. Por ejemplo, datos que se encuentren almacenados en un blockchain o en un sistema de enterprise resource planning (ERP).
- No Estructurados. Se trata de datos que no cuentan con formato específico. Por ejemplo, mensajes de textos. Este tipo de información representa un reto importante para su procesamiento. Por ejemplo, documentos de oficina en archivos de texto, archivos PDF o datos de ubicaciones y mensajería.
- Semiestructurados. Se trata de datos que a pesar de aparecer como no estructurados, contienen elementos que pueden ser utilizados para su estructuración. Por ejemplo, archivos comprimidos o XML.

En principio, el uso de Big Data en el sector financiero está centrado en información y datos obtenidos de los clientes. Su uso puede ayudar a obtener información valiosa relativa a:

- Patrones de consumo (o gasto).
- Segmentar y mantener almacenados perfiles.
- Realizar procesos de administración de riesgos y PLD/FT de manera más efectiva.
- Personalizar las ofertas de servicios y la experiencia de los Usuarios.
- Crear estrategias para generar lealtad a largo plazo.
- Apoyar los esfuerzos para prevenir fraudes.

El Big Data también sirve para analizar factores macroeconómicos y su impacto directo en la Entidad: en la medida en que la Entidad logre vincular los factores “ambientales” de la economía (nacional y mundial) con sus propios datos, podrá estar en posición de diseñar estrategias más exitosas para prevenir riesgos y adaptarse mejor a ese entorno.

21.1 Datos.

Definir Big Data exclusivamente en términos del volumen de los datos ofrece una visión parcial y limitada. Tampoco es útil sólo hacer referencia a las ventajas potenciales. Es necesario definirlos en términos de lo que implica su manipulación. Existen tres parámetros que nos ayudan a entender el proceso de uso de los datos:

- Velocidad: se refiere al ritmo en que se genera cierto volumen de datos en un periodo de tiempo determinado.
- Variedad: el tipo de datos que se espera obtener en una empresa o de ciertos procesos.
- Veracidad: significa la exactitud de los datos y su correspondencia con fenómenos reales.

Con base en dichos parámetros es posible realizar una planeación adecuada para utilizar los datos que se generan en una organización o, en su caso, entender qué tipo de datos se desea obtener, crear y, por lo tanto, interpretar. Esto influirá en el tipo de Infraestructura Tecnológica que la Entidad debe adquirir o contratar para efecto de llevar un registro digital, garantizar el rápido acceso y procesamiento de los datos y realizar el análisis requerido[111].

Así pues, los procesos relacionados con el Big Data permiten identificar patrones y tendencias, y ofrece al sector financiero la posibilidad de localizar nuevas oportunidades de negocio. También el análisis y el desarrollo de métodos predictivos pueden proporcionar pautas para automatizar procesos y simplificar procedimientos. De este modo, las Entidades pueden optimizar recursos y encontrar nuevas oportunidades de desarrollo.

De cara a la relación con los clientes, el Big Data permite realizar una segmentación más precisa y completa. Esto es, tanto con los datos internos de la empresa como aquellos que se generan de forma externa (web, redes sociales, etc.) se pueden obtener clasificaciones y detalles de las clientes mucho más completas que con los métodos de análisis de

[111] BIS. The supertech generations. (Internet) Consultado en: https://www.bis.org/fsi/publ/insights19.htm

mercado tradicionales. Con la información recogida, las empresas pueden mejorar la fidelización de sus clientes. Al mismo tiempo, tener una información más pormenorizada permite a las empresas llevar adelante una estrategia de marketing personalizado, de acuerdo con las características de cada cliente.

Otra de las ventajas que ofrece el Big Data para el sector financiero es una mejor y más precisa evaluación de riesgos. Son muchos y distintos los riesgos que se dan en las finanzas, y el Big Data puede ayudar a evaluarlos, gestionarlos y mitigarlos.

21.2 Coordinación y Acercamiento Inicial

Para comenzar un Proyecto relacionado con el uso de Big Data para una entidad, consideramos tomar en cuenta los siguientes aspectos:

- Identificar las fuentes (actuales o potenciales) de los datos que se estarán creando, almacenando y utilizando. Sobre todo, establecer, con el apoyo del área de sistemas, cuáles serán los formatos de los mismos y la manera en que potencialmente podrían ser visualizados.
- Diagnosticar la Infraestructura Tecnológica actual para poder soportar los datos con base en parámetros de velocidad, variedad y veracidad.
- Considerar opciones de implementación por parte de proveedores externos. En algunos casos existen soluciones completas para todos los aspectos relacionados con el ciclo de uso de los datos.
- Entender la manera en que los datos se podrán transformar en beneficios tangibles para la Entidad. Se trata de entender las maneras en que generar esta información podrá traducirse en reducciones de costos o ganancias concretas. Esto implica contextualizar los datos dentro del modelo de negocios.
- Se debe buscar asesoría de un profesional en ciencias de datos que cuente con experiencia considerable en Proyectos similares.
- Para aproximarse al programa del Big Data en el contexto de una Entidad, recomendamos comenzar analizando los siguientes aspectos
- Identificar el tipo de datos que está produciendo la Entidad hasta este punto. La manera en que los sistemas actuales de la Entidad son capaces de generar

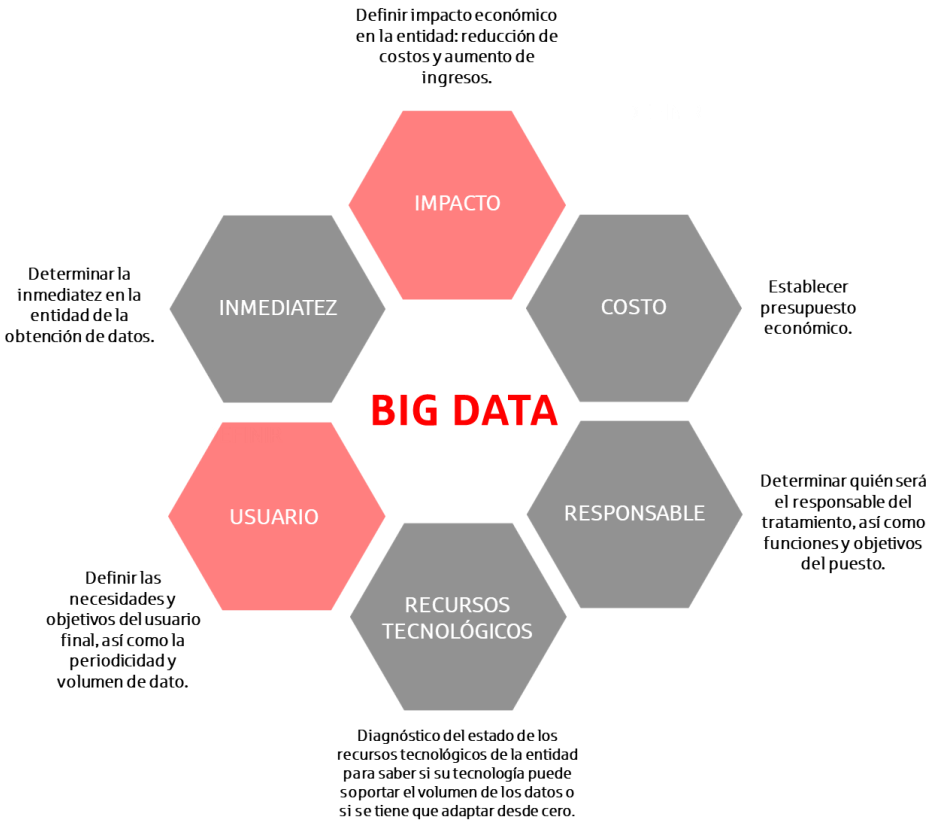
- Es necesario analizar el tipo de datos que se están generando y la manera en que se encuentran estructurados.
- Este primer análisis, de preferencia de la mano de un asesor externo, deberá dar a la Entidad un panorama de la calidad y cantidad de datos que pueden ser utilizados.
- Asimismo, es posible que debido a la manera en que la Entidad esté generando y procesando los datos, estos sean poco útiles o irrelevantes. En este caso será necesario determinar si con ayuda de nuevas herramientas informáticas es posible obtener más y mejores datos que sean relevantes para la Entidad.
- Considerar que un proyecto que implique realizar una recolección intensiva de datos va a requerir capacidades de almacenamiento. El primer reto es entender si es posible realizar este almacenamiento de manera interno o si será necesario contratar a un Proveedor Relevante (con las consecuencias que analizamos en las Secciones 15 y 16) y revisar si desde el punto de vista del Aviso de Privacidad puesto a disposición de los Socios o Clientes sea suficiente para dichos efectos.
- Establecer las necesidades de infraestructura tecnológica en materia de canales de recolección de dicha información. Esto está relacionado con la velocidad a través de la cual se generan los datos y las capacidades de red de la Entidad o de sus Proveedores Relevantes.
- Identificar los sistemas de acceso y análisis de los datos. No basta con recolectarlos por canales adecuados y almacenarlos de manera segura, sino que los mismos deben desplegarse de la manera más estructurada posible. Asimismo, dicho despliegue debe permitir un análisis útil. Esto tiene que ver con tecnologías de sistemas de bases de datos.

21.3 Diagrama y Plan de Trabajo.

En algunos casos la implementación de un plan de trabajo de un Proyecto relacionado con el Big Data comparte aspectos relacionados con cómputo en la nube y Proveedores Relevantes. (Ver Sección 14 Almacenamiento en la Nube y Sección 15 Contratación de Proveedores y Comisionistas).

En ese sentido recomendamos que una ruta crítica se establezca con base en los siguientes pasos:

Plan de trabajo para utilizar *Big Data* en las Entidades



Gráfica 23. Plan de trabajo para utilizar Big Data en las Entidades. Fuente: Vite Abogados

21.4 Evaluación de Prestadores de Servicios.

Las soluciones para uso de Big Data son similares a las que hemos realizado para cómputo en la nube (ver Sección 14) y automatización de procesos (ver Sección 20).

21.5 Perspectiva Regulatoria.

La emisión de regulación sobre Big Data como tal no existe en nuestro país. Preguntas como a quién atribuir la titularidad de la información pueden ser materia de mucho

debate[112] debido a que en ocasiones los datos de los Socios o Clientes pueden estar disociados, es decir, pueden analizarse (de manera estadística) sin necesidad de saber quién es el titular (lo cual también puede tener consecuencias importantes para determinar si el procesamiento hecho por un tercero tiene repercusiones en materia regulatoria). Una legislación adecuada debe ser integral y abarcar todos los pasos, desde la recopilación hasta el análisis de datos. Por ejemplo, un procedimiento que sólo recolecte código postal, fecha de nacimiento y género podría aparentar proteger bien la privacidad de los involucrados, pero un estudio en los EUA demostró que esta información bastó para identificar correctamente a 87% de la población.[113]

21.6 Temas prácticos y recomendaciones.

Los beneficios del Big Data en el SACP son varios entre los que se encuentran[114]:

1) Procesamiento de la información para realizar ofertas inteligentes e individualizadas de servicios. Se trata de mejoras en la gestión de datos, de análisis de patrones de uso de aplicaciones y herramientas, y de la implementación de cambios con base en toda esta información procesada. Dependiendo del perfil de cada persona se le ofrecerá una serie de servicios enfocados a sus intereses y necesidades. Asimismo, la detección de patrones en el comportamiento de un usuario puede permitir a la empresa anticiparse a una posible cancelación de los servicios. Entre otras opciones, el análisis les aporta información para buscar las opciones que le permitan fidelizar al usuario, y con ello anticiparse a ese abandono.
2) Evaluación de riesgos y prevención del fraude, la evaluación de riesgo y prevención del fraude es de gran importancia por el valor que puede aportar. Esto permite obtener las posibilidades de incumplimiento y tomar decisiones con esa información. También permite establecer patrones para identificar el riesgo de pérdida de clientes, o patrones de evolución de los tipos de interés. Otra aplicación, de cara al servicio a los clientes, es cómo la evaluación de riesgos da ventaja a las Entidades a la hora de

[112] Rodríguez P, Palomino N, Mondaca J. (2017) El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el Caribe.

[113] Sweeney L. Simple Demographics Often Identify People Uniquely (Internet). Consultado en: https://dataprivacylab.org/projects/identifiability/paper1.pdf

[114] ¿De qué hablamos cuando hablamos de Big Data en el sector financiero? (Internet) 19 de febrero de 2020 Consultado en: https://www.empresaactual.com/big-data-sector-financiero/

analizar los mercados, con datos complejos y en tiempo real, para gestionar sus carteras de inversión.

SECCIÓN 22.- OPEN BANKING.

La directiva de sistemas de pago (PSD2) que se implementó en la Unión Europea a partir de 2018, así como la regulación de la banca abierta en el Reino Unido han dado mucho impulso a la creación de un entorno de lo que se conoce como "Banca Abierta" (*open banking*). La Banca Abierta es una nueva manera de utilizar datos generados y administrados por entidades financieras mediante la introducción de interfaces de programación de aplicaciones informáticas estandarizadas (API, por sus siglas en inglés).

La Banca Abierta implica el cambio desde un modelo cerrado de datos financieros a uno en donde éstos se comparten entre diferentes miembros del ecosistema financiero, en algunos casos y dependiendo del tipo de datos, con autorización del cliente. Es un sistema que utiliza la disponibilidad de los datos públicos, agregados y transaccionales de los participantes del sistema financiero con el fin de promover mayor competencia entre los intermediarios, y ofrecer productos y servicios a la medida de los usuarios. Es decir, en el caso de los datos transaccionales, los usuarios autorizan compartir su información (por única ocasión, por tiempo determinado o de manera indefinida) y así concentrar en un solo sistema, información relacionada con varios servicios administrados por distintas entidades financieras en donde dicha persona sea cliente[115].La información se comparte a través de API**,** que es el mecanismo técnico abierto de comunicación e intercambio seguro de información entre dos entidades distintas, la entidad proveedora y la solicitante, según se describen más adelante, de forma estandarizada. Los datos que se intercambian a través de la API, en principio, solamente se intercambian entre la entidad proveedora y la solicitante.

22.1 Banca Abierta: Regulación Abierta.

22.1.1 Regulación internacional

[115] Gawer, A. (2009) Platforms, Markets and Innovation. Edward Elgar.

A nivel global, existen tres modelos de implementación: adopción obligatoria, adopción voluntaria y el descentralizado o definido por las propias entidades financieras:

a) Adopción obligatoria, que se caracteriza por contar con estándares muy detallados, emitidos por la autoridad u órganos competentes para efecto de llevar a cabo la aplicación del esquema (por ejemplo: Reino Unido, Australia y México).

b) Adopción voluntaria, que consiste en el establecimiento de lineamientos generales, que dan cierta libertad para el desarrollo de las API. Este modelo funciona mediante recomendaciones o estándares para su desarrollo (por ejemplo: Hong-Kong y Singapur).

c) Modelo descentralizado, en el que los propios integrantes de dicho sector se han organizado para crear su propia manera de proceder en materia de banca abierta (por ejemplo: Estados Unidos).

En 2009 fue creada la primera Directiva de Servicios de pago (PSD, por sus siglas en inglés), con el objetivo de contribuir al mercado único de pagos en la Unión Europea y fomentar la innovación, competencia y eficacia en el territorio europeo. En 2013, la Comisión Europea propuso una revisión de la primera directiva buscando mejorar la protección del consumidor y reforzar la seguridad en el mercado de pagos.

La segunda Directiva de servicios de pago (PSD2, por sus siglas en inglés), la cual hemos referido anteriormente, es un marco normativo para los servicios de pago que entró en vigor en enero de 2016 y, de alguna manera, es una continuación de su antecesora. Los objetivos clave de PSD2 son integrar aún más y apoyar un mercado de pagos de la Unión Europea más eficiente, así como promover la competencia en un entorno donde están surgiendo nuevos actores, como son las instituciones de tecnología financiera (Fintech) y una nueva generación de productos y servicios de pago.

El marco regulatorio PSD2 describe las funciones y responsabilidades de los proveedores de servicios de información de cuentas y los proveedores de servicios de pago. Este servicio puede ser proporcionado por bancos, instituciones de tecnología financiera y otras empresas de servicios financieros no tradicionales, así como minoristas y empresas de redes sociales y telecomunicaciones.

Paralelamente a la reforma regulatoria de la Unión Europea, en agosto de 2015 el gobierno del Reino Unido estableció un "Grupo de Trabajo de Banca Abierta" (OBWG, por sus siglas en inglés) con el fin de crear un marco para el diseño de un estándar API abierto en la banca. El año siguiente, la "Autoridad de Competencia y Mercados" (CMA, por sus siglas en inglés) de ese mismo país, publicó varias recomendaciones provisionales y, posteriormente, ordenó a nueve grandes bancos que formaran una entidad de implementación para establecer los estándares técnicos comunes que sustentan la banca abierta en el Reino Unido.

22.1.2 Regulación nacional

México cuenta con un modelo de adopción obligatoria de banca abierta en el que las autoridades regulatorias son las encargadas de emitir las normas aplicables. La Ley Fintech, así como la normatividad secundaria emitida (y aún pendiente de emitirse) por CNBV conforman la base jurídica para su aplicación en México.

La Ley Fintech, en sus artículos tercero, quinto y sexto transitorios prevé que las autoridades regulatorias cuentan con 24 meses a partir de la entrada en vigor de esta ley para emitir la normatividad secundaria que regule este modelo de adopción obligatoria de Banca Abierta.

El 4 de junio de 2020 se publicaron en el Diario Oficial de la Federación las "Disposiciones de carácter general relativas a las interfaces de programación de aplicaciones informáticas estandarizadas" ("Disposiciones de Banca Abierta"), en las que se regula el intercambio de datos abiertos a través del uso de interfaces de programación de aplicaciones estandarizadas. Sin embargo, como se explica en el numeral siguiente, la Ley Fintech contempla el intercambio de información de datos abiertos entre las entidades, así como el intercambio de datos agregados y datos transaccionales, por lo que se espera que en los próximos meses las autoridades regulatorias expidan la regulación aplicable a los otros datos.

22.2 Tipos de Datos.

La Ley Fintech establece cuáles son los datos e información que deberán compartirse mediante los procesos de banca abierta:

- Datos financieros abiertos: aquellos que no contienen información confidencial y, por lo tanto, pueden ser objeto de acceso por cualquier tercero. Dentro de estos, se encuentran: información de productos y servicios que las Entidades ofrecen al público general, ubicación de sus oficinas y sucursales, CAT, GAT, tasa de interés; comisiones, productos; entre otros.
- Datos agregados: relativos a la información estadística relacionada con operaciones sin contener un nivel de desagregación que pueda identificarse como personal o transaccional. Solamente podrán acceder a estos datos agregados las personas que cuenten con mecanismos de autenticación establecidas por las autoridades reguladoras. Dentro de estos datos se encuentran: número promedio de retiros de efectivo por mes en un área de código postal, solicitudes de préstamos exitosas de empresas dentro de un mismo giro o industria, productos contratados por rango de edades, entre otros.
- Datos transaccionales: los relacionados con el uso de un producto o servicio contratado a nombre del cliente o relacionada con las transacciones y estos datos solo puede compartirse con previa autorización expresa. Dentro de estos se encuentran: saldos; movimientos; depósitos; créditos; inversiones; compras; entre otros.

El intercambio de los datos e información de datos agregados y datos transaccionales estarán sujetos a las Disposiciones de Banca Abierta, así como a las disposiciones de carácter general que se expidan en los próximos meses.

22.3 Obligatoriedad de Implementación.

La Ley Fintech establece en su artículo 76 que las entidades financieras, incluyendo el sector de ahorro y crédito popular (dentro del cuales se contempla a las Cajas de Ahorro y a las SOFIPO), los transmisores de dinero, sociedades de información crediticia, las cámaras de compensación, las ITF y las sociedades autorizadas para operar con Modelos

Novedosos estarán obligadas a establecer interfaces de programación de aplicaciones informáticas estandarizadas que posibiliten la conectividad y acceso de otras interfaces desarrolladas o administradas por los mismos sujetos a que se refieren las disposiciones y terceros especializados en tecnologías de la información, con el fin de compartir los datos e información mencionados en el numeral anterior.

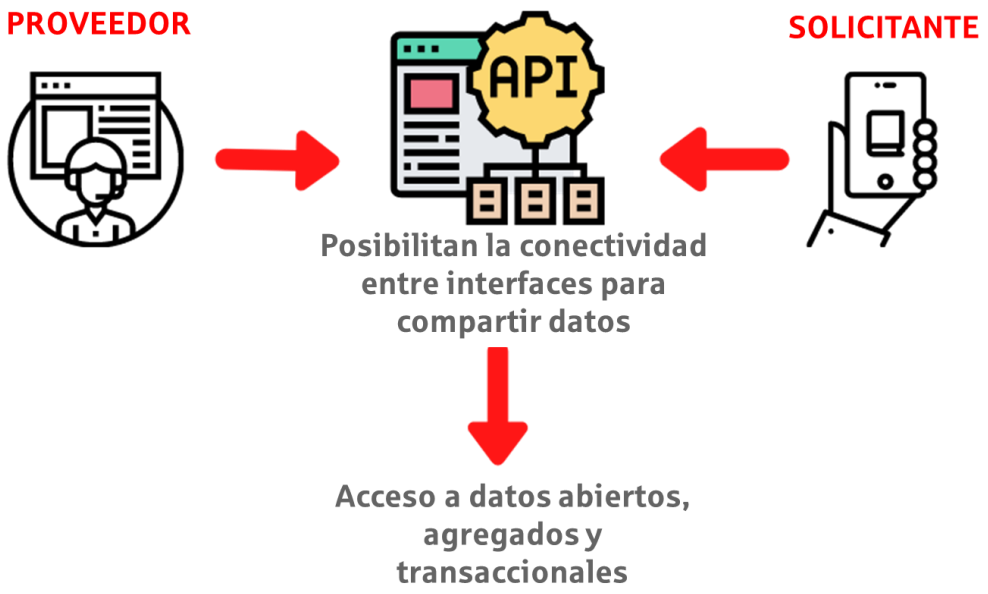
En las Disposiciones de Banca Abierta se regulan a dos tipos de participantes

- Proveedores de Datos, que son las entidades financieras, instituciones de tecnología financiera, transmisores de dinero, burós de crédito, cámaras de compensación deberán habilitar API para compartir datos financieros abiertos, agregados y transaccionales.

- Solicitantes de Datos, son todas las personas físicas o morales que cuenten con la tecnología suficiente para conectarse a las API y solicitar datos financieros abiertos, agregados o transaccionales.

Para acceder a los datos abiertos de los clientes, los Solicitantes de Datos deberán seguir el proceso señalado por los Proveedores de Datos y pagar a dichos Proveedores de Datos las contraprestaciones autorizadas.

Diagrama del funcionamiento de la Banca Abierta



Gráfica 24. Diagrama del funcionamiento de la Banca Abierta. Fuente: Vite Abogados

Por otra parte, aunque la información que se intercambia entre las entidades financieras y los terceros participantes puede ser diferente de los datos de los consumidores (datos abiertos y agregados), el enfoque mayor se encuentra en estos, ya que el fin de los receptores de la información es crear y distribuir soluciones personalizadas basadas en los comportamientos financieros de cada persona, pero para que esto ocurra es de suma relevancia que el intercambio de la información ocurra únicamente cuando el titular de la información (el consumidor) lo autorice de forma transparente y consciente, y pueda revocar dicha autorización de forma sencilla y en cualquier momento.[116]

Los términos y condiciones que establezcan los Proveedores de Datos con los Solicitantes de Datos para llevar a cabo el intercambio de los datos financieros abiertos, datos agregados y datos transaccionales a través de API, deberán establecer mecanismos y controles que aseguren la confidencialidad e integridad de los datos en su acceso, procesamiento y almacenamiento por parte de los Solicitantes de Datos.

[116] CECOBAN, Reporte Open Banking MX-2019.

Las disposiciones también establecen que los Proveedores de Datos deberán contar con una política de seguridad de la información que proteja en todo momento la infraestructura a la que tienen acceso los Solicitantes de Datos, así como la confidencialidad e integridad de los datos abiertos que, en su caso, compartan a través de APIs (ver Sección 9 Datos Personales y Secreto Financiero).

En el momento de escribir estas líneas la regulación sólo obliga a compartir "datos abiertos", por lo que las implicaciones y maneras de compartir legalmente los demás datos será materia de una regulación independiente que esperamos sea emitida en los próximos meses.

La política de seguridad deberá contener procedimientos continuos, mecanismos y controles mínimos, dentro de los cuales se encuentran:

- Configuración segura de los componentes tecnológicos de su Infraestructura;
- Mecanismos de identificación y autenticación del personal responsable del manejo de API bajo el principio de mínimo privilegio;
- Se entenderá como principio de mínimo privilegio a la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias del personal referido;
- Cifrado de la información almacenada y de los canales a través de los que se envíen los datos abiertos, así como mecanismos de identificación y autenticación
- Procesos de gestión para la atención de incidentes de seguridad de la información que se presenten en la operación de las API
- Programa de pruebas de escaneo de vulnerabilidades y amenazas, así como programa de pruebas de penetración;
- Mecanismos de respaldo.

Las Disposiciones de Banca Abierta también establecen que en los casos en que se presente un incidente de seguridad de la información, los Proveedores de Datos deberán

reportarlo a la CNBV, de manera inmediata, indicando fecha y hora de inicio, descripción de dicho incidente y evaluación de este.

Para que la Banca Abierta funcione de manera adecuada, es necesario que todas las partes que participan en este ecosistema, incluidos reguladores, terceros y bancos se unan para abordar los desafíos técnicos en las siguientes áreas principalmente:

- Desarrollo de mecanismos estandarizados, más allá de las disposiciones, mediante los cuales los bancos y terceros puedan interactuar.
- Establecimiento de soluciones apropiadas para maximizar la seguridad y minimizar la exposición de los participantes al fraude.
- Enseñar a los consumidores sobre los beneficios de la banca abierta.

Más allá del cumplimiento de las disposiciones, está el potencial que tienen los bancos para superar los niveles mínimos exigidos por la legislación.

22.4 Coordinación y Acercamiento Inicial.

Para que la Entidad pueda llevar a buen puerto el proyecto de Banca Abierta, sobre todo como un Proveedor de Datos, sugerimos que la coordinación y el acercamiento inicial al tema se realice de la siguiente manera.

1. Dirección General. Será el responsable de obtener el apoyo del Consejo de Administración, así como organizar los esfuerzos para la implementación del proyecto de Banca Abierta, además de establecer los objetivos y esbozar cuáles son los datos abiertos que la Entidad está en posibilidad de proveer al ecosistema.

2. Área de Sistemas. Se trata del equipo más importante y quien deberá jugar un papel central en la selección del futuro proveedor o bien en el desarrollo de la Infraestructura Tecnológica. En caso de que contraten a un proveedor de estos servicios, deberán verificar que éste conoce y pueda cumplir con los requisitos técnicos establecidos en las Disposiciones de Banca Abierta. Además, tendrá un papel central en apoyar en el desarrollo de la política de seguridad para todas las cuestiones técnicas solicitadas en las Disposiciones de Banca Abierta.

3. Área legal. Esta área, ya sea interna o a través de un asesor externo, debe realizar actividades de (i) verificar que los términos y condiciones del contrato que se llegue a celebrar con el proveedor que apoye en la implementación de la Banca Abierta cumpla con los requisitos establecidos en las Disposiciones de Banca Abierta; (ii) junto con el área tecnológica, verificar el cumplimiento de los requerimientos establecidos en la Ley Fintech, Disposiciones de Banca Abierta a lo largo del proceso; (iii) coordinar los aspectos legales de la implementación con el proveedor externo; (iv) realizar la inscripción de las comisiones que se van a cobrar; (v) apoyar en la redacción (junto con el Área de Sistemas) de la política de seguridad para verificar que se cumplan con los requisitos mínimos legales establecidos en las Disposiciones de Banca Abierta; (vi) vigilar el intercambio de datos abiertos a través del uso de interfaces de programación de aplicaciones estandarizadas para que en todo momento se cumplan con la Ley Fintech, Disposiciones de Banca Abierta y las normatividad de datos personales; y (vii) revisar la documentación legal que formalice la relación con el futuro proveedor así como asegurarse de que existen aprobaciones corporativas (de ser el caso).

4. Auditoría Interna. El cumplimiento de los objetivos de sistema de control interno debe cuidarse en todo momento. Si el nuevo proceso no es capaz de adoptar normas mínimas que aseguren el cumplimiento de las reglas de control interno, es poco probable que el proyecto de banca abierta sea viable para la entidad.

5. Área de Administración de Riesgos. Esta área debe evaluar si existe o cuáles son los riesgos que traerá a la entidad el intercambio de datos abiertos a través del uso de las API.

22.5 Diagrama y Plan de Trabajo.

La Entidad debe estar consciente que la entrada a Banca Abierta como Proveedor de datos no es opcional (debido a que México sigue el modelo de adopción obligatoria como se explicó al inicio de esta Sección). Actuar como Solicitante de Datos, sí lo es. Una vez que se ha realizado el acercamiento inicial para coordinar a las distintas áreas, sugerimos organizar un plan de trabajo para acercarse al Proyecto desde la siguiente perspectiva:

1) Identificar con las áreas de negocios cuáles son los Datos Abiertos que la Entidad está en posibilidad de compartir. La definición de la normatividad es amplia, por lo cual quizás habría que crear grupos de trabajo que definan de manera adecuada qué es lo que, por ahora, la Entidad estaría obligada a poner a disposición de posibles Proveedores de Datos.

2) El área legal debe validar que los Datos Abiertos tengan precisamente dicha característica, es decir, debe cuidar que los mismos puedan ser compartidos sin violar las reglas en materia de datos personales y secreto financiero (ver Sección 9 Datos Personales y Secreto Financiero).

3) El área legal y el área de sistemas deben revisar detalladamente los requerimientos técnicos sobre la manera en que las Disposiciones de Banca Abierta requieren que se comparta la información, en específico los anexos técnicos de la misma que contienen especificaciones de seguridad y arquitectura de datos.

4) Las reuniones anteriores deberán servir para efecto de sacar las siguientes conclusiones:

    1) Necesidad de un proveedor (ya sea un Proveedor Relevante o uno que se encuentre dentro de la categoría de Servicios Excluidos), así como la infraestructura propia que deberán adquirir.

    2) Puntos abiertos y sujetos a consulta del regulador, sobre todo relacionados con aspectos de implementación inmediata: plazos estimados para terminar el proceso, caracterización de ciertos datos como abiertos, entre otros.

5) Una vez realizado este diagnóstico inicial, el Director General junto con las áreas de negocios o financieras deberá establecer un presupuesto y los costos asociados al establecimiento de dicho esquema, así como los objetivos inmediatos para poder cumplir con las Disposiciones de Banca Abierta.

Para todos los efectos prácticos, estamos asumiendo que el Proyecto anterior tendrá como objetivo inmediato que la Entidad se encuentre en cumplimiento de los aspectos esenciales que le marca las Disposiciones de Banca Abierta actualmente emitidas y

vigentes. En todo caso, actuar como Solicitante de Datos constituiría un tema distinto. Así mismo, cuando se emitan las disposiciones siguientes en materia de datos transaccionales y agregados.

Beneficios de la Banca Abierta para Solicitantes y Proveedores

Gráfica 25. Beneficios de la Banca Abierta para Solicitantes y Proveedores. Fuente: Vite Abogados

22.6 Regulador.

Consideramos que un acercamiento con CNBV para efecto de poder cumplir adecuadamente con las Disposiciones de Banca Abierta es importante. Es necesario que la Entidad realice un diagnóstico de los Datos Abiertos con los que cuenta para efecto de establecer los costos y la dimensión de lo que implicará cumplir con la normativa.

22.7 Temas prácticos y recomendaciones.

A partir de una investigación realizada por una firma internacional de investigación de mercados[117], se desprendió que el 58% de los consumidores con una aplicación de banca móvil podría ser persuadido para cambiar a una entidad financiera solo para dispositivos móviles para obtener la "*capacidad de realizar un mayor número de acciones relacionadas con la banca abierta a través del móvil*". Además, de esta investigación también se desprendió que los consumidores también están dispuestos a acceder a sus servicios a través de una interfaz de terceros de un proveedor no tradicional: de los consumidores con una aplicación relacionada con servicios financieros, el 49% confiaría un proveedor de pagos digitales para proporcionar esto, mientras que el 43% confiaría en un minorista tradicional para hacerlo[118].

Los datos, la innovación habilitada por la tecnología y las preferencias cambiantes de los clientes a largo plazo conducirá a un futuro en el que las entidades, los productos, servicios y funciones están abiertos a terceros. En este nuevo modelo de mercado los clientes podrán utilizar una única interfaz bancaria para acceder a los productos y servicios de una multitud de actores, incluidos los titulares de bancos, entidades financieras e instituciones de tecnología financiera. Esta interfaz otorga a los clientes una descripción general y utilizan análisis cognitivos para ayudar a que los clientes administren y optimicen sus finanzas.

A medida que sea más fácil para los clientes cambiar entre proveedores de cuentas y comparar otros productos basados en precio, los operadores tradicionales corren el riesgo de perder participación de mercado y ver márgenes de beneficio reducidos. Además, los terceros pueden crear nuevas propuestas que satisfacen las necesidades insatisfechas, utilizando los datos abiertos para brindarle al cliente beneficios. Como resultado, los operadores tradicionales podrían perder relación con los clientes si estos eligen cada vez más gestionar sus finanzas a través de una interfaz de terceros.

[117] YouGov. Breaking the Banks? Revolut, Starling and the rise of "challenger" firms. (2020) Consultado en: https://yougov.co.uk/topics/finance/articles-reports/2020/08/14/breaking-banks-revolut-starling-and-rise-challenge

[118] YouGov. Future Banking. (2015) Consultado en: Results-for-Pinsent-Mason-Future-Banking-221015.pdf

En particular, la Banca Abierta se ha inspirado en el aumento de las API en otras industrias. Las API definen métodos estandarizados para interacción con sistemas de software.

Al igual que un enchufe que permite la conexión de dispositivos eléctricos a la red, las API permiten que las aplicaciones móviles se "conecten" a sistemas de terceros. El aumento de la popularidad entre los desarrolladores de aplicaciones del uso de API para incorporar datos de terceros destaca su potencial de apertura hasta los datos bancarios del cliente.

Casos de Uso	
Banca tradicional	**Banca Abierta**
Ana necesita retirar efectivo del cajero y al visitarlo, éste no tiene efectivo disponible.	Ana podrá entrar a una aplicación móvil bancaria o no, en la que obtendrá la ubicación y visibilidad sencilla en línea del cajero o sucursal de cualquier entidad. Además de visualizar la disponibilidad de efectivo, acceso a contratación de diferentes servicios, precio de comisiones, depósitos en efectivo, si cuenta o no con estacionamiento, acceso para discapacitados, ubicación dentro o fuera de plazas comerciales, entre otros.
Juan está por empezar a planear sus vacaciones de este año con su familia y tiene que buscar las mejores ofertas y mejores planes de pago, lo cual sabe que será un proceso tedioso.	Con una solución digital autorizada por Juan conocerá las fechas en las que él viajará y reconoce cuándo planea y cuáles son sus gustos por lo que le evita este largo proceso de selección y le sugiere las opciones de hoteles, transportación y actividades que más le convienen con base en sus vacaciones previas, así como los métodos de pago que más le convienen en este momento.
Ana está interesada en una tarjeta de crédito que tenga beneficios exclusivos y que no tenga anualidad. Para escoger la mejor opción, investiga en cada sitio web de los bancos o visita sus sucursales para así obtener información y hacer una tabla comparativa.	Desde una app, Ana puede visualizar todas las ofertas de tarjetas de crédito, puede comparar la línea de crédito, anualidad, comisiones, recompensas y su historial crediticio. Puede obtener una recomendación personalizada de acuerdo a sus necesidades.

Tabla 9. Casos de Uso

SECCIÓN 23.- CREACIÓN DE OPORTUNIDADES DE NEGOCIO EN LÍNEA.

El día de hoy existen muchas fuentes para realizar actividades de publicidad de los servicios financieros. Además, existe el reto de hacer productiva dicha publicidad. La abundancia de medios en línea o a través de medios masivos de comunicación hace que el espacio de atención de las personas se reduzca, lo cual resulta en el hecho que dichos anuncios no siempre se reflejen en un aumento en el número de clientes o Socios para una Entidad.

Existen diversas tendencias de publicidad (o *marketing*) para las entidades financieras, entre las cuales destacamos las siguientes:

- Publicidad mediante teléfonos celulares o móviles, mediante la inserción de anuncios en sitios web o aplicaciones especialmente diseñadas para este medio. Asimismo, el pago de publicidad a buscadores (e.g. Google) juega un papel relevante.
- Campañas dirigidas a grupos o sectores de mercado específico, brindando información útil sobre los servicios que ofrece la Entidad. Esto puede realizarse de manera bastante efectiva si se realizan acercamientos en línea. Actualmente existen herramientas de publicidad dirigida a través de redes sociales que algunos miembros del SACP utilizan para dirigir la oferta de sus productos y servicios a personas cuyo perfil en internet indica que podrían ser de su interés.
- Asistencia e información a través de chatbots (ver Sección 20 Automatización de Procesos), es decir, programas automáticos que estén capacitados para realizar una interacción (así sea limitada) con los potenciales clientes para completar procesos de contratación, resolución de dudas, entrega de documentos, entre otros.
- Identificar patrones en los visitantes de los sitios web o usuarios de las aplicaciones ofrecidas por las Entidades para efecto de realizar ofertas personalizadas. Sin embargo, ello debe hacerse con respeto a los datos personales de los potenciales Clientes o Socios (Ver Sección 8 Datos Personales y Secreto Financiero).

Desde luego, la lista anterior no es exhaustiva y existe la posibilidad de realizar una mezcla de varias tendencias con el fin de llegar a una fórmula que se adapte al plan de marketing de cada Entidad.

Una modalidad que resulta bastante útil es la contratación de un especialista en publicidad que diseñe una plataforma que contenga las ofertas de productos y servicios financieros de la Entidad, incluyendo el apoyo para ciertos procesos de evaluación o pre-contratación de los servicios financieros. Ello tiene la ventaja de liberar a la Entidad de la carga de realizar planes de diseño web o aplicaciones móviles y dejar que un experto en la materia utilice su experiencia para generar "oportunidades de negocio", es decir, información de personas que están dispuestas a contratar los servicios de la Entidad.

El modelo anterior incluso puede combinarse o contratarse por las Entidades a través de un modelo de Marketplace, es decir, mediante la inclusión de la oferta de servicios de las Entidades en un sitio web especializado que permita a un cliente potencial comparar los diversos productos y servicios y obtener datos que les permitan tomar una decisión informada. Esto corresponde a cierta tendencia a "uberizar" el ofrecimiento de los servicios: así como la famosa aplicación. Aunque quizás una mejor analogía sea la de Amazon: un mercado abierto donde se facilita el ofrecimiento de bienes de manera abierta y mediante el uso inteligente de información. De este modo, un esquema de Marketplace financiero permite a una persona seleccionar a una entidad financiera entre varias dentro de un mismo entorno. No se trata de que las Entidades comiencen a realizar actividades de intermediación a modo de las instituciones de financiamiento colectivo (ver Sección 24 Alianzas). El modelo de financiamiento colectivo o P2P (*peer to peer* o de persona a persona) tiene características propias. En especial, es un modelo donde existe una intermediación por parte de un tercero para que se realice un flujo a través de una plataforma para fondear proyectos o personas específicas. Como veremos más adelante, existen diferencias importantes entre un servicio profesional basado en publicidad y la realización de una actividad regulada de financiamiento colectivo.

Lo anterior tiene que llevarse a cabo mediante un cuidadoso análisis del proveedor de servicios publicitarios o de Marketplace. A diferencia de lo que hemos comentado para Uber, el modelo mexicano de Marketplace financiero es incipiente y las Entidades deben considerar su uso siempre que se hayan analizado varios elementos legales, regulatorios

y operativos. Algunas Entidades que ya utilizan este tipo de servicio han notado las siguientes ventajas:

- Captación adicional o colocación más efectiva de servicios ofertados.
- La contraprestación de la plataforma puede pactarse según el éxito de la misma y no por rentas fijas, por lo que es fácilmente amortizable el costo mencionado.
- Las funciones de marketing, administración y operación corren a cargo del proveedor de la plataforma.
- Capacidad de llegar a una audiencia importante de clientes potenciales.
- Creación de presencia en línea sin incurrir en los costos que conllevaría desarrollarla *in-house* o contratar un proveedor.

23.1 Concepto.

Como hemos mencionado en la Sección 1 (Introducción), cada caso debe ser analizado por los expertos y asesores de las Entidades previo a su implementación. El modelo al que podrían acceder las Entidades para generar oportunidades de negocio bajo el modelo de Marketplace tiene las siguientes características:

- El objetivo primordial es la generación de "oportunidades de negocio" (Potencial Cliente), es decir, generar el interés de un visitante a la página o aplicación correspondiente para que dicha persona: (i) manifieste su voluntad de adquirir en el presente o en el futuro, un servicio ofertado por una Entidad, y (ii) proporcione los datos necesarios para efecto de recibir publicidad o realizar un proceso de contratación con la Entidad.
- La página o aplicación exhibe diversas ofertas de servicios financieros (por ejemplo, de captación) ofrecidos por diversas entidades financieras (bajo este esquema, la plataforma trabaja como un escaparate de varias ofertas de servicios) de modo que el Potencial Cliente puede elegir entre varias opciones. Las ofertas son realizadas bajo la marca y por las Entidades directamente. El proveedor de la plataforma (Agente de Publicidad) no interviene en el ofrecimiento ni realiza por sí mismo la actividad financiera.

- Las ofertas dentro de la plataforma se refieren a servicios ya autorizados y ofrecidos por las Entidades. El Agente de Publicidad no genera ni proyecta servicios nuevos, pues se presupone que dichos servicios ya están debidamente implementados por la Entidad y que incluso pueden ser corroborados en su propio sitio web, así como en los registros que administra Condusef en materia de transparencia.

- El Agente de Publicidad se rige bajo un principio de neutralidad en el ofrecimiento de los servicios. La Entidad debe asegurarse que sus servicios sean ofrecidos bajo un principio de igualdad y no discriminación frente a los ofrecidos dentro de la plataforma. El Agente de Publicidad no debe actuar como un asesor de inversión de los Potenciales Clientes, por lo que no existe bajo este esquema la creación de portafolios de servicios o instrumentos que sean recomendados: el Potencial Cliente es quien debe tener la última palabra y la decisión de iniciar un proceso de contratación con alguna de las Entidades.

- El Agente de Publicidad no debe ostentarse como entidad financiera ni actuar como tal. Las Entidades deben ser conscientes de que los procesos de contratación, operaciones y administración de la relación con el Potencial Cliente cuando éste ya está por convertirse en un cliente deben correr y realizarse por la Entidad misma. En este caso el Agente de Publicidad debe abstenerse de recibir o administrar dinero.

- La función del Agente de Publicidad es doble: (i) proporcionar el medio virtual (aplicación o web) para la oferta de servicios y (ii) recolectar datos de los Potenciales Clientes para efecto de transmitirlos a las Entidades seleccionadas por aquel para iniciar el proceso de contratación. En algunos casos el Agente de Publicidad puede actuar como auxiliar de las Entidades para resolver dudas puntuales sobre los servicios ofertados por la Entidad y orientación para comenzar el proceso de contratación con ésta.

- El Agente de Publicidad no realiza la contratación por cuenta de las Entidades. Este punto es especialmente relevante en el esquema descrito: no existe una representación de la Entidad por parte de dicho Agente de Publicidad, lo cual lo excluye (en principio) de una relación de comisión mercantil. No existe siquiera una intermediación de servicios financieros pues no existe flujo transaccional a través del Agente de Publicidad. Como dijimos antes, se trata más bien de un escaparate (más parecido en cierto sentido a Amazon en cuanto que muestra diversos productos o servicios disponibles, con la salvedad de que en la contratación y el

depósito o desembolso no existe a través de la plataforma), de conjuntar las diversas ofertas vinculantes de varias Entidades.

- El proceso de contratación final (y en la conversión del Potencial Cliente a Cliente) se realiza entre la Entidad y el Potencial Cliente de manera directa, mediante los medios (físicos o electrónicos) que ésta tenga a disposición. Si bien el Agente de Publicidad puede realizar labores de facilitación para llevar a cabo la contratación, la Entidad debe tener en mente que no se trata de un servicio "todo incluido" donde se pueda confiar la totalidad del proceso a dicho Agente de Publicidad.
- El ciclo de la generación de los Potenciales Clientes puede resumirse de la siguiente manera:

  (i) El Potencial Cliente visualiza las diversas ofertas de servicios que residen en la plataforma.

  (ii) Revisa los servicios que se ofertan por las Entidades en la plataforma. Tiene oportunidad de realizar preguntas genéricas sobre cada producto mediante chatbots o servicios de asistencia puestos a su disposición de los Potenciales Clientes.

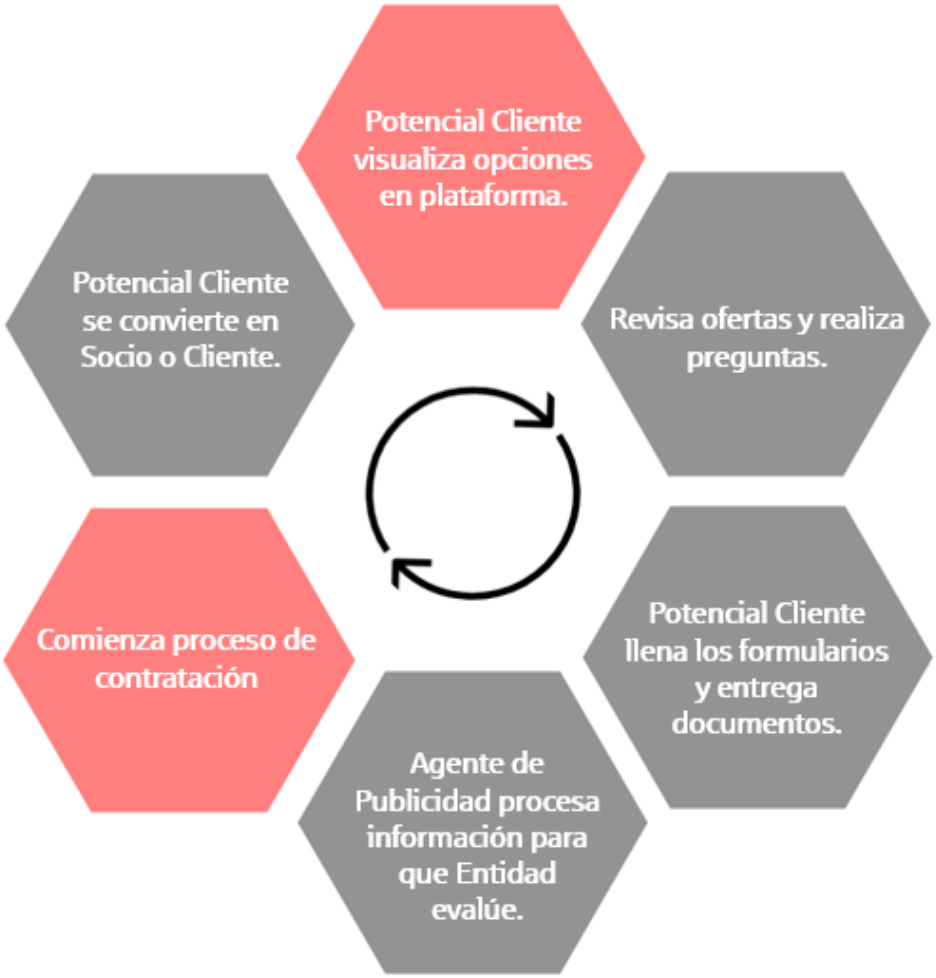
  (iii) El Potencial Cliente llena los formularios y entrega vía la plataforma ciertos documentos y datos necesarios para que la Entidad esté en posibilidad de evaluar la posible contratación con dicha persona.

  (iv) El Agente de Publicidad procesa dicha información y, en caso de ser viable, la entrega a la Entidad para efecto de que realice una evaluación de esta y, en su caso, comience el proceso de contratación.

  (v) En caso de considerar viable la posible contratación la Entidad se pone en contacto con el Potencial Cliente para efecto de comenzar el proceso de contratación.

  (vi) Finalmente, el Potencial Cliente se convierte en Socio o Cliente de pleno derecho y realiza los actos conducentes a ejecutar o cumplir con su parte en el contrato celebrado con la Entidad (por ejemplo, realiza el depósito).

Diagrama del funcionamiento de oferta de servicios en línea



Gráfica 26. Diagrama del funcionamiento de oferta de servicios en línea. Fuente: Vite Abogados

23.2 Regulación.

Las Entidades, son personas morales altamente reguladas, cuyo régimen legal influye en las decisiones de negocios. En ese sentido, dependiendo del tipo de esquema de Marketplace, podríamos tener varios escenarios:

- Modelo Publicitario Simple. El proveedor únicamente provee servicios de publicista y operador de una plataforma propia de la Entidad. En este sentido, es probable

que estemos en un supuesto de servicio profesional que puede considerarse como un Servicio Excluido, siempre que sólo exista un contrato en donde prácticamente el proveedor no realiza ningún proceso continuado y no tiene acceso alguno a información. La implementación por lo tanto sería más sencilla y no requeriría de una intervención tan activa por parte de CNBV.

- Comisionistas. La contratación de un comisionista o de un tercero con facultades para representar de manera activa a la Entidad frente a terceros, así como desarrollar procesos de contratación y apoyo a la Entidad para atender a los Socios o Clientes requiere de una intervención activa del regulador, así como una planeación más extensa. En ese sentido, estaríamos frente a un contrato como los descritos en la Sección 15 (Contratación de Proveedores y Comisionistas), por lo cual el proceso sería el mismo que hemos descrito en esa sección.

- Modelo Marketplace. El Marketplace como está descrito en la sección anterior, es un modelo "híbrido" entre los supuestos mencionados anteriormente: no existe la facultad de representar a la Entidad, no existe acceso a la información o procesos de los Clientes o Socios (sólo previo a que adquieran dicha calidad cuando son Potenciales Clientes, es decir, cuando sólo son una oportunidad de negocio para la Entidad).

- Transparencia. Como se mencionó en la Sección 5 (Transparencia y Ordenamiento de los Servicios Financieros), las Entidades deben cumplir con ciertos estándares mínimos para el ofrecimiento de sus servicios. En general, tal como se indicó en esa sección, el usuario (o posible usuario en este caso) de los servicios financieros, debe conocer los términos y las condiciones bajo las cuales podrá contratar con una entidad financiera. Al respecto, el contrato que documente el esquema que se propone esta sección debe ser muy claro para obligar al contratista a cumplir con la regulación aplicable en materia de transparencia. Incluso sugerimos establecer un esquema de vigilancia y de monitoreo para asegurarse que el sitio web donde se establezca el Marketplace cumple con las especificaciones normativas indispensables. El contrato no puede usarse por las Entidades como una manera de delegar o deshacerse de su responsabilidad en la materia, por lo que deben prestar especial atención a este tema.

El Modelo Marketplace tendría como base de prestación de servicios para efecto de que el Agente Publicitario ponga a disposición de la Entidad la plataforma, así como servicios

auxiliares para efecto de generar oportunidades de negocio. El Agente Publicitario interviene sólo en la creación de la página web, en realizar el soporte de la misma, en proporcionar la herramienta para la obtención de información de identificación y contacto de las personas potencialmente interesadas en contratar los servicios y productos autorizados que ofrece la Entidad al público en general, para efectos de que ésta realice los procesos de originación y, en su caso, celebración de los contratos correspondientes con dichas personas, y apoyar a la Entidad a brindar orientación muy general a las personas interesadas en dichos servicios.

Es importante precisar que en ningún caso ni los Potenciales Clientes ni Clientes o Socios finales (ya con relación jurídica y de negocios con la Entidad) pueden realizar operación financiera o de ahorro alguna a través de la plataforma, siendo ésta únicamente un primer canal de la Entidad para la identificación y contacto de oportunidades de negocio y de provisión de información sobre los productos y servicios de la Entidad.

Hay que tomar en cuenta que los procesos de integración de expedientes únicos de identificación y realización de entrevistas con clientes potenciales, evaluación y análisis de historiales crediticios, contratación de cliente, apertura de cuentas, realización de depósitos, firma de contratos y manejo y administración de la cuenta, fondeo y manejo de información relacionada con la misma deben realizarse directamente por la Entidad, sin que el Agente Publicitario tenga injerencia, capacidad de decisión, visibilidad o intervención alguna, ni a nivel información o sistema.

Como consecuencia, el Agente Publicitario deberá realizar sus actividades dentro de los siguientes parámetros para que el proceso de revisión del contrato correspondiente ante CNBV sea más rápido e, incluso, se le caracterice como un Servicio Excluido:

- El Agente Publicitario no debe, bajo ninguna circunstancia, ofrecer por sí mismo servicio ni producto financiero ni de ahorro o cualquier otro que requiera autorización de los Reguladores, ni fungir como intermediario entre los clientes potenciales o finales y la Entidad a través de la transmisión de dinero o esquema similar que implique temas transaccionales dentro de la plataforma.
- El Agente Publicitario no debe actuar por cuenta ni a nombre de la Entidad en su carácter de comisionista o mandatario para efecto de realizar la contratación de clientes.

- Una vez que los Potenciales Clientes se convierten en Clientes o Socios de las Entidades, el Agente Publicitario no debe intervenir en los procesos de administración de la información confidencial y transaccional de los clientes de la Entidad.
- El Agente Publicitario no debe prestar servicios operativos ni administrativos relacionados con la clientela de la Entidad, ni en relación con los servicios que son propios de la Entidad como entidad regulada.
- Los servicios del Agente Publicitario no deben incluir procesos de identificación de clientes en materia de PLD/FT. La identificación a distancia es un proceso que requiere autorizaciones y cambios específicos, por lo que la Entidad deberá ser la encargada de realizar y completar por sí misma dicho proceso.
- La plataforma que el Agente Publicitario ponga a disposición de las Entidades debe considerarse como una herramienta comercial de las Entidades para potencializar el ofrecimiento de sus servicios. La Entidad en todo momento debe ser la persona moral que realice la oferta de servicios y, en su caso, captación de recursos como tal.

No obstante que un modelo de Marketplace regido por las reglas anteriores podría conceptualizarse como un Servicio Excluido y, por lo tanto, no ser objeto de una autorización por parte de la CNBV, sugerimos acercarse a dicho regulador para efecto de caracterizar de manera adecuada el contrato: cada acuerdo con Agentes Publicitarios puede tener variaciones y la interpretación de dicho organismo es importante para asegurar que habrá una implementación adecuada.

Asimismo, será necesario que ambas partes celebren un contrato de cesión de datos personales (ver Sección 9 Datos Personales y Secreto Financiero) y tomar en cuenta la normatividad en la materia para efecto de evitar contingencias en la transmisión de datos de los Potenciales Clientes.

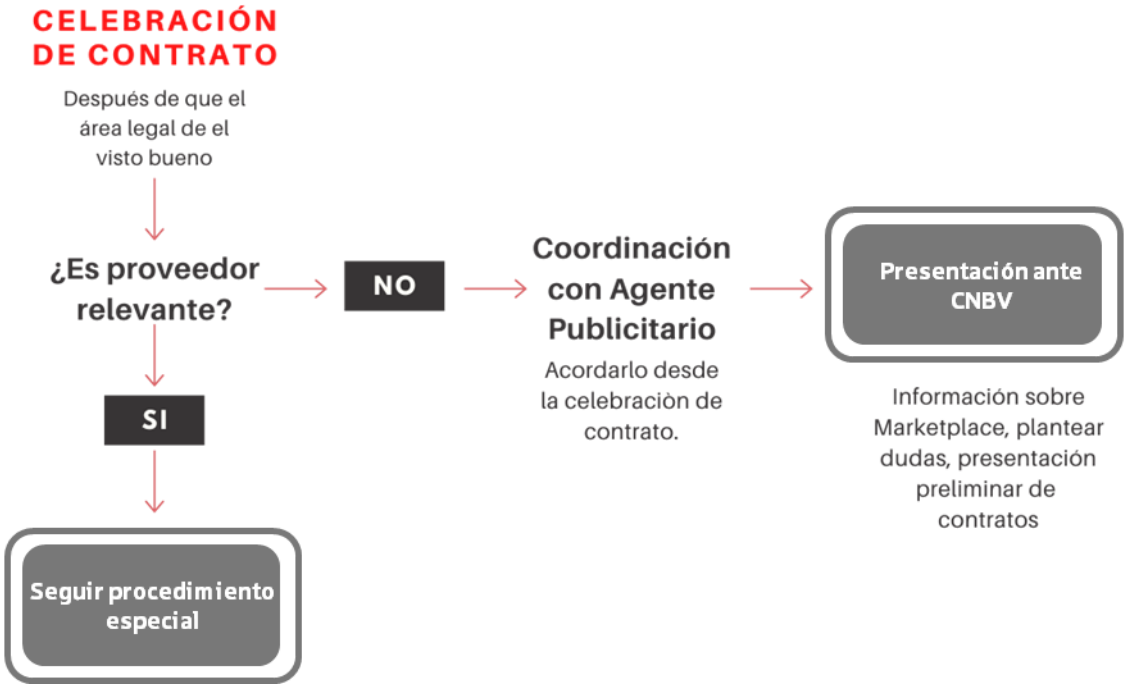
23.3 Coordinación y Acercamiento Inicial

La coordinación inicial para llevar a cabo una implementación de contrato Marketplace con un tercero, debe considerar lo siguiente:

- Identificar de manera adecuada cuáles son los servicios que requieren de una oferta en línea. Establecer el catálogo de los mismos para efecto de revisar si no existe algún impedimento para realizar una oferta en línea en el propio contrato de adhesión del servicio relevante.
- Involucrar a las siguientes áreas en el análisis inicial: Oficial de Cumplimiento, Auditoría Interna, Dirección General y áreas de negocios para efecto de recorrer con ellos el proceso publicitario e identificar aspectos problemáticos en la implementación o que consideren necesario consultar con CNBV.
- Las áreas convocadas deberán examinar los Manuales de la Entidad para entender la necesidad de modificarlos conforme al nuevo proceso publicitario, así como las autorizaciones corporativas que deban solicitarse.
- El Oficial de Cumplimiento deberá validar que, en su caso, el contrato con el Agente Publicitario no implique que el proceso acordado sea caracterizado como identificación no presencial: como se mencionó en la sección 6 (Prevención de Lavado de Dinero y Financiamiento al Terrorismo), ello está sujeto a varias limitaciones y requiere autorizaciones especiales. El Agente Publicitario es sólo un auxiliar para recabar información de potenciales relaciones de negocio, bajo ninguna circunstancia debe entenderse como un auxiliar en materia de identificación de clientes.
- Nombrar a una sola persona como administrador del proyecto y canalizar el contacto con el Agente Publicitario mediante dicha persona. Es recomendable que todas las preguntas, objeciones y comentarios al Agente Publicitario se realicen de manera ordenada.
- Mapear tanto el proceso de publicidad como el de contratación, estableciendo puntos importantes y áreas encargadas de supervisarlos. Tomar en cuenta que el proceso de contratación pertenece a la Entidad.
- Firmar los convenios de confidencialidad y cartas de intención con el Agente Publicitario para asegurar que cualquier información relevante de la Entidad permanecerá con dicho carácter.
- Acordar con el Agente Publicitario la estrategia que se seguirá para presentar el contrato a la CNBV. Si bien la entidad regulada por un acto de cortesía profesional frente al regulador debe realizar dicha presentación de manera coordinada. Esto

también conlleva la necesidad de crear presentaciones y materiales necesarios para acordar cada uno de los procesos, que podrían verse de la siguiente manera

Diagrama de flujo para celebrar un contrato de *Marketplace*



Gráfica 27. Diagrama de flujo para celebrar un contrato de Marketplace. Fuente: Vite Abogados

23.4 Diagrama y Plan de Trabajo.

El plan de trabajo para un Proyecto de un Marketplace debe considerar los siguientes pasos y procesos:

- Coordinación inicial adecuada y análisis legal y operativo con base en lo expuesto en la sección anterior. Una planeación inicial de los aspectos operativos y legales es esencial.

- Revisión de los diversos proveedores publicitarios para determinar si se ajustan al modelo de Marketplace y acordar con ellos un acercamiento que permita (i) entender si efectivamente sus servicios pueden considerarse Servicios Excluidos,

(ii) los procesos específicos que llevará a cabo el Agente Publicitario para cumplir con sus obligaciones y (iii) resolver cualesquier dudas u objeciones que surjan sobre los aspectos legales y operativos del proceso.

- Presentar al Consejo de Administración la posible alianza con el Agente Publicitario y obtener su aprobación para la celebración del contrato correspondiente. Explicar, mediante presentaciones o materiales elaborados para ello, el tipo de servicio de que se trata.

- Revisar la plataforma (web o aplicación) para determinar si será necesario solicitar adaptaciones al Agente Publicitario e involucrar al asesor o área legal en dicha revisión: como hemos visto anteriormente en la **Sección 5** de la Guía Legal, las Entidades deben cumplir con ciertas obligaciones en materia de transparencia y el hecho de tercerizar dicho proceso no implica una excepción a cumplir con esas normas.

- Es posible que el Agente Publicitario tenga ya un contrato estandarizado. Para ello será necesario que las Partes Responsables del Proyecto tengan especial atención en lo siguiente:

  (i) Aspectos relacionados con la contraprestación que se pagará al Agente Publicitario.

  (ii) Supuestos de incumplimiento y responsabilidades mutuas de las partes en el futuro contrato.

  (iii) Clausulado mínimo y regulatorio que debe cumplir el Agente Publicitario.

  (iv) Condiciones y términos bajo las cuales se prestarán los servicios publicitarios, incluyendo la facultad de la Entidad de realizar revisiones a la plataforma para asegurarse de que todo está en cumplimiento con la normatividad aplicable.

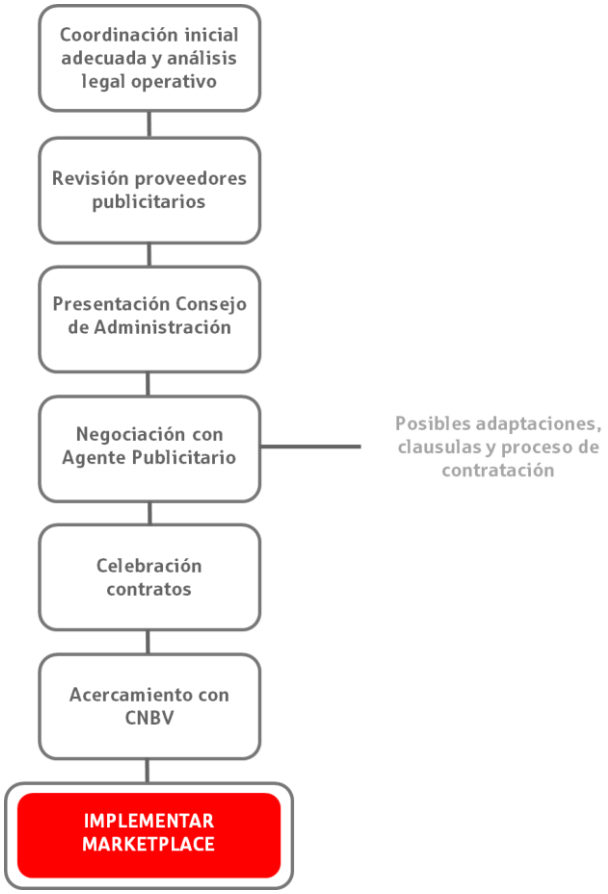
  (v) Detalle sobre la responsabilidad de gastos en cada proceso que se haya mapeado por las Partes Responsables.

- Acordar el proceso de contratación y, en su caso, el apoyo que el Agente Publicitario requiera para cerrar la relación con el Potencial Cliente, cuidando en todo momento la confidencialidad de la información de los Socios o Clientes.

- Celebrar los contratos de cesión y administración de datos personales con el Agente Publicitario para efecto de hacer legal la operativa de transmisión de datos.

- Acercamiento con CNBV para efecto de determinar si el contrato debe estar sujeto a un proceso similar al de un Proveedor Relevante, incluso en el supuesto de que se trata de un Servicio Excluido y ajustar el cronograma y las expectativas del negocio a dicho proceso.

Plan de Trabajo para la implementación de un Marketplace



Gráfica 28. Plan de Trabajo para la implementación de un Marketplace. Fuente: Vite Abogados

23.5 Regulador.

Sugerimos realizar un acercamiento pronto y adecuado con CNBV previo a celebrar un contrato bajo alguna de las modalidades presentadas en esta sección. Si bien puede tratarse de Servicios Excluidos, es decir, servicios profesionales que no constituyen ninguno de los supuestos tratados en las secciones 15 (Contratación de Proveedores y Comisionistas) y 16 (Prestadores de Servicios Operativos), de cualquier modo, se trata de un cambio importante en aspectos que pueden incidir en el modelo de captación de la Entidad.

23.6 Temas prácticos y recomendaciones.

En nuestra experiencia, para efecto de llevar a cabo una implementación adecuada de este tipo de contratos es muy importante considerar:

- El involucramiento de la Dirección General y el Consejo de Administración es esencial para garantizar el éxito del Proyecto. Es común que al considerarse esto como un contrato común o no sujeto a regulación esto no se lleve a cabo. Un análisis a tiempo y adecuado de todos los aspectos mencionados hace mucho más eficiente la comunicación interna.
- El acercamiento con CNBV debe hacerse en el momento en que se tengan acordados los procesos que se llevarán a cabo con ayuda del Agente Publicitario. El tiempo de los Reguladores debe ser aprovechado de manera productiva y todos los datos son relevantes para que ellos emitan un punto de vista.
- Las negociaciones deben ser dirigidas por una sola persona (generalmente un funcionario de la Entidad), debidamente asesorada sobre los aspectos técnicos, de negocios y operativos. Contradicciones o discutir frente al Agente Publicitario temas que deben ser objeto de análisis interno pueden ir en contra del cumplimiento de los tiempos de implementación.

SECCIÓN 24.- ALIANZAS.

24.1 Tipos de Alianzas.

La celebración de alianzas con otras entidades financieras o comerciales puede ser una forma extremadamente eficiente y efectiva de acercar a las Entidades a sus metas de digitalización a corto, mediano y largo plazo. Estas alianzas pueden aportar nuevos clientes o socios, apoyarlas a reducir sus riesgos, a hacer más eficientes sus procesos y, en particular, aportarles infraestructura tecnológica, conocimiento (*know-how)* e insumos para apoyarlas con la digitalización de sus servicios.

Genéricamente, las Entidades pueden documentar las alianzas estratégicas que celebren con otras entidades de la siguiente forma:

- *Alianzas Contractuales*[119],. Estas alianzas pueden adaptarse fácilmente a las necesidades específicas de ambas partes. Pueden celebrarse, por ejemplo, contratos de prestación de servicios, de comisión mercantil o de licencia, entre otros, de acuerdo con las necesidades de ambas partes en la alianza.
- *Virtual Joint Ventures*[120], en los cuales no se crea una nueva sociedad, sino que, para aprovechar las actividades permitidas para cada una de las partes, sus capacidades, la infraestructura tecnológica, el alcance de mercado y demás insumos, ambas partes se unen, como empresas separadas, con el objetivo de maximizar su rentabilidad.
- *Joint Ventures o Convenios de Cooperación*[121], para crear nuevas entidades que permitan a las partes aprovechar la experiencia y los conocimientos que cada una ha adquirido a lo largo de su trayectoria comercial.
- *"Socios de Etiqueta Blanca",* en donde tanto las Entidades como los potenciales aliados refieren a los clientes o potenciales clientes a la otra entidad cuando esta última ofrece productos o servicios que ella misma no ofrece.

[119] De Man, Ard-Pieter. (2013) *Alliances.* P. 101.
[120] Op. Cit. P. 71.
[121] Op. Cit. P. 121.

Área de oportunidad para alianzas estratégicas

Gráfica 29. Área de oportunidad para alianzas estratégicas. Fuente: Vite Abogados

Aunque esta lista no pretende ser exhaustiva, nuestra experiencia es que la mayoría de las alianzas estratégicas se celebran mediante alguna de estas cuatro formas o alguna variante similar. Cada una de estas alianzas tienen ventajas y desventajas que deben valorarse para determinar la forma más eficiente y efectiva de colaborar con otras entidades.

Específicamente, los tipos de alianzas están limitados únicamente por lo que está permitido por la regulación aplicable para las partes (Instituciones de Tecnología Financiera y los miembros del SACP) y, en segundo lugar, por las capacidades tecnológicas y financieras de cada una. A modo de ejemplo, proponemos las siguientes capacidades

que hemos identificado en el mercado de servicios tecnológicos y financieros en México que podrían fungir como potenciales aliados de las Entidades:

- Los servicios financieros a través de páginas de internet y/o aplicaciones móviles tienen acceso a mercados distintos y a un gran porcentaje de la población mexicana.
- El uso del sistema de pagos SPEI o CoDi permiten que se puedan entregar y recibir fondos a través de transferencias electrónicas.
- Las Instituciones de Fondos de Pago Electrónico (explicadas más adelante) podrían permitir a los socios o clientes de las Entidades mantener un saldo virtual a través de una página de internet o una aplicación.
- Software de originación y *onboarding* de créditos.
- Aplicaciones para la administración de los recursos del público en general.
- Software que permite el análisis del comportamiento de los clientes.
- Infraestructura en la nube que permite reducir costos.
- Software que robustece la seguridad de los sistemas de las empresas.
- Automatización de procesos como aplicación de cuestionarios *Know Your Customer* ("KYC").
- Explorar la posibilidad de crear un modelo novedoso (explicado más adelante) junto con otras entidades financieras.
- Intercambio de capacidades informáticas, tecnológicas, de infraestructura, etc.

24.2 Consideraciones Regulatorias.

Como se menciona en la Sección 15 (Contratación de Proveedores y Comisionistas) de la presente Guía Legal, las Entidades pueden contratar con terceros, incluyendo a otras entidades financieras, la prestación de servicios necesarios para su operación. Al respecto, las Entidades deberán tomar en cuenta lo mencionado en la Sección 15 (Contratación de Proveedores y Comisionistas) de la presente Guía Legal en relación con las alianzas que pretenda celebrar cuando se trate de Proveedores Relevantes y cuando se requiera la autorización de la CNBV para su celebración.

Es importante considerar, asimismo, la regulación a la que está sujeta la contraparte de la potencial alianza. En caso de que se busque implementar una alianza con una Institución de Tecnología Financiera (o "ITF"), por ejemplo, deben tomarse en cuenta los requisitos que la CNBV solicita para que estas instituciones celebren determinados contratos. Por el contrario, si la entidad con la que se busca aliarse es una entidad comercial, simplemente habría que considerar algunos aspectos de especial relevancia como la protección de datos personales, la prevención de lavado de dinero y algunos otros, dependiendo de la naturaleza jurídica de la entidad comercial.

24.3 Actividades de Instituciones de Tecnología Financiera.

La publicación de la Ley Fintech tiene el objetivo de regular los servicios financieros que se llevan a cabo a través de las siguientes figuras:

- Las Instituciones de Financiamiento Colectivo, también conocidas como Crowdfunders (las "IFC"). Las IFC son entidades financieras supervisadas por la CNBV que tienen el objetivo de poner en contacto a personas del público en general con el fin de que entre ellas se otorguen financiamiento de deuda, de capital o de copropiedades o regalías a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónico o digital.[122]
- Las Instituciones de Fondos de Pago Electrónico, también conocidas como e-wallets (las "IFPE"). Las IFPE, igualmente, son entidades reguladas por la CNBV que tienen el objetivo de emitir, administrar, redimir y transmitir fondos de pago electrónico, que la Ley Fintech define como "fondos que estén contabilizados en un registro electrónico de cuentas transaccionales" y que queden referidos, en general, a un valor monetario equivalente a una cantidad de dinero.[123]
- El uso de activos virtuales, para lo cual las ITF deben solicitar la autorización de Banxico.
- Los Modelos Novedosos. Los Reguladores están facultados para autorizar a entidades financieras, o bien, a personas morales distintas de las ITF, las entidades financieras y otras instituciones supervisadas para obtener una autorización temporal para operar mediante un "modelo novedoso", que les permita prestar

[122] Artículo 15 de la Ley Fintech.
[123] Artículo 22 de la Ley Fintech.

temporalmente servicios propios de las instituciones financieras utilizando herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado.[124]

Todas estas figuras requieren autorización de la CNBV (salvo los Modelos Novedosos, donde es necesario solicitarla al Regulador correspondiente). Las autoridades encargadas de implementar el contenido de la Ley Fintech son la CNBV, Banxico y la SHCP, por lo que, al igual que las Entidades, las ITF están sujetas a regulación en materia de contratación con terceros, prevención de lavado de dinero, límite de recepción y de entrega de recursos y en relación con las actividades que están permitidas por la legislación.

Es relevante tomar en cuenta que, a diferencia de las Entidades, los recursos de las ITF no estarán garantizados por el Gobierno Federal ni por ninguna dependencia gubernamental.

En el momento de escribir estas líneas existen varias ITFs autorizadas para operar. Existen, sin embargo, muchas otras que se encuentran operando normalmente al amparo de la Disposición Octava Transitoria de la Ley Fintech. Esta disposición indica lo siguiente:

> *Las personas que a la entrada en vigor del presente ordenamiento se encuentren realizando las actividades reguladas en esta Ley deberán dar cumplimiento a la obligación de solicitar su autorización ante la Comisión Nacional Bancaria y de Valores en los términos en que se establezca en las disposiciones de carácter general que para tal efecto se emitan, en un plazo que no exceda de doce meses contado a partir de la entrada en vigor de estas disposiciones. Dichas personas podrán continuar realizando tales actividades hasta en tanto la Comisión Nacional Bancaria y de Valores resuelva su solicitud, pero hasta en tanto no reciban la autorización respectiva deberán publicar en su página de internet o medio que utilice que la autorización para llevar a cabo dicha actividad se encuentra en trámite por lo que no es una actividad supervisada por las autoridades mexicanas.*[125]

[124] Artículo 86 de la Ley Fintech.
[125] Ley Fintech.

Esta Disposición permite que algunas ITF puedan operar como tal sin estar reguladas por las autoridades mexicanas durante un periodo que terminará en los próximos meses (cuando se resuelva su solicitud de autorización). Este punto es relevante en cuanto a que, al no estar reguladas como entidades financieras, el riesgo de cualquier alianza o potencial alianza aumenta considerablemente, toda vez que existe la posibilidad de que se le niegue la autorización. Este debe ser un punto central en caso de que se busque celebrar una alianza con cualquier ITF en este momento.

24.4 Régimen de Contratación de las ITF.

Al igual que las Entidades, las ITF, tienen reglas especiales de contratación para determinados proveedores, las cuales pueden resumirse de la siguiente manera:

- Para que una IFC pueda contratar con terceros, debe observar Las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera (las "Disposiciones IFC"); y
- Para que una IFPE pueda contratar con terceros, debe observar las disposiciones aplicables a las instituciones de fondos de pago electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera (las "Disposiciones IFPE").

En general, las ITF deberán dar cumplimiento a lo siguiente para efecto de contratar con terceros que requieran de autorización: (i) contar con un padrón de prestadores de servicios (donde se incluirá a la Entidad contratante), (ii) realizar auditorías anuales para verificar el grado de cumplimiento a las obligaciones de la contraparte; (iii) verificar que los comisionistas informen a los clientes de la ITF que actúan a nombre y por cuenta de la ITF.

En cuanto a la responsabilidad derivada de las operaciones celebradas por terceros y/o comisionistas, las ITF responderán en todo momento por el servicio que sus comisionistas proporcionen a los clientes, aun cuando la realización de las operaciones correspondientes se lleve a cabo en términos distintos a los pactados, así como por el incumplimiento a las disposiciones en que incurran dichos comisionistas.

24.4.1. Contratación con las IFPE[126]

De acuerdo con las Disposiciones IFPE, estas instituciones únicamente deberán presentar ante Banxico y a la CNBV un aviso previo a la contratación cuando contrate la prestación de servicios de un tercero cuando el tercero:

- Funja como proveedor secundario o de respaldo para complementar la operación de un proveedor primario o garantizar la continuidad de negocio en caso de que el proveedor primario no esté en condiciones de prestar el servicio, o;
- Corresponda a una entidad financiera legalmente facultada y sujeta a regulación en el ámbito federal, en materia financiera. Dicho aviso se debe de presentar con 20 días hábiles de antelación a la contratación del tercero.

Asimismo, las Disposiciones IFPE prevén que las IFPE podrán celebrar contratos de comisión mercantil con terceros que actúen frente al público en general a nombre y por cuenta suya únicamente para:

- Realizar retiros de efectivo por el cliente de la IFPE;
- Recibir recursos para abono en cuentas propias o de terceros;
- Consultas de saldos y movimientos de cuentas;
- Puesta en circulación de instrumentos para la disposición de los fondos de pago;
- Abrir cuentas de fondos de pago electrónico; y
- Transferencias con cargo a cuentas de fondos de pago electrónico, incluyendo pagos de servicios.

En caso de que las Entidades busquen celebrar un contrato de comisión con las IFPE para llevar a cabo las actividades mencionadas, deberán presentar una solicitud de autorización ante Banxico y la CNBV que contenga, al menos:

[126] Disposiciones IFPE.

- Plan general del funcionamiento, el cual debe tener una descripción detallada y diagrama de flujo de los procesos de cada operación que se va a contratar, así como mecanismos de vigilancia del desempeño del comisionista.
- Proyecto de contrato con el comisionista, en el que deberá señalarse los datos generales de la alianza como la fecha de su celebración, los derechos y obligaciones de las partes, las operaciones que realizará el comisionista, los límites de operaciones, entre otros.
- El proyecto de contrato deberá contener una constancia de aceptación expresa en la cual el comisionista se obligue a lo siguiente:

(i) Entregar, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate.

(ii) Informar a la ITF de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar las operaciones objeto de la contratación.

(iii) Guardar confidencialidad respecto de la información que haya sido recibida.

(iv) Manifestar la aceptación de la responsabilidad directa por el uso indebido de la información de la ITF y, en su caso, pagar las indemnizaciones por daños y perjuicios causados por cualquier incumplimiento a lo señalado en el inciso anterior.

(v) Cumplir con los términos, condiciones y procesos para garantizar a la ITF la transferencia, la devolución y eliminación segura de la información sujeta a la comisión contratada cuando el contrato se dé por terminado.

(vi) Prevenir el uso indebido de los factores de autenticación de los clientes y empleados que operen el servicio contratado.

(vii) Capacitar al personal respecto del proceso para realizar operaciones.

Además de lo anterior, las ITF para la contratación de servicios con terceros que sean objeto de autorización, deben de dar cumplimiento a lo siguiente:

- Realizar, al menos anualmente, auditorías internas o externas sobre el servicio contratado o contar con evidencia de que el tercero contratado las lleva a cabo.
- Actualizar la descripción o documentación respectiva cuando existan modificaciones que se consideren que tienen un impacto relevante en cuanto al servicio.

24.4.2. Contratación con las IFC[127]

Por otro lado, las Disposiciones IFC no prevén la excepción para que las IFC puedan contratar con instituciones financieras únicamente dando aviso a la CNBV, sino que la contratación de terceros por parte de estas instituciones requiere la autorización de dicha Comisión cuando el tercero:

- Preste servicios que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de información personal o información sensible de los clientes, siempre y cuando el tercero tenga privilegios de acceso para conocer dicha información o la información de configuración de seguridad, o bien, a la administración de control de accesos;
- Realice procesos en el extranjero relacionados con la contabilidad o tesorería,
- Funja como el proveedor primario de aquellos servicios cuya interrupción, parcial o permanente, imposibilite a la IFPE la emisión, administración, redención o transmisión de fondos de pago electrónico.

En caso de que las Entidades busquen aliarse con IFC y se encuentren en cualquiera de los supuestos mencionados anteriormente, estarán obligados a proporcionarle a la IFC la siguiente información para que esta, a su vez, se la entregue a la CNBV como parte del expediente técnico de la solicitud de autorización para contratar con la Entidad de que se trate:

[127] Disposiciones IFC.

- Plan general del funcionamiento, que debe contener una descripción detallada y un diagrama de flujo de los procesos de cada operación que se va a contratar, así como mecanismos de vigilancia del desempeño del comisionista.
- Proyecto de contrato con el comisionista, en el que deberá señalarse los datos generales de la alianza y la fecha de su celebración, los derechos y obligaciones de las partes, las operaciones que realizará el comisionista, los límites de operaciones, entre otros.
- El proyecto de contrato deberá contener una constancia de aceptación expresa en la cual el comisionista se obligue a lo siguiente:

  (i) Entregar, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate.

  (ii) Informar a la ITF de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar las operaciones objeto de la contratación.

  (iii) Guardar confidencialidad respecto de la información que haya sido recibida.

  (iv) Reportar cualquier subcontratación;

  (v) Cumplir con los términos, condiciones y procesos para que el tercero garantice la transferencia, devolución y eliminación de la información sujeta al servicio contratado cuando deje de prestarlo;

  (vi) Mantener registros de auditoría íntegros;

  (vii) Contar con controles de acceso a la información de acuerdo con los nivele de acceso y perfiles determinados por la IFC;

  (viii) Permitir que la IFC realice revisiones de seguridad.

- Documentación relativa a la Infraestructura Tecnológica:

  (i) Descripción de los enlaces de comunicación utilizados por la IFC.

  (ii) Un diagrama de telecomunicaciones donde se muestre la comunicación existente entre cada uno de los participantes en la prestación del servicio.

(iii) La dirección completa del lugar donde se realizarán cada uno de los servicios.

(iv) El esquema de interrelación de aplicaciones o sistemas objeto de la contratación.

(v) Los mecanismos de continuidad del servicio contratado.

- Evidencia que permita verificar que los terceros tengan e implementen políticas de protección de datos personales y confidencialidad de la información que permitan a la IFC cumplir con las disposiciones legales que la rigen en la materia.

24.5 Seleccionar un Aliado.

La selección de un aliado, desde el punto de vista legal, debe atender en todo momento a las posibilidades y limitaciones de la regulación aplicable a las Entidades y, en su caso, a los aliados. En ese sentido, sugerimos, antes de celebrar una alianza de cualquier tercero, practicar un *due diligence* legal que permita a las Entidades identificar el grado de cumplimiento (*compliance*) de sus obligaciones, para lo cual proponemos los siguientes niveles de cumplimiento:

- Grado de cumplimiento de sus obligaciones corporativas básicas.
- Grado de cumplimiento de sus obligaciones fiscales.
- Grado de cumplimiento de sus obligaciones regulatorias.

Cabe mencionar que esta lista es enunciativa; en realidad, las Entidades deben solicitar a su contraparte cualquier información y documentación que estimen relevante para fines del acto en específico a través del cual se documente la alianza estratégica que se celebre.

En caso de que se detecte alguna irregularidad o inconsistencia entre las afirmaciones de la contraparte y la documentación presentada, o bien, cuando el potencial aliado se rehúse a compartir la información que la Entidad requiere, la Entidad debe considerarlo como una posible contingencia futura. El objetivo de esta evaluación es detectar y evitar, en la

medida de lo posible, potenciales contingencias legales futuras que pudieran no solamente presentar un riesgo legal para las Entidades, sino también un riesgo financiero, reputacional o inclusive regulatoria frente a la CNBV.

24.6 Contratar otra Entidad Financiera.

La contratación con entidades financieras, en términos generales, tiene implicaciones similares para las Entidades desde el punto de vista regulatorio. La diferencia radicaría principalmente en la regulación para la contratación de terceros por parte de la otra entidad financiera. Adicionalmente, debe considerarse que cada entidad financiera tiene un giro comercial específico y actividades permitidas por la regulación aplicable, por lo que los tipos de alianzas que pueden formarse con otras entidades financieras no necesariamente serán las mismas que las que se pueden realizar, por ejemplo, con las ITF. En todo caso hay que tener en mente varios aspectos de negocios que tienen una consecuencia contractual y regulatoria importante:

- Establecer si la alianza consiste únicamente en creación de oportunidades de negocio mutua (en cuyo caso podría ser un esquema similar al expuesto en la Sección 23 (Creación de Oportunidades de Negocio en Línea).
- En el caso de servicios "complementarios" es necesario tener claridad sobre los esquemas y los procesos que llevará a cabo cada Entidad y el límite de participación y responsabilidad de cada una en la implementación.
- En el supuesto de contratos de tecnología o de administración de procesos operativos o administrativos, considerar los aspectos expuestos en las Secciones 15 y 16 para el caso de Proveedores Relevantes.
- Los temas que siempre tendrán un impacto regulatorio en estos esquemas son (i) los canales de ofrecimiento o captación de clientes, (ii) la administración y los procesos internos (sobre todo cuando involucren clientes), (iii) el flujo y tipo de información a compartirse por las Entidades y (iv) las restricciones y límites legales para efecto de realizar ofertas o procesos conjuntos.

24.7 Acercamiento Inicial.

Al igual que se ha mencionado en secciones anteriores de esta Guía Legal, antes de acudir ante la CNBV para plantearle un proyecto de alianza estratégica, sugerimos que las Entidades, de manera interna, hayan desarrollado algunos aspectos generales del Proyecto, a modo de comunicarle a la CNBV toda la información que necesita para determinar la viabilidad del proyecto. Al respecto, es necesario lo siguiente:

- Proporcionar información suficiente para que la CNBV puede expresar alguna opinión sobre la propuesta.
- Plantear dudas y comentarios concretos a la CNBV sobre la viabilidad del proyecto, incluyendo aspectos regulatorios y legales de la contraparte y cualesquiera otros que surjan durante el desarrollo de la propuesta.
- Preparar una presentación y documentación preliminar que permita a la CNBV entender de manera clara la forma, el alcance y la naturaleza de la alianza. La presentación debe ser congruente con lo que indiquen las Entidades por lo que sugerimos llevar a cabo sesiones de trabajo conjuntas.
- Atender cualesquiera comentarios u observaciones que la CNBV pudiera tener tan pronto como sea posible.

24.8 Diagrama y Plan de Trabajo.

Proponemos, en forma genérica, el siguiente plan de trabajo para comenzar a abordar las alianzas estratégicas con otras entidades:

- Realizar un análisis sobre la necesidad de celebrar una alianza con otra entidad y establecer los objetivos principales que se buscan al celebrar dicha alianza, atendiendo a lo siguiente:

  (i) Identificar oportunidades, necesidades o deficiencias de la Entidad. Las alianzas estratégicas deben generarse cuando una Entidad estima que, de llevarla a cabo, se convertiría en un negocio más rentable, o bien, que la

alianza ayudaría a la Entidad a subsanar necesidades o deficiencias que se hayan identificado a través de un análisis del negocio.

(ii) Las alianzas estratégicas deben acercar a las Entidades a sus objetivos a corto, mediano y largo plazo. Para ello, se deben considerar los costos asociados con la alianza, los riesgos y las potenciales contingencias relacionadas con la alianza, las capacidades tecnológicas y de recursos de ambas partes y los temas regulatorios y operativos. Al respecto, proponemos un análisis a partir de un "árbol de decisiones", que permita a cada equipo involucrado identificar las ventajas y desventajas potenciales de la alianza.

(iii) Identificar el tipo de alianza estratégica desde el punto de vista legal y operativo que mejor se ajusta a los objetivos principales que se persiguen.

(iv) Acordar el alcance y la duración de la alianza.

(v) Elaborar esquemas y diagramas de flujo en los cuales se describa a detalle el funcionamiento de la alianza. Estos deben contener el detalle de la Infraestructura Tecnológica que se está poniendo a disposición de la otra parte, la jerarquía y los directivos relevantes que participarán en la alianza y el flujo de los recursos, entre otras cosas.

(vi) Identificar de forma específica las capacidades que las Entidades adquieren al celebrar la alianza y los nuevos productos y/o servicios que pueden implementarse a través de ellas o si, por el contrario, las capacidades únicamente modifican la manera en la que la Entidad ofrece los productos o presta los servicios.

(vii) Analizar si será necesario solicitar la autorización de la CNBV a partir del tipo de alianza que se haya elegido, o bien, si se trata de un área no regulada que requiera el apoyo de un asesor externo para determinar el alcance del proyecto desde el punto de vista regulatorio.

(viii) Determinar las entidades que potencialmente pueden apoyar a las Entidades para lograr los objetivos planteados y los resultados que se esperan del aliado. Para ello, es importante que las Entidades determinen: (i) las actividades en concreto que realizará el aliado dentro y fuera de la operación de la Entidad; (ii) el tipo de entidad que se requiere para lograr dichos objetivos; (iii) el giro del negocio que debe tener el aliado; y (iv) las capacidades operativas, humanas y tecnológicas mínimas que el aliado requiere para poder formar parte del proyecto.

(ix) Elaborar una lista de términos y condiciones que las Entidades no están dispuestas a negociar, o bien, dada la regulación aplicable, no les es posible negociar.

- Ejecutar un diagnóstico sobre las capacidades y deficiencias tecnológicas actuales para determinar cuáles se requiere desarrollar, contratar o adquirir para implementar la alianza estratégica.

- Nombramiento interno de partes responsables que estarán encargadas de la elaboración del plan de trabajo correspondiente y de las negociaciones con la contraparte (las "Partes Responsables").

- Identificar las necesidades financieras, contables y operativas del proyecto.

- Identificar las necesidades legales para la implementación del proyecto, tomando en cuenta lo siguiente:

(i) Requisitos de contratación y operación, dependiendo del tipo de alianza estratégica que se haya elegido.

(ii) Limitaciones regulatorias y legales.

(iii) Identificación de requerimientos y limitaciones en materia PLD/FT.

(iv) Identificación de necesidades y regulación aplicable en materia de protección de datos personales (ver Sección 9 Datos Personales y Secreto Financiero).

(v) Identificación de la estructura contractual y legal de la operación: convenios de confidencialidad, versión preliminar de los contratos, versiones finales de los contratos, según lo requiera la alianza.

(vi) Borrador de los contratos de adhesión que implementarán los nuevos productos y servicios, en su caso, o modificación de los existentes para reflejar la alianza.

(vii) Evaluación sobre la utilidad de la Firma Electrónica (ver Sección 12 Implementación de Firma Electrónica).

- Sesiones de trabajo preliminares entre las áreas responsables y las Partes Responsables donde intervengan, al menos:

(i) Los directivos relevantes de todas las áreas.

(ii) El área de riesgos.

(iii) El Oficial de Cumplimiento.

(iv) El área legal.

(v) El área financiera y contable.

(vi) El asesor externo, en su caso.

Las sesiones deben estar guiadas por diagramas explicativos que elaboraron, en su momento, las Partes Responsables para que todas las áreas identifiquen claramente las necesidades y riesgos del proyecto.

- Presentación del proyecto al Consejo de Administración por parte del Director General para su aprobación, discusión y modificación. Es recomendable que el Consejo de Administración o, en su caso, el Director General nombre a un Administrador del Proyecto que tenga facultades suficientes para verificar el cumplimiento de las metas del proyecto.
- Identificar a los potenciales aliados que cumplan con los requerimientos mínimos que las Entidades han determinado para la implementación del proyecto y buscar

la forma más efectiva de plantearles el Proyecto. La selección del aliado depende en una gran medida de los siguientes elementos:

(i) Visión de las partes. Que las partes compartan objetivos y visión a corto, mediano y largo plazo para continuar colaborando.

(ii) Cultura de las empresas. Mientras que las empresas tecnológicas tienden a tener acercamientos más acelerados, empresas acostumbradas a operar de forma tradicional tienen como prioridad otros objetivos, como la precisión y el cuidado al detalle.

(iii) Lograr que ambas partes compartan el mismo grado de interés y responsabilidad dentro de la alianza.

- Presentación preliminar de la alianza ante la CNBV mediante el uso de materiales informativos que identifiquen las responsabilidades de cada participante.

- Una vez que la CNBV emita comentarios al respecto, se debe elaborar un plan de trabajo detallado junto con un cronograma que establezca fechas límite de entrega e hitos. Este esquema de trabajo permite organizar a los diversos equipos de trabajo que participarán en la alianza tanto interna como externamente y que todas las partes involucradas se rindan cuentas entre ellas.

- El cierre y la entrega de este tipo de Proyectos deben estar coordinados y aprobados por todas las áreas y no ocurre sino hasta que CNBV ha dado comentarios al Plan Estratégico de Negocios, al formato de contrato de comisión y a las políticas que deben modificarse para efecto de estar en cumplimiento con los temas operativos, control interno, PLD/FT, productos o servicios (captación, crédito, etc.) y transparencia y ordenamiento de los servicios financieros. Esta es una etapa “informal” del proceso donde, si bien no existe una calendarización definida, es posible que varias reuniones e intercambio de información existan previo a la realización del aviso o solicitud de autorización formales.

- La finalización típicamente coincide con el visto bueno o la autorización por parte de la CNBV, la presentación del cierre frente al Consejo de Administración de las Entidades y la aprobación de las modificaciones a los Manuales existentes y a las

políticas requeridas para la contratación con terceros (ver Sección 15 Contratación de Proveedores y Comisionistas).

Es importante mencionar que las particularidades de cada Entidad y alianza dificultan generar un plan de trabajo que sea aplicable en todos los casos; sin embargo, el propuesto puede servir como un punto de partida para que cada Entidad pueda generar un plan de trabajo que sea congruente con su alianza.

Plan de trabajo para la implementación de alianzas estratégicas

Gráfica 30. Plan de trabajo para la implementación de alianzas estratégicas. Fuente: Vite Abogados

24.9. Temas prácticos y recomendaciones

El 22 de junio del 2020, Grupo Financiero Banorte, S.A. de C.V. (clave "GFNORTE") celebró con la empresa colombiana Rappi una alianza estratégica mediante la cual ambas empresas serán accionistas al 50% de una nueva entidad dedicada al ofrecimiento de servicios financieros digitales[128]. Esta alianza tiene el objetivo, desde el punto de vista de GFNORTE, de generar penetración el ecosistema financiero digital a través de la

[128] Alianza GFNORTE – Rappi. (Internet) Consultado en: https://www.bmv.com.mx/docs-pub/visor/visorXbrl.html?docins=../eventemi/eventemi_1020680_1.zip#/visorXbrl

penetración que Rappi ha generado en el mercado digital mexicano[129]. Si bien el giro del negocio principal de Rappi no es ofrecer servicios financieros, a través de desarrollo de productos esta empresa comenzó a ofrecer servicios como un saldo virtual a través de la aplicación y el "Rappi Cash"[130], mediante el cual los usuarios pueden solicitar dinero en efectivo "a domicilio". Aproximadamente seis meses después de la celebración de esta alianza estratégica, la sociedad producto de esta alianza estratégica, Tarjetas del Futuro, S.A.P.I. de C.V., sacó al mercado una tarjeta de crédito. Este ejemplo ilustra el alcance que puede tener una alianza estratégica y la diversidad de entidades que pueden celebrarlas.

El ecosistema Fintech en México merece algunas consideraciones prácticas adicionales. De acuerdo con información del periódico El Economista en línea, al 21 de enero de 2020 la CNBV estaba en proceso de revisar y, en su caso, autorizar 93 empresas que buscan operar bajo las figuras reguladas en la Ley Fintech. De esas 93, únicamente 69 se encuentran operando bajo la Disposición Octava Transitoria de la Ley Fintech; es decir, solamente 69 actualmente pueden estar operando mientras la CNBV no emita una resolución respecto a su autorización[131]. Al momento de buscar celebrar una alianza con una ITF, es de especial importancia verificar si su trámite se encuentra en proceso y se encuentra operando al amparo de la Disposición Octava Transitoria de la Ley Fintech o si, por otro lado, ya es una ITF autorizada por la CNBV.

En relación con lo anterior, el 4 de diciembre de 2020 la CNBV emitió un comunicado[132] en el cual se indica al público en general que en México solamente están autorizadas para ofrecer, promover y prestar productos y servicios financieros las entidades financieras que cuentan con autorización, registro o concesión del Gobierno Federal, o bien, las ITF que se encuentren operando al amparo de la Disposición Octava Transitoria. Si bien este comunicado no es aplicable para las Entidades, sí lo es para las potenciales alianzas estratégicas que estas estén considerando con entidades que, o se ostentan como entidades financieras sin serlo, o están en proceso de obtener la autorización correspondiente y se encuentran llevando a cabo actividades para las que aún no están

[129] Para mayor información respecto a la alianza estratégica entre GFNORTE y Rappi, consultar: https://www.bmv.com.mx/docs-pub/visor/visorXbrl.html?docins=../eventemi/eventemi_1020680_1.zip#/visorXbrl

[130] Para más información, consultar la página oficial de Rappi: https://blog.soyrappi.com/rappicashcl/

[131] Gutiérrez, Fernando (2021) CNBV analiza 93 solicitudes para operar bajo la le Fintech. El Economista (en línea). Consultado en: https://www.eleconomista.com.mx/sectorfinanciero/CNBV-analiza-93-solicitudes-para-operar-bajo-la-ley-fintech-20210121-0030.html

[132] Para consultar el comunicado de la CNBV respecto al *Fintech as a Service*, visitar la siguiente dirección web: https://www.gob.mx/cms/uploads/attachment/file/597033/CNBV_Aviso_sobre_entidades_autorizadas.p

autorizadas. Debe tomarse en cuenta este comunicado al evaluar cualquier potencial alianza estratégica con una ITF y, cuando se determine que el proyecto se llevará a cabo, las Entidades deben ser especialmente cuidadosas con los servicios que ofrecerá cada una de las partes. El denominado *Fintech as a Service*, es decir, que las ITF licencien sus interfaces de programación de aplicaciones (o API, por sus siglas en inglés), de acuerdo con el comunicado es una figura que merece especial cuidado y cautela. En casos como este siempre debe consultarse a la CNBV sobre lo que es aceptable dentro de una alianza estratégica con otras entidades financieras y lo que no lo es.

La Ley Fintech, como hemos mencionado anteriormente, regula exclusivamente las figuras señaladas en la Sección 24.3 (Actividades de Instituciones de Tecnología Financiera); sin embargo, el denominado "ecosistema Fintech" en México comprende un conjunto mucho más amplio de productos y servicios que se ofrecen a través de medios tecnológicos y que no necesariamente se encuentran regulados por la legislación financiera mexicana. En ese sentido, es importante realizar el *due diligence* legal que permita a las Entidades identificar si se trata de una ITF regulada por la CNBV o de una sociedad que se ostenta como "Fintech", sin que sus actividades estén reguladas por la legislación financiera mexicana. Las implicaciones que esto tiene pueden ser altamente trascendentes para fines de la autorización de los contratos por parte de la CNBV, así como para las actividades que efectivamente se pueden llevar a cabo a través de las alianzas.

A modo de ejemplo, proponemos recabar la siguiente información y documentación al realizar el *due diligence* para identificar el grado de cumplimiento de los potenciales aliados:

- Solicitar el acta constitutiva de la empresa junto con su registro en el Registro Público de Comercio, los poderes del apoderado, los libros corporativos debidamente protocolizados, registros de marca, certificados de propiedad, etc. Esto permite a las Entidades:

  (i) Identificar el tipo de entidad de que se trata; es decir, identificar si es una institución financiera del sistema financiero mexicana, una entidad comercial mexicana, una institución financiera extranjera, o bien, una entidad comercial extranjera.

(ii) Verificar si su objeto social le permite celebrar los actos que documenten las alianzas estratégicas, si su apoderado legal efectivamente cuenta con los poderes para ello y si la regulación que le es propia le permite celebrar dichos actos.

(iii) Que sean capaces de evidenciar los derechos sobre los insumos que dicen tener para celebrar el contrato. A modo de ejemplo, si se va a celebrar un contrato de licencia para una plataforma digital, que el aliado efectivamente cuente con el certificado del Instituto Nacional de Derechos de Autor que acredite la propiedad.

- Solicitar una opinión positiva de cumplimiento emitidas por el Servicio de Administración Tributaria.

- En su caso, que las entidades financieras sean capaces de proporcionar la información y documentación requerida por la CNBV para contratar con las Entidades.

En el caso de que se identifique que el potencial aliado es una institución financiera, se puede solicitar también evidencia del cumplimiento de sus obligaciones regulatorias y en materia de prevención de lavado de dinero, por ejemplo, en la medida permitida por la regulación. Es relevante considerar que las instituciones financieras, al estar reguladas por las autoridades mexicanas, tiene información registrada ante estas, por lo que elementos como la existencia de su autorización para operar como institución financiera, sus contratos de adhesión y algunos otros datos pueden consultarse fácilmente a través de las páginas de dichas autoridades[133].

Por su parte, en el caso de las entidades comerciales, las Entidades podrían solicitarles, a modo de ejemplo, un aviso de privacidad actualizado, sus términos y condiciones de servicio, los contratos que celebran con sus clientes, así como una opinión favorable por parte del Servicio de Administración Tributaria en relación con sus obligaciones fiscales, entre otra información y documentación.

[133] Para mayor información respecto a las entidades supervisadas por la CNBV sugerimos consultar el Padrón de Entidades Supervisadas, disponible en: https://www.cnbv.gob.mx/Paginas/PADR%C3%93N-DE-ENTIDADES-SUPERVISADAS.aspx

SECCIÓN 25.- PROYECTOS PARA EL MANEJO Y CONSERVACIÓN DIGITAL DE LA INFORMACIÓN.

25.1 Grabación y Microfilmación.

Un "documento" es aquel objeto en que consta un acto o hecho realizado por una institución o una persona, ya sea física o jurídica, pública o privada. A través de los documentos se puede guardar y acceder a información relacionada con convenios, políticas, manuales, procesos y muchas otras cuestiones relevantes, en este caso, para las Entidades. Podemos decir que los documentos se distinguen de los registros en que los primeros especifican "lo que se hará" y los segundos señalan "lo que ya se hizo"[134]. Los registros de documentos prueban la actividad de una Entidad o decisiones de negocio que ocurrieron y que deben ser conservadas para justificar y explicar alguna situación actual o futura.

Una de las actividades fundamentales que se realizan en los registros, es la preservación continua de la información contenida en los documentos, misma que garantizará que al paso del tiempo no se pierdan.

El manejo y conservación adecuada de la información es relevante, no solamente para efectos legales y de contabilidad, sino para un buen funcionamiento de una Entidad, redundando en las siguiente ventajas:

- Apoyan de manera efectiva y eficiente la organización de la Entidad, proveyendo a los Socios o Clientes, administradores, empleados, clientes y proveedores acceso a documentos que se encuentren al día.
- Facilitan la realización de tareas diarias en la entidad a través de una comunicación efectiva entre las distintas áreas de la Entidad y, por lo tanto, mejoran el cumplimiento de procesos y políticas.
- Otorgan seguridad jurídica a los clientes y proveedores de la entidad.

[134] KASSA, Dawit. (2015) Document control. Lifecycle and the governance challenge.

- Ayudan a materializar conceptos, ideas, estudios, políticas y guías para que se puedan comunicar a otras personas.
- Mejoran la confianza que tienen los clientes en la entidad.
- Reducen tiempos al momento de revisar, archivar y registrar documentos.
- Mejoran la seguridad de los documentos para evitar acceso no autorizado a los mismos y lograr asegurar la confidencialidad de los mismos.

Es igual de importante la definición de responsabilidades en el manejo de documentos. Entre más personas estén envueltas en el manejo de un documento, el cuidado del mismo se vuelve más complejo y puede traer como consecuencia el daño o incluso pérdida del mismo. Debido a esto es recomendable que siempre exista un responsable del documento, quién se asegurará de registrar el proceso por el que pasa el documento y las áreas que han sido encargadas del mismo.

Para un correcto manejo y conservación de los documentos, consideramos oportuno explicar el ciclo de vida de un documento, ya que atendiendo al "momento de vida del documento" se tendrán que tomar distintas precauciones para el manejo del mismo. El ciclo de vida de un documento es el siguiente[135]:

- *Creación.* Los documentos son creados una vez que se introducen caracteres de identificación y de registro, tales como nombre, números de identificación, fecha, etc.

Para una Entidad, se entiende creado un documento en dos posibles momentos:

(a) el documento se crea de manera interna y envía para revisión y aprobación.
(b) el documento es recibido de una fuente externa para revisión y aprobación.

Para un buen manejo de documentos, recomendamos que la Entidad tenga formatos preestablecidos en los que se solicite a los creadores de los documentos que envíen el documento junto con el formato. Un ejemplo de formato sería el siguiente:

[135] *Op. Cit.* KASSA.

No. Revisión	Fecha creación	Objetivo	Autor	Revisor	Responsable autorización

De igual forma se recomienda que los nombres sean lo más descriptivos posibles, evitando el uso de nombres imprecisos, y de preferencia que los nombres sea únicos y de fácil búsqueda.

- *2. Revisión y aprobación. Los documentos una vez que son creados, requieren revisión y actualización por una serie de distintas razones.*

Los cambios que se realizan a los documentos deben guardarse y necesitan ser aprobados por el supervisor, con el propósito de que el documento final contenga un resumen de todos los cambios que se le realizaron sea aprobado por distintas personas, previniendo errores.

Se recomienda a las entidades que todos los documentos tengan por lo menos dos personas distintas que los revisen.

- *3. Uso.* Una vez que el responsable de autorizar los cambios al documento lo aprueba, el documento será usado en distintas ocasiones para consulta. Las entidades deben determinar a un responsable del documento para tener control sobre quién lo tiene y dónde se encuentra.

- *4. Conservación y/o destrucción.* Cuando el documento deja de ser objeto de uso continuo, deben archivarse de tal forma que sea fácil de encontrar en caso de que el documento sea requerido nuevamente. Cuando el documento se vuelve obsoleto y no existe obligación jurídica de conservarlo, el siguiente paso en el ciclo de vida del documento es la destrucción, para lo cual se tienen que seguir reglas especiales.

Es importante considerar que tanto el archivo del documento como la destrucción debe ser debidamente documentados y aprobados.

Por la naturaleza de los documentos y al estar frecuentemente expuestos a factores y mecanismos de alteración, los documentos sufren constantes cambios en su composición

física, afectando su funcionalidad y poniendo en peligro la información contenida en los mismos. Por ello, es indispensable el cuidado preventivo y adecuado de los documentos que se encuentren en el archivo.

Cuando hablamos de información digital, debemos considerar que esta es intrínsecamente más fácil de alterar que los documentos físicos. Los soportes de almacenamiento digital tienen menos esperanza de vida y requieren de la existencia de unas tecnologías para acceder a los mismos que cambian a una velocidad incluso mayor que los propios formatos. Además, se deterioran más fácilmente haciendo que se pierdan los contenidos.

A causa de la rapidez de los cambios tecnológicos, el periodo en que se deben considerar los problemas de preservación y conservación de los documentos digitales se acorta considerablemente. El tiempo transcurrido entre la producción de los documentos y la necesidad de definir estrategias de preservación de los mismos es mucho más corto en el entorno electrónico que en el impreso. Por lo tanto, se plantea la necesidad de definir nuevas guías de buenas prácticas que satisfagan las necesidades y sean útiles para todos los grupos implicados en el proceso de generación y distribución de documentos electrónicos.

La UNESCO ha reconocido la importancia del problema de la conservación de los documentos electrónicos y por ello ha redactado la Carta para la preservación del patrimonio digital[136] . En el artículo 3 de la misma se reconoce el peligro de pérdida al que están sometidos estos materiales y se afirma: "El patrimonio digital del mundo corre el peligro de perderse para la posteridad. Contribuyen a ello, entre otros factores, la rápida obsolescencia de los equipos y programas informáticos que le dan vida, las incertidumbres existentes en torno a los recursos, la responsabilidad y los métodos para su mantenimiento y conservación y la falta de legislación que ampare estos procesos". Si bien el problema de la preservación digital es arduo y complicado, también es cierto que el proceso de preservación y archivo se hace de forma más eficiente cuando se pone atención en las cuestiones de consistencia, formatos, normalización y descripción bibliográfica en los primeros pasos del ciclo de vida de la información. Por ello, se enfatiza la importancia de considerar buenas prácticas de conservación en todos los estados del ciclo de vida de

[136] UNESCO, Carta para la preservación del patrimonio digital, 2003. (en línea). http://www.r020.com.ar/enlaces/ir.php?ir_id=665 (Consulta: 26 de agosto de 2004).

gestión de la información: creación, adquisición, catalogación, almacenamiento, preservación y acceso.

En relación con lo expuesto anteriormente, debido a la importancia que es el manejo y la conservación de los documentos, no solo físicos si no de forma digital, la legislación lo regula de forma específica y de manera técnica, a través de las leyes que rigen el funcionamiento de las Entidades[137].

Existen conceptos importantes relacionados con el manejo de documentos por parte de las Entidades:

- Grabación, conforme a la normativa es aquel acto mediante el cual un libro, registro o documento original, es transformado en una imagen en formato digital en medio óptico o magnético, utilizando equipos y programas de cómputo diseñados para tal efecto.
- Microfilmación, conforme a la misma normatividad, es definido como el acto mediante el cual un libro, registro o documento original, es filmado en una película.

Las Entidades, al conservar todos aquellos libros, registros y documentos en general que obren en su poder, relativos a sus operaciones activas, pasivas, de servicios y demás documentos relacionados con su contabilidad, podrán utilizar la Microfilmación, Grabación, o bien, cualquier otro medio que para tal efecto les autorice la CNBV para dichos efectos.

El proceso de Microfilmación deberá prever la generación de un índice de los documentos objeto de dichos procesos, en donde se indique, por lo menos, (i) el nombre de este; (ii) el lugar de almacenamiento; (iii) el tamaño; (iv) la fecha y la hora de creación; (v) el número de imágenes y (vi) una referencia descriptiva de su contenido, así como la clave del medio en donde se microfilmó la documentación. Tratándose de los procesos de Grabación, se deberá generar un archivo que contenga los datos antes señalados.

[137] Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo y Ley de Ahorro y Crédito Popular.

En caso de que las Entidades usen mecanismos de Microfilmación y Grabación bastará con presentar el documento certificado por el funcionario responsable del área y por el Director General, en el cual se describan los procedimientos institucionales que se seguirán para la microfilmación o grabación, así como también una descripción del sistema establecido para el control de documentos microfilmados o grabados. En el supuesto en que se utilicen sistemas o medios para la conservación de libros, registros y documentos, distintos a la Microfilmación o Grabación es necesario presentar una solicitud de autorización para utilizar sistemas o medios distintos a la microfilmación o grabación.

Las disposiciones secundarias[138] aplicables a las Entidades contienen un instructivo técnico para microfilmación y destrucción de documentos, mismo que tiene que ser cumplido por las entidades y, en su caso, por el proveedor de este servicio.

Cabe destacar que todos los aspectos relacionados con los procesos de Microfilmación y destrucción de documentos deberán quedar a cargo y bajo la responsabilidad del o de los funcionarios que expresamente designe la Entidad. Si la Entidad cuenta con más de una oficina, es necesario la designación de un responsable por oficina en que se realicen dichas labores.

Las entidades que utilicen procedimientos de Microfilmación deberán establecer un sistema de control a través del cual puedan localizarse e identificarse con facilidad, en cualquier tiempo, los documentos Microfilmados.

25.2 Proveedores.

Cuando se busca a un proveedor para efecto de llevar a cabo procesos de grabación o microfilmación, se debe de considerar: (i) fiabilidad y la integridad de la información, a que la grabación de información en formatos digitales no se hace en un formato fijo y los datos se pueden reproducir, alterar o borrar fácilmente, (ii) la obsolescencia de los soportes digitales: que determina la necesidad de mantener el entorno informático original o renovarlo con cierta frecuencia, y (iii) la necesidad de que los usuarios sepan utilizar las tecnologías sucesivas (usabilidad). Se recomienda visitar las instalaciones del proveedor

[138] Artículos 240 a 254 de las Disposiciones Generales SOFIPO.

de servicios y asegurarse que estas tengan las capacidades de hardware y software para el trabajo, junto con el personal necesario para el alcance del trabajo.

Se debe buscar que el proveedor cubra el ciclo de vida completo de los documentos y ser aplicable en la Entidad. Tiene que ser aplicable también sobre todas las actividades diarias; por lo que los procedimientos deben ser documentados de forma clara y concisa, para ser puestos en práctica.

25.3 Tipo de Contrato.

El contrato que se celebre con el proveedor de servicios de microfilmación y grabación deberá establecer de manera expresa el cumplimiento de las políticas internas que tengan por objeto establecer los lineamientos y procedimientos relativos al manejo y, en su caso, destrucción de libros, registros, documentos y demás información relativa a su contabilidad, que hayan sido objeto de Microfilmación y Grabación.

Las políticas internas en esta materia deberán prever por lo menos lo establecido en las disposiciones secundarias aplicables a las Entidades, en las cuales se contempla lo siguiente:

- Garantizar el adecuado manejo y control de los documentos que contengan la información confidencial de los Socios;

- Cumplir, en todo momento, con las disposiciones aplicables en materia de secreto financiero;

- Evitar proporcionar a terceras personas, información que las entidades obtengan con motivo de la celebración de operaciones con sus Socios o Clientes, para la comercialización de productos o servicios por parte de dichas personas;

- Implementar mecanismos que aseguren que la información pueda ser proporcionada en tiempo y forma a las autoridades financieras competentes, cuando así se lo soliciten;

- Obtener copias de toda aquella información que hubiere sido objeto de Microfilmación o Grabación en cualquiera de los sistemas o medios que al efecto utilicen, a fin de que pueda ser utilizada ante la eventual pérdida de los negativos originales de cámara o, en su caso, de la primera copia que se hubiere obtenido de los discos ópticos o magnéticos.

Las políticas internas deben ser aprobadas por el Consejo de Administración de las Entidades, por lo tanto, recomendamos que los contratos con los proveedores de estos servicios de igual manera sean aprobados por el Consejo de Administración a fin de garantizar el cumplimiento de las mismas. De igual manera, se recomienda que en el contrato de prestación de estos servicios se agregue el cumplimiento de los anexos técnicos.

Dependiendo de la amplitud de los servicios que presente un proveedor para el manejo del ciclo de documentación, el mismo podría considerarse como un Proveedor Relevante en atención a que: (i) el manejo de información podría considerarse como un aspectos operativo o administrativo esencial para el funcionamiento de la Entidad, y (ii) existe (posiblemente) acceso a información que pertenece a los Socios o clientes o a transacciones llevadas a cabo por ellos. Sin embargo, el análisis debe realizarse caso por caso pues existen esquemas de contratación que pueden no requerir de manejo de dichos aspectos de la documentación y que podrían configurarse como un servicio profesional dentro de los Servicios Excluidos.

25.4 Diagrama y Plan de Trabajo.

Para digitalizar los documentos de manera exitosa es necesario llevar un control estricto del personal, los procesos y la tecnología de la Entidad. Un programa sólido permitirá a la Entidad facilitar el proceso de digitalización. Se recomienda tomar como base lo siguiente[139][140]:

[139] 10 steps to building an integrated Information management roadmap. (Internet) Consultado en: https://www.accesscorp.com/blog/10-steps-to-building-an-integrated-information-management-roadmap/

[140] 6 Tips for File Digitalization. (Internet) Consultado en: http://nimble.ca/6-Tips-for-File-Digitization

- Hacer un inventario de todos los libros, registros y documentos en general que obren en el poder de la Entidad, relativos a sus operaciones activas, pasivas, de servicios y demás documentos relacionados con su contabilidad.

- Designar a un responsable de la Entidad que será el encargado de: (i) realizar un cronograma para la digitalización de documentos; (ii) designar el personal encargado de realizar este proceso o en su caso, elegir al proveedor de estos servicios; y (iii) supervisar al personal o al proveedor elegido.

- Comparar los costos de digitalización de los archivos de manera interna con los costos de digitalización de un tercero. Es importante que la Entidad considere dentro de los costos: mano de obra, servicios públicos, espacio de oficina, equipo, mantenimiento, suministros y tiempo.

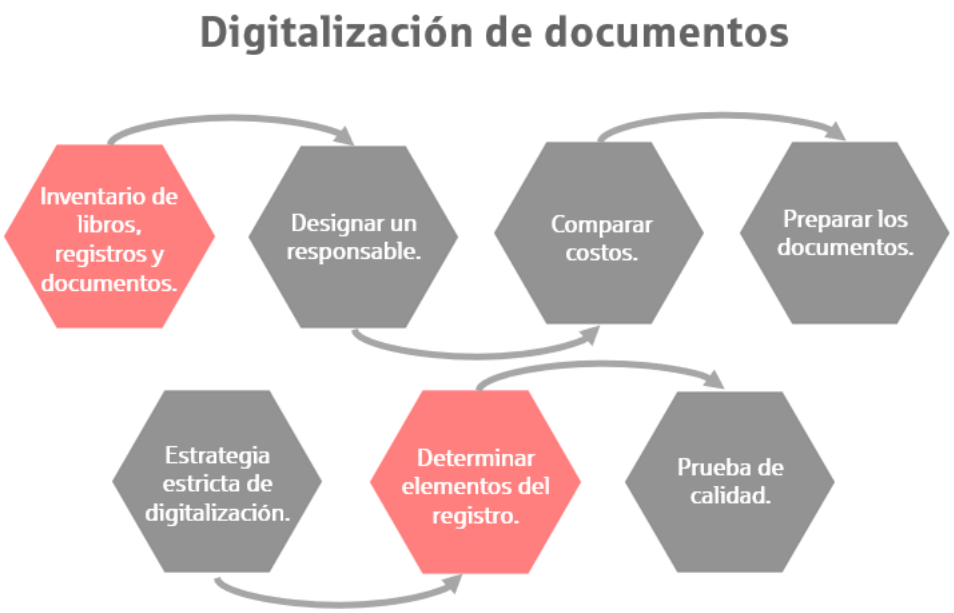
- Preparar los documentos antes de que estos se digitalicen. Esto consiste en quitar los clips, las grapas y las notas adhesivas, los documentos encuadernados deben separarse y todo debe estar organizado correctamente para optimizar la velocidad y la precisión. Este proceso se tiene que realizar de igual forma si se subcontrata a un tercero para llevar a cabo la digitalización y no se pierda información de los documentos.

- Determinar los elementos que tendrá registro de los documentos desde el principio del proceso de digitalización para que la transición a la tecnología sea lo más sencilla posible. Es decir, determinar si las carpetas llevarán el nombre del documento, tipo de documento, fecha de realización, área encargada, etc. Dicho registro tiene que ser claro, uniforme y completo, ya que este registro será la guía para buscar documentos.

- Llevar una estrategia estricta de digitalización, de tal manera que le permita a la Entidad escanear documentos nuevos a medida que ingresan, pero mantenga sus archivos en papel hasta que lleguen a la fecha de archivo o destrucción.

- Se debe realizar una prueba de calidad, es decir, antes de comprometerse por completo con una solución de digitalización de archivos interna o subcontratada,

es necesario asegurarse que la calidad y funcionalidad de los archivos es la adecuada, confirmado si el archivo es de fácil localización y la lectura del documento es clara.



Gráfica 31. Digitalización de documentos. Fuente: Vite Abogados

25.5 Aspectos Prácticos.

Desde el punto de vista organizativo, los documentos digitales presentan 3 funciones fundamentales:

- Operativa: los documentos digitales son la base de la operativa habitual de la entidad. Respecto a esta función, el uso de las tecnologías es intensivo para permitir un desarrollo más eficiente y eficaz del trabajo. Sin embargo, las condiciones especiales de los documentos digitales, rara vez se tienen en cuenta en esta fase.
- Responsabilidad organizativa: las entidades demuestran su adherencia al marco normativo y legislativo a través de documentos electrónicos, auténticos e íntegros que son almacenados en softwares que garantizan su almacenamiento seguro y posterior acceso.

- Archivo histórico: los documentos que se han considerado lo suficientemente valiosos o importantes para ser conservados en el largo plazo, documentan la historia corporativa de la entidad y deben ser mantenidos y migrados entre plataformas tecnológicas que aseguren su integridad y contexto.

Desde el punto de vista de la gestión documental electrónica, las estrategias de conservación deberían centrarse en las fases de diseño, uso y conservación de los documentos.

Para cumplir estas fases, las entidades suelen apoyarse en el uso de sistemas de gestión de documentos y registros electrónicos. Los softwares de gestión de documentos y registros electrónicos soportan la gestión de la información electrónica de 2 formas diferentes, pero complementarias:

- Gestión de documentos electrónicos: ayuda a las entidades a utilizar su información más eficientemente, contribuyendo con un mejor control de la creación, almacenamiento, revisión y distribución de los documentos entre los usuarios (también de correos electrónicos). Lo mismo ocurre con el control de flujo de archivos.
- Gestión de registros: ayuda a la entidad en la gestión eficaz de documentos, sobre todo en lo que respecta a la creación, recepción, mantenimiento, uso y disposición de información en forma de registros, que muestran las actividades y operaciones de la entidad.

SECCIÓN 26.- ACTIVOS VIRTUALES Y *BLOCKCHAIN.*

26.1 Diferencia entre Activos Virtuales y Blockchain.

En años recientes, la comunidad internacional ha volteado la mirada hacia los activos virtuales y la tecnología *blockchain* como una alternativa para ofrecer una gran cantidad de servicios y revolucionar la forma en que una gran cantidad de industrias operan. Quizá la industria más beneficiada es la industria de los servicios financieros. A continuación, hacemos algunas precisiones y consideraciones sobre estos dos conceptos.

Los activos virtuales, en primer lugar, surgieron como una propuesta de esquema alternativo para realizar pagos. Su objetivo, al menos en un inicio, fue evitar la intervención de un tercero en las transacciones tales como los bancos centrales y las instituciones financieras tradicionales. Aunque el valor del dinero *fiat* y los activos virtuales ambos están respaldados por la confianza, la diferencia principal entre ambos es en quién se deposita esa confianza: (i) el dinero *fiat*, o fiduciario, está respaldado por la confianza que tiene la gente en que el gobierno respalda su valor; (ii) los activos virtuales, por su parte, adquieren su valor cuando la gente deposita su confianza en una red descentralizada de usuarios que se encargan de verificar la transacción.

La legislación mexicana entiende los activos virtuales como:

> *"(i) una unidad de información que no representa la tenencia de algún activo subyacente a la par, y que es unívocamente identificable, incluso de manera fraccional, almacenada electrónicamente, (ii) cuyo control de emisión está definido mediante protocolos predeterminados y a los que se pueden suscribir terceros, (iii) y que cuenta con reglas que impiden que las réplicas de la unidad de información o sus fracciones se encuentren disponibles para ser transmitidas más de una vez en un mismo momento."*[141]

De acuerdo con la primera parte de la definición, la legislación mexicana considera que un activo virtual no debe representar la propiedad de un bien subyacente ni de un activo ajeno

[141] Banco de México. ¿Qué es un activo virtual? [Internet] Consultado en: Activos virtuales, definición, Banco de México (banxico.org.mx) el 25 de enero de 2021.

que respalde el valor del activo virtual. El valor está definido por la oferta y demanda, la cual, como se ha mencionado, depende de la confianza de los compradores en la tecnología que le da seguridad y operatividad al activo virtual. En este sentido, la definición no considera a activos que utilizan la misma tecnología que los activos virtuales más y que representan la tenencia a la par de algún activo subyacente como acciones, divisas o moneda de curso legal. A modo de ejemplo, activos virtuales como el *True USD* (que imita el valor del Dólar Estadounidense), el *CannDollar* (que está respaldada por plata) y *Tether* (que se encuentra respaldada por diversos activos físicos) no se consideran activos virtuales de acuerdo con la legislación mexicana y, por lo tanto, su uso y comercialización no está regulado.

Respecto a la segunda parte de la definición, la tecnología que soporta a los activos virtuales permite que las unidades de dichos activos e incluso sus fracciones no sean fungibles; es decir, que no sean intercambiables por otras de igual calidad y cantidad. En particular, cada unidad o fracción tiene un registro histórico de transacciones que permite la distinción entre las demás. Debido a que no tienen un carácter físico, los activos virtuales yacen en una red de computadoras que contiene toda la información transaccional de los activos virtuales. Las computadoras que forman la red están constantemente confirmando nuevas transacciones y actualizando el registro compartido por todas ellas.

Sobre lo referente a los protocolos, destacamos que las computadoras que operan en la red, las cuáles registran las transacciones de activos virtuales, deben seguir las reglas de emisión para poder confirmar las transacciones y que dichas reglas se deben establecer en protocolos predeterminados. Existe la posibilidad de que nuevas computadoras puedan formar parte de la red. Sin embargo, no es una característica necesaria.

Por último, respecto a la tercera parte de la definición se logra evitar que las réplicas de la unidad de información puedan ser transmitidas más de una vez en un mismo momento (el doble gasto) por medio de la identificación de las unidades o fracciones de un activo virtual a través de una revisión de su historial de transacciones particular, así como por medio de elementos criptográficos y etiquetas de tiempo, se evita que dicho activo virtual pueda ser gastado más de una vez al mismo tiempo.

Por el tratamiento en los medios, los activos virtuales tienden a asociarse con el concepto de moneda e incluso con servicios o productos financieros. Sin embargo, los activos virtuales legalmente no son moneda de curso legal en México[142]:

Hoy en día la mayoría de los sistemas informáticos funcionan de una manera centralizada, es decir, los datos se organizan a través de un solo sistema. Sin embargo, a pesar de ser la manera más usada de resguardo de información, estos sistemas no son completamente seguros y son vulnerables a fraude, *hackers*, *malwares*, o simplemente por cuestiones externas. Esta invasión genera tres problemas principales: (i) la alteración y/o pérdida de la información; (ii) el riesgo de fraude (ver la sección 7); y (iii) que el usuario conozca que la información fue alterada.

En segundo lugar, la tecnología "*Blockchain*" o "cadena de bloques" busca evitar prevenir las contingencias anteriores creando una serie de registros (en forma de bloques) que se encuentran unidas entre sí y que no se pueden alterar ni sobrescribir. Cualquier alteración en el registro "1", por ejemplo, se refleja de forma automática en el registro "2" y en los subsecuentes, además de que alerta a la red descentralizada de usuarios encargados de la supervisión de la cadena de bloques.

La idea de la tecnología *blockchain* surge en 1991 con la propuesta de "sellado de tiempo digital", tal como se realiza en las notarías, a fin de que no se pudieran modificar indebidamente. Pero, no fue conocida hasta la publicación del primer activo virtual: bitcoin.

26.2 Regulación.

Tanto los activos virtuales como la tecnología *blockchain* se encuentran regulados en la Ley Fintech y en las disposiciones secundarias de la misma emitidas por la CNBV y en la Circular 4/2019 publicada por Banxico.

Para efectos del artículo 30 de la Ley Fintech "activo virtual" se define como la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos[143]. De acuerdo con la citada ley, Banxico es

[142] *Op. Cit.* Banco de México. ¿Qué es un activo virtual?

[143] Ley Fintech.

la autoridad competente para establecer la forma en que los activos virtuales pueden ser utilizados, sus características, así como los convenios, mecanismos, reglas o protocolos que permitan generar, identificar, fraccionar y controlar la replicación de dichas unidades de valor. En ese sentido, para realizar operaciones con activos virtuales se debe solicitar autorización ante el Banco de México con el contenido señalado en la Ley Fintech y en la Circular 4/2019.

Las Entidades podrían contratar con terceros la prestación de servicios relacionados con operaciones con activos virtuales con sujeción a lo señalado a la Circular 4/2019. Dicha contratación debe ser autorizada por el Banco de México.

Conforme a la regulación emitida por Banco de México el uso de activos virtuales por parte de las Entidades se encuentra restringido y, sólo bajo ciertos supuestos, pueden usarse para usos "internos" y que no representen un riesgo para ellas.

26.3 Casos de uso de Blockchain.

El *blockchain* es usado no solamente a través de activos virtuales sino a través de contratos inteligentes. Los contratos inteligentes son protocolos o algoritmos computacionales que facilitan, verifican o refuerzan la ejecución parcial o total de un contrato[144]; es decir, al igual que los contratos tradicionales son acuerdos entre partes, pero no se necesita una tercera parte para la ejecución de los mismos, sino que, cuando se cumple el supuesto objeto del contrato, se ejecutan automáticamente. A continuación, señalamos algunas de las diferencias más relevantes entre los contratos tradicionales y los contratos inteligentes:

[144] LARSEN, Warren. *Blockchain Technology Explained* 2021.

Contrato tradicional	Contrato inteligente
Es necesaria la intervención de terceras partes para su ejecución.	No se necesita intervención de terceras personas para su ejecución.
El tiempo de ejecución puede tomar días.	El tiempo de ejecución es en minutos o instantáneo.
El proceso para la celebración es físico, costoso y consume mucho tiempo.	El proceso de celebración es automático.
La seguridad en la ejecución depende de mecanismos externos y de terceros.	La seguridad está garantizada ya que se encuentra protegido por cripto-seguridad.
Las firmas pueden ser difíciles de conseguir o no verificables.	Las firmas son digitales, son completamente seguras y siempre están verificadas por el emisor de la firma electrónica (ver Sección 12 Implementación de Firma Electrónica).

Tabla 10. Diferencia entre contratos tradicionales e inteligentes

Podemos comparar los contratos inteligentes con una máquina expendedora, debido a que la persona solamente "mete" el dinero, selecciona lo qué quiere y la maquina se encarga de entregar el producto, eliminando así cualquier tipo de intermediario. Cuando un contrato inteligente está montado sobre un *blockchain*, ninguna de las partes puede modificar ni alterar el contrato. Asimismo, ningún tercero puede intervenir en la ejecución del contrato. Recordamos que una de las características más importantes de la tecnología *blockchain* es que es descentralizada y distribuida, por lo que disminuyen los riesgos de los contratos y los sistemas informáticos tradicionales como virus informáticos[145].

Los contratos inteligentes, en forma general, tienen las siguientes características. Tienen las siguientes características:

- Los términos y condiciones, al igual que los contratos tradicionales, pueden ser tan específicos o generales según las necesidades de las partes.

[145] REED, Jeff. Smart Contracts.

- Se ejecutan solos.
- Se apegan absolutamente a su contenido, es decir, si algo no está escrito en el código, no se puede contemplar y no se prestan a interpretación de las partes. Así, si se suscitarán imprevistos, causas de fuerza mayor o casos fortuitos, el contrato se anula automáticamente.
- Es inmutable. Una vez creado y colocado sobre la cadena de bloques no se puede cambiar o modificar por nadie, incluyendo al creador del código.
- Debido a su naturaleza inmutable, deben contemplarse la mayor cantidad de circunstancias posibles en el clausulado del contrato para evitar la necesidad de modificarlo y/o darlo por terminado y generar otro.

Los contratos inteligentes se pueden aplicar a cualesquiera proyectos. A modo de ejemplo, proponemos la siguiente lista enunciativa:

- Celebrar contratos con proveedores con los que se tenga una relación estrecha.
- Generar los contratos de los empleados de las Entidades que se encuentren laborando en la modalidad de teletrabajo o en el extranjero.
- Ejecutar convenios de confidencialidad con potenciales aliados o proveedores que se encuentren en el extranjero y, en su caso, los convenios o contratos a través de los cuales se documenta la relación.
- En materia de seguros, para entregar la suma asegurada en cuanto suceda el siniestro.

Por último, proponemos las siguientes ventajas y desventajas de los contratos inteligentes a nuestra consideración:

Ventajas	Desventajas
No existen intermediarios	No se pueden prever todas las circunstancias
Es un proceso automatizado	Se requiere de tecnología altamente especializada y de un técnico que la conozca.
La implementación es un proceso rápido	La creación del contrato puede tomar tiempo la primera vez que se genere.
Es completamente seguro.	En este momento, la tecnología y sus aplicaciones en México son muy limitadas y costosas.
La ejecución es exacta y automática.	No se encuentran regulados por las autoridades mexicanas, por lo que entrarían dentro de un área gris de la regulación y requieren la opinión de un consultor externo que ayude a las Entidades a delimitar su aplicabilidad.

Tabla 11. Ventajas y desventajas de los contratos inteligentes

26.4 Consideraciones sobre Proyectos Blockchain.

Reiteramos que, hasta este momento, la tecnología *blockchain* (que no los activos virtuales) se encuentra regulada de forma tangencial. Esta circunstancia da lugar a ambigüedades en su aplicación, usos y, en especial, en la opinión de las autoridades financieras al respecto. Toda vez que la CNBV no ha emitido criterios ni informes respecto al uso de esta tecnología para los procesos, productos y/o servicios de las entidades financieras, cualquier proyecto que de esta naturaleza que se busque implementar deberá realizarse a través de una comunicación muy estrecha con la CNBV.

Adicionalmente, aunque determinados proveedores de firmas electrónicas, sistemas de contabilidad y otros procesos utilizan la tecnología *blockchain* para prestar sus servicios,

hasta este momento no conocemos de instituciones financieras de ninguna clase, incluyendo ITF, que utilicen la tecnología *blockchain* para prestar sus servicios. En ese sentido, aunque la tecnología *blockchain* ofrece nuevas posibilidades, hasta este momento no hay evidencia pública en relación con su implementación para entidades del sistema financiero mexicano. Adicionalmente, se requiere un alto nivel de especialización y una gran cantidad de recursos humanos, financieros y temporales para poder desarrollar e implementar proyectos con tecnología *blockchain*, además de que estos proyectos suponen un suelo de capacidades e infraestructura tecnológica propia de las Entidades.

La tecnología *blockchain* y los contratos inteligentes ofrecen posibilidades nuevas en cuanto al control interno, los productos y los servicios que pueden ofrecer las entidades financieras y comerciales, la implementación efectiva de proyectos de esta naturaleza se vislumbra aún distante. Cabe destacar, sin embargo, que la regulación mexicana en materia de nuevas tecnologías ha sufrido recientemente (y está sufriendo constantemente) modificaciones importantes y aceleradas para tratar de seguirle el paso a las nuevas tecnologías conforme incursionan en el mercado mexicano.

ANEXOS DOCUMENTACIÓN EJEMPLIFICATIVA

I. Aviso de Privacidad

A continuación, presentamos un modelo de aviso de privacidad que las Entidades podrían utilizar, en su caso, para elaborar el aviso de privacidad y ponerlo a disposición de sus clientes. En ese sentido, hacemos de su conocimiento que este modelo de aviso de privacidad únicamente es ejemplificativo y no debe considerarse como un documento aplicable para todas las entidades ni para todos sus productos y servicios. Por favor tome en cuenta que cualquier uso de este aviso de privacidad requiere de la asesoría legal de un experto en protección de datos personales para su elaboración y posterior uso y que el mismo en ninguna forma pretende sustituir la asesoría legal que un experto en la materia pudiera proveer.

AVISO DE PRIVACIDAD

1. Responsable de los Datos Personales.

[Denominación de la Entidad] (la "Entidad") con domicilio ubicado en (*), es responsable de recabar sus datos personales (en adelante el "Titular"), del uso que se le dé a los mismos y de su protección en cumplimiento a lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares ("LFPDPPP") y el Reglamento de dicha ley, observando en todo momento los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad en la recolección, administración y demás actos relacionados con sus datos personales.

2. Datos Personales que se recaban del Titular y son sometidos a tratamiento.

Para las finalidades establecidas en el presente Aviso de Privacidad, la [Entidad] podrá recabar de sus clientes de manera enunciativa más no limitativa, los siguientes datos: datos de identificación generales (tales como nombre, dirección, edad, entre otros), datos de contacto (incluyendo correo electrónico), datos financieros, mismos que son recabados a través de nuestra [página de internet/aplicación móvil].

Los datos personales recabados por la Entidad serán tratados para el cumplimiento de las finalidades identificadas en el presente Aviso de Privacidad, para lo cual la Entidad en este acto requiere y obtiene su consentimiento expreso para el tratamiento de dichos datos, de conformidad con lo establecido en el artículo 9° de la LFPDPPP.

De acuerdo con nuestras políticas comerciales, la Entidad no solicita ninguna información que bajo la LFPDPPP se entienda como datos sensibles, tales como religión, estado de salud, preferencias sexuales, opiniones políticas, entre otros.

El Titular reconoce de este momento en adelante que estos datos serán procesados de acuerdo a este Aviso de Privacidad, incluyendo sin limitar, su transferencia por consentimiento expreso de acuerdo al artículo 8 de la LFPDPPP y el artículo 15 del reglamento de la LFPDPPP en favor de aquellas personas que tengan el carácter de "Adquirente" o prestadores de servicios financieros que permiten a la Entidad prestar los servicios de pago y similares que aparecen en la página […] así como a cualesquier terceros que se mencionan en la sección IV del presente Aviso de Privacidad.

3. Finalidades para las que se recaban los Datos Personales.

Sus datos personales podrán ser utilizados por […] para (i) el mantenimiento y desarrollo de relaciones comerciales y legales con el Titular; (ii) la retroalimentación del servicio que prestamos a través del sitio web; (iii) transferir dicha información a un tercero no relacionado con la Sociedad para efecto de proporcionar los servicios que presta la Entidad; (iv) pago de servicios que el Titular solicite a través de nuestro [sitio web/aplicación móvil] y bajo los términos y con las limitaciones del mismo; (v) emisión de facturas; (vi) envío de publicidad de servicios, productos y líneas de negocios; (vii) cumplimiento de nuestras obligaciones legales y fiscales; y (viii) [en esta sección se deben incluir de forma específica todos los propósitos con los que se utilizarán los datos de los clientes.

4. Transferencia de Datos Personales.

Sus datos personales podrán ser transferidos y tratados por personas distintas de la Entidad, tales como: (i) sociedades subsidiarias, afiliadas o controladoras de la Entidad con finalidades de resguardo de la información, control de altas y bajas, (ii) evaluar cualquier cambio a los términos y condiciones del servicio; (iii) terceros no relacionados (prestadores de servicios), con la finalidad exclusiva de asistir a la Entidad en la ejecución de su objeto social y de la prestación del servicio; (iv) cuando sea requerido por mandato judicial de autoridades administrativas, judiciales o gubernamentales mexicanas o extranjeras de cualquier índole; y (v) al subcontratar a terceros, encargados de procesar su información por cuenta y bajo instrucciones de la Entidad o de cualquiera de sus sociedades afiliadas o partes relacionadas.

En términos del artículo 68 del Reglamento de la LFPDPPP y el artículo 36 de la LFPDPPP, el Titular consiente y autoriza expresamente cualquier transferencia de sus datos personales que la Entidad realice a las empresas relacionadas, subsidiarias, proveedores o consultores, así como a aquellas empresas que le permiten prestar servicios de pagos, incluyendo agregadores y/o bancos adquirentes y demás entidades o personas mencionadas en el párrafo anterior. Además, la Entidad garantiza que las transferencias realizadas cumplirán en todo momento lo dispuesto por los artículos 36 de la LFPDPPP y 68 del Reglamento de la LFPDPPP.

En términos del artículo 8 de la LFPDPPP y del artículo 15 del Reglamento de la LFPDPPP, por este medio usted autoriza y libera a la Entidad de toda responsabilidad en relación con la transferencia de sus datos (financieros o de cualquier especie) que esta realice o vaya a realizar ante terceras personas (con o sin contraprestación). Además, la Entidad está obligada a asegurarse que todas las transferencias cumplan, en todo momento, con la LFPDPPP y el Reglamento de la LFPDPPP en relación con los derechos ARCO y, en su caso, transferencias nacionales e internacionales de datos. La Entidad bajo ningún motivo transferirá los datos financieros del Titular, salvo por aquellos que este último autorice de manera expresa y los cuáles estén permitidos de acuerdo con lo establecido en la legislación aplicable.

5. Derecho de Acceso, Rectificación, Cancelación, Oposición (ARCO).

Usted tiene derecho de acceder, rectificar y cancelar sus datos personales, oponerse al tratamiento de los mismos, limitar su uso o divulgación o revocar el consentimiento que nos ha otorgado para el tratamiento de sus datos (estos derechos se conocen como derechos ARCO), enviando una solicitud al correo electrónico […].

Su solicitud deberá contener, al menos, la siguiente información: (i) nombre completo y correo electrónico para comunicarle la respuesta a su solicitud; (ii) los documentos que acrediten su identidad o, en su caso, la representación legal; (iii) la descripción clara y precisa de los datos personales respecto de los que busca ejercer alguno de los derechos antes mencionados; y (iv) cualquier otro elemento o documento que facilite la localización de los datos personales. Su petición será atendida dentro del plazo permitido por la ley y le informaremos sobre la procedencia de la misma a través del correo electrónico o domicilio que nos haya proporcionado.

En caso de que la información proporcionada en la solicitud sea insuficiente o errónea, o bien, no se acompañen los documentos necesarios, dentro de los 5 (cinco) días hábiles siguientes a la recepción de la solicitud, podremos requerirle que aporte los elementos o documentos necesarios para dar trámite a la misma. Usted contará con 10 (diez) días hábiles para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente.

Le comunicaremos la determinación adoptada en un plazo máximo de 20 (veinte) días hábiles contados desde la fecha en que se recibió la solicitud (o, en su caso, desde el día siguiente en que usted haya atendido el requerimiento de información) a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los 15 (quince) días hábiles siguientes a la fecha en que se comunique la respuesta. La respuesta se dará vía electrónica a la dirección de correo que se especifique en su solicitud. Los plazos antes referidos únicamente podrán ser ampliados de conformidad con la normatividad aplicable.

6. Revocación

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales en relación con las finalidades de tratamiento del presente Aviso de Privacidad a través del correo electrónico que se menciona en el presente. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales o en aquellos casos en los cuales usted haya aceptado la transferencia de datos. Asimismo, usted deberá considerar que, para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros. Usted podrá revocar su consentimiento siguiente el mismo procedimiento descrito anteriormente relacionado con los derechos ARCO.

7. Derecho de Limitar el Uso de los Datos Personales

Usted también podrá ejercer su derecho de limitar el uso o divulgación de su información, por ejemplo, para fines de mercadotecnia, siguiendo el mismo procedimiento descrito anteriormente relacionado con los derechos ARCO.

8. Modificaciones al Aviso de Privacidad

Cualquier modificación a este Aviso de Privacidad se la haremos llegar al último correo electrónico que haya proporcionado a la Entidad o podrá ser consultada en nuestro sitio web/aplicación móvil […].

Al aceptar los términos de este Aviso de Privacidad, usted manifiesta su consentimiento expreso para que la Entidad use, trate y transfiera los datos personales materia del presente para las finalidades aquí previstas.

9. Datos

En este acto el Titular reconoce que debido a la naturaleza de los servicios que presta la Entidad como entidad financiera, dicha Entidad tendrá acceso a datos personales (incluyendo sin limitar datos financieros) en términos del presente Aviso de Privacidad.

Fecha de última actualización: […].

II. Matriz de contratos de proveedores

A continuación, ponemos a su disposición un ejemplo de matriz de contratos en la cual es posible que las Entidades identifiquen los aspectos más relevantes de cada uno de ellos, incluyendo si el contrato es regulado o no regulado conforme a la Sección 15.- Contratación de Proveedores y Comisionistas. del presente documento.

TIPO DE CONTRATO	PARTES	DENOMINACIÓN O RAZÓN SOCIAL (TERCERO PRESTADOR DE SERVICIOS)	SERVICIO QUE SE CONTRATARÁ	DESCRIPCIÓN DEL SERVICIO	CONTRATO REGULADO O NO REGULADO	LÍMITE DEL CONTRATO (EN SU CASO)

III. Resoluciones ejemplificativas de aprobación de los manuales y sus modificaciones

A continuación, ponemos a su disposición una propuesta de resoluciones en las cuales (i) se aprueben los manuales, o (ii) se aprueben las modificaciones a los manuales. Por favor tome en cuenta que estas resoluciones únicamente son ejemplificativas y que será necesaria la asesoría del área jurídica interna de cada Entidad para elaborar las resoluciones correspondientes de conformidad con los estatutos sociales de cada una de ellas. Adicionalmente, tome en cuenta que este ejemplo no pretende sustituir en forma alguna la asesoría legal que pudieran proveer las áreas jurídicas internas de la Entidad o, en su caso, de asesores externos.

3.1. En caso de que se aprueben los manuales por primera vez:

En términos del Artículo […] de los estatutos sociales de la Entidad, la totalidad de los miembros del Consejo de Administración de la Entidad adoptamos [unánimemente, en su caso] la siguiente resolución:

RESOLUCIÓN

Se aprueban los siguientes manuales de la Entidad: (i) Manual de Administración Integral de Riesgos, (ii) Manual de Control Interno, (iii) Manual de Cumplimiento en Materia de Prevención de Operaciones de Procedencia Ilícita, (iv) Manual de Captación, (v) Manual de Crédito y (vi) Manual de Tecnologías de la Información.

3.2. En caso de que se aprueben modificaciones a los manuales:

Se someten a consideración del Consejo de Administración de la Entidad las siguientes modificaciones al Manual de Administración Integral de Riesgos:

a) Adicionar una sección en la cual se describen integralmente los riesgos a los que está expuesta la Entidad a partir del desarrollo de la aplicación móvil para prestar sus a través de ella.

b) Modificar las secciones relevantes para incluir los riesgos mencionados en el inciso a) anterior.

En términos del Artículo […] de los estatutos sociales de la Entidad, la totalidad de los miembros del Consejo de Administración de la Entidad adoptamos [unánimemente, en su caso] la siguiente resolución:

RESOLUCIÓN

Se aprueban las modificaciones a los siguientes manuales de la Entidad en virtud de lo expuesto anteriormente: (i) Manual de Administración Integral de Riesgos, (ii) Manual de Control Interno, (iii) Manual de Cumplimiento en Materia de Prevención de Operaciones de Procedencia Ilícita, (iv) Manual de Captación, (v) Manual de Crédito y (vi) Manual de Tecnologías de la Información.

IV. Cláusulas más relevantes del contrato de adquirencia

A continuación, ponemos a disposición de las Entidades algunas de las cláusulas más comunes que se utilizan en los contratos de adquirencia con Instituciones de Crédito. Por favor tome en cuenta que cada contrato responde a las circunstancias individuales de la relación jurídica entre las partes, por lo que las cláusulas que se presentan a continuación no representan: (i) la totalidad del clausulado de un contrato de adquirencia; (ii) cláusulas que se encuentren en todos los contratos de adquirencia; ni (iii) que la Entidad esté en posibilidades de negociar las cláusulas con el banco adquirente ya que, aunque no se trata de contratos de adhesión propiamente, en nuestra experiencia el Banco Adquirente ya tiene los contratos elaborados previamente.

- "El banco [adquirente] proporcionará a el afiliado [el agregador] únicamente dentro del territorio nacional, el servicio de Banco Adquirente mediante las siguientes modalidades, mismas que se activarán a solicitud del afiliado, ya sea, por medio de la carátula de servicios o mediante solicitud por escrito que deberá ser autorizada por el banco:

    - Mediante el uso de las TPV ["terminal punto de venta"] electrónica o sistemas interredes/Terminales de aceptación desatendida.
    - Mediante el uso de software de cargos automáticos.
    - Mediante el uso del software para comercio electrónico."

- "El afiliado se obliga a aceptar todos los pagos efectuados con tarjetas de crédito, tarjetas de débito, o ambas, operadas en el territorio nacional, en cualquiera de las modalidades, pudiendo optar por solo aceptar tarjetas de crédito o tarjetas de débito, o ambos tipos de tarjetas conforme a lo que decida el afiliado."

- "Las transacciones con tarjeta se tramitarán mediante las TPV o por medio de sistemas interredes, siendo este último aquellas TPV electrónicas y/o dispositivos similares o conexos incorporados a cajas registradores en el (los) establecimiento(s) del afiliado, las cuales deberán contar con la capacidad técnica y operativa para realizar la lectura y procesamiento del chip."

- “En la operación de los servicios objeto del presente contrato, el afiliado, sus dependientes, empleados y terceros involucrados en recibir pagos en su(s) establecimiento(s) se sujetarán, adicionalmente, a lo estipulado en el presente contrato, a las siguientes disposiciones:

    - Manual de integración e instructivo que el banco entrega en formato físico o electrónico a la firma del presente contrato.
    - Reglas emitidas o las que en el futuro se general por las empresas propietarias de marcas de tarjetas.
    - Reglamentos operativos interbancarios.
    - Convenios y/o acuerdos que se encuentren celebrados o que en un futuro celebren las Instituciones de Crédito y los relativos a procesadores de tarjetas y/o proveedores de servicios”.

- “El afiliado pagará a el banco, por los servicios objeto del presente contrato, los conceptos especificados en el formulario de comisiones y tarifas del banco que, firmado por el afiliado, formará parte integrante del presente contrato. El afiliado conoce y está de acuerdo en cubrir a el banco por los conceptos que se indican en el anexo correspondiente, los importes con cargo a la cuenta concentradora correspondiente donde se depositan sus ventas y/o a lo estipulado en el anexo correspondiente y caratula de servicios. Las comisiones se aplicarán por cada una de las transacciones con tarjeta, debiendo efectuarse el pago, el día del depósito de la transacción o al día siguiente de su rechazo por parte del procesador de tarjetas.”

- “El afiliado, sus dependientes, empleados o cualesquiera terceros encargados de las ventas del afiliado tienen prohibido, en la operación de las transacciones con tarjeta, incurrir en los siguientes supuestos:

    - Aceptar pagos de tarjetahabientes para amortizar pagarés suscritos por ellos.
    - Tramitar depósitos en la cuenta concentradora derivados de operaciones y/o pagarés de otros comercios.

- Tomar números de tarjetas de crédito y/o débito para hacer eso indebido de estos, por sí mismo o por terceros.
- Desembolsar efectivo en transacciones con tarjeta sin haber sido autorizado por el banco.
- Prestar a terceros y/o se utilicen por estos la(s) TPV asignadas a el afiliado, o no generar en dicho equipo lo pagarés derivados de transacciones con tarjeta.
- Guardar, copiar, imprimir o almacenar en cualquier medio la banda magnética o chip de las tarjetas de crédito y/o débito y/o los datos contenidos en la misma.
- Efectuar transacciones con tarjeta en operaciones no coincidentes con el giro o actividad principal del afiliado.
- Cobre a los tarjetahabientes consumidores alguna cantidad adicional al monto de la operación por realizar el pago con tarjetas de crédito y/o débito."

V. Cuestionario de contratación con terceros

A continuación, presentamos un cuestionario ejemplificativo que las Entidades pueden utilizar para identificar los datos más importantes de la relación contractual.

Cuestionario para contratar con *terceros y/o comisionistas*

Nombre del proveedor	
Partes	
Fecha de celebración del contrato	
Vigencia del contrato	
Objeto del contrato	
Tipo de actividad que lleva a cabo el tercero y/o comisionista (ver sección 15.4 "Tipos de corresponsales")	
Domicilio del tercero y/o comisionista	
Nacionalidad del tercero y/o comisionista	

¿Se trata de un Proveedor Relevante?	
¿Tiene limitaciones en cuanto al monto?	
¿La contratación afecta las operaciones de la Entidad?	
¿Requiere de modificaciones a los manuales? Especificar en cuáles y la modificación correspondiente.	
¿Requiere clausulado especial? (Ver Sección 15.8.2. relativa al Clausulado Específico de los contratos)	
¿Cuenta con la autorización del Consejo de Administración?	
¿Cuenta con la autorización de la CNBV para su celebración?	
Estatus de la autorización ante la CNBV (pendiente, otorgada, N/A)	

Glosario

Abogado, significa para efectos de esta Guía Legal el asesor legal, externo o interno, de las Entidades en cada uno de los proyectos de digitalización.

Administrador del Proyecto o AP, significa el administrador de un proyecto de digitalización tal como se presentan en esta Guía Legal.

Agregador, significa el Participante en Redes que, al amparo de un contrato de prestación de servicios celebrado con un Adquirente ofrece a Receptores de Pagos el servicio de aceptación de Pagos con Tarjetas y, en su caso, provee la infraestructura de TPVs conectadas a dichas redes

Área de Sistemas, significa para efectos de esta Guía Legal el asesor en materia informática, externo o interno, de las Entidades en cada uno de los proyectos de digitalización.

Asesor Legal, significa la firma de asesoría legal Vite Abogados.

Auditoría Interna, significa la modalidad de auditoría basada en el control y la vigilancia interna de la Entidad.

Autenticación, significa el conjunto de técnicas y procedimientos utilizados para verificar la identidad de: (a) un Usuario y su facultad para realizar operaciones a través de Servicios Electrónicos y (b) una Entidad y su facultad para recibir instrucciones a través de Servicios Electrónicos.

Aviso de Privacidad significa el documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con la LFPDPPP.

Banca Electrónica, significa la presentación de servicios de una Entidad a través de una plataforma virtual.

Banxico, significa el Banco de México

Buró de Entidades Financieras, significa la herramienta de consulta y difusión a través de la cual se publican los productos que ofrecen las entidades financieras, así como sus comisiones y tasas, las reclamaciones de los usuarios, las prácticas no sanas en que incurren, las sanciones administrativas que les han impuesto, las cláusulas abusivas de sus contratos y otra información que resulte relevante para informarte sobre su desempeño.

CAT, significa el Costo Anual Total de financiamiento expresado en términos porcentuales anuales que, para fines informativos y de comparación, incorpora la totalidad de los costos y gastos inherentes a los créditos, préstamos o financiamientos que otorgan las Entidades.

Cajero Automático, significa al dispositivo de acceso de autoservicio que permite realizar consultas y operaciones diversas, tales como la disposición de dinero en efectivo y al cual el usuario accede mediante una tarjeta o cuenta para utilizar los servicios electrónicos.

Cifrado, significa el mecanismo que deberá utilizar la Entidad para proteger la confidencialidad de información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.

CNBV, significa la Comisión Nacional Bancaria y de Valores.

Comité de Supervisión Auxiliar, significa el órgano del Fondo de Protección encargado de ejercer la supervisión auxiliar de las Cajas de Ahorro con niveles de operación de I a IV, realizar operaciones preventivas tendientes a evitar problemas financieros que puedan presentar dichas sociedades, llevar a cabo las evaluaciones a que se refiere la LRASCAP a las Cajas de Ahorro con niveles de operación básico, así como procurar el cumplimiento de obligaciones relativas a los depósitos de ahorro de sus Socios en los términos y condiciones que dicha ley establece.

Comité de Supervisión, significa el órgano de las Federaciones encargado de ejercer la supervisión auxiliar de las SOFIPO.

Condusef, significa la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

Consejo de Administración, significa el consejo de administración de cualquiera de las Entidades, que es el máximo órgano de gobierno de dichas Entidades. Normalmente se elige al Consejo de Administración a través de los accionistas; en el caso de las SOCAP se elige a algunos Socios como Consejeros.

Cuenta Destino, significan las cuentas receptoras de recursos dinerarios en Operaciones Monetarias.

Datos Financieros, significa toda aquella información que se relaciona y/o se identifica con el patrimonio de una persona física o moral.

Datos Personales, significa cualquier información concerniente a una persona física identificada o identificable.

Director General, significa la persona que es la principal autoridad de la administración de la Entidad.

Disposiciones Generales SOCAP, significa las Disposiciones de Carácter General Aplicables a las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo.

Disposiciones Generales SOFIPO, significa las Disposiciones de Carácter General Aplicables a las Entidades de Ahorro y Crédito Popular, Organismos de Integración, Sociedades Financieras Comunitarias y Organismos de Integración Financiera Rural a que se refiere la Ley de Ahorro y Crédito Popular.

Disposiciones PLD/FT, significan las Disposiciones de Carácter General a que se refieren los artículos 71 Y 72 de la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo; las Disposiciones de Carácter General a que se refiere el artículo 124 de la Ley de Ahorro y Crédito Popular; y las Disposiciones de Carácter General a que se refieren los artículos 115 de la Ley De Instituciones De Crédito en relación con el 87-D

de la Ley General de Organizaciones y Actividades Auxiliares del Crédito y 95-Bis de este último ordenamiento, aplicables a las Sociedades Financieras De Objeto Múltiple.

Dispositivo, significa el equipo que permite acceder a la red mundial denominada Internet, el cual puede ser utilizado para realizar aperturas de cuenta o celebrar contratos, así como realizar operaciones.

Dispositivo de Acceso, significa al equipo que permite a un Usuario acceder a los Servicios Electrónicos.

Encargado, significa aquella persona física o moral que sola o en conjunto con otra persona trata Datos Personales por cuenta del responsable.

Entidades, significa de manera conjunta y para efectos del presente documento las SOCAP, las SACP, las SOFINCO y las SOFOM.

Expedientes KYC, significa los expedientes de conocimiento de cliente que las Entidades están obligadas a formar conforme a las disposiciones PLD/FT.

Evaluación Nacional de Riesgos, significa la Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo.

Factor de Autenticación, significa al mecanismo de Autenticación, tangible o intangible, basado en las características físicas del Usuario, en dispositivos o información que solo el Usuario, posea o conozca. Estos mecanismos podrán ser:

- Información que el Usuario conozca y que la Entidad valide a través de cuestionarios practicados por operadores de atención telefónica.

- Información que solamente el Usuario conozca, tales como contraseñas y números de identificación personal (NIP).

- Información contenida, recibida o generada en medios o dispositivos respecto de los cuales el Usuario tenga posesión, tales como dispositivos o mecanismos

generadores de contraseñas dinámicas de un solo uso y tarjetas de crédito o débito con circuito integrado, que tengan propiedades que impidan la duplicación de dichos medios, dispositivos o de la información que estos contengan o generen.

- Información del Usuario derivada de sus características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, siempre que dicha información no pueda ser duplicada y utilizada posteriormente.

Federación, en singular o plural, a las Federaciones autorizadas por la Comisión, para ejercer de manera auxiliar la supervisión de las SOFIPO.

Firma Electrónica Avanzada o Fiable, significa la Firma Electrónica que cumpla con los siguientes requisitos:

- Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

- Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

- Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y

- Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

FOCOOP o Fondo de Protección, significa el Fideicomiso del Fondo de Supervisión Auxiliar de Sociedades Cooperativas de Ahorro y Préstamo y de Protección a sus Ahorradores.

GAT, significa la Ganancia Anual Total Neta expresada en términos porcentuales anuales, que, para fines informativos y de comparación, incorpora los intereses que generen las operaciones pasivas de ahorro, inversión y otras análogas, que celebren las instituciones de crédito, las entidades de ahorro y crédito popular y las uniones de crédito con sus Clientes, menos todos los costos relacionados con la operación, incluidos los de apertura,

será expresado tanto en términos reales como nominales, conforme a las disposiciones que emita el Banco de México para su cálculo.

Geolocalización, significan las coordenadas geográficas de latitud y longitud en que se encuentre el Dispositivo.

Guía Legal, significa el presente documento de orientación legal para la implementación de proyectos de digitalización del sector SACP.

Guía para la Contratación de Servicios, significa la Guía para la Autorización de Contratación de Servicios o Comisiones dirigida a las SOCAP.

Guía para la Contratación Comisionistas, significa la Guía para la Autorización de Contratación de Comisionistas dirigida a las SOFIPO y SOFINCO.

IFPE, significa las Instituciones de Fondos de Pago Electrónico.

IFC, significa las Instituciones de Financiamiento Colectivo.

Identificador de Usuario, significa la cadena de caracteres, información de un dispositivo o cualquier otra información que conozca tanto la Entidad como el Usuario, que permita reconocer la identidad del propio Usuario para el uso de Servicios Electrónicos.

Infraestructura Tecnológica, significa los equipos de cómputo, instalaciones de procesamiento de datos y comunicaciones, equipos y redes de comunicaciones, sistemas operativos, bases de datos, aplicaciones y sistemas que utilizan las Entidades para soportar sus operaciones;

INAI, significa Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Información Sensible del Usuario, significa la información personal del Usuario que contenga nombres, domicilios, teléfonos o direcciones de correo electrónico, en conjunto

con números de tarjetas de crédito o débito, números de cuenta, límites de crédito, saldos, Identificadores de Usuarios o información de Autenticación.

ITF, significa Instituciones de Tecnología Financiera.

KYC, significa políticas conoce a tu cliente o *know your client*, por sus siglas en inglés.

LACP, significa la Ley de Ahorro y Crédito Popular.

Ley Fintech o LRITF, significa la Ley para Regular a las Instituciones de Tecnología Financiera.

LFPDPPP, significa la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

LGOAAC, significa Ley de Organizaciones y Actividades Auxiliares del Crédito.

LGSM, significa la Ley General de Sociedades Mercantiles.

Lista de Personas Bloqueadas, significa la lista que contiene los nombres de las personas que han sido identificadas por realizar actividades con recursos de procedencia ilícita conforme a los parámetros internacionales y nacionales.

LMV, Ley del Mercado de Valores.

LRASCAP, significa la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo.

LTOSF, significa la Ley para la Transparencia y Ordenamiento de los Servicios Financieros.

Manuales, significa aquellos documentos internos de cada Entidad que marcan la pauta de aspectos financieros, operativos y legales de conformidad con la regulación aplicable.

Medio de Disposición, significa tarjetas de débito asociadas a depósitos de dinero a la vista; tarjetas de crédito emitidas al amparo de un contrato de apertura de crédito; cheques; órdenes de transferencia de fondos, incluyendo el servicio conocido como domiciliación; cualquier dispositivo, tarjeta, o interfaz que permita la realización de pagos, transferencias de recursos o disposición de efectivo cuyas operaciones se procesen por medio de las Redes de Medios de Disposición, así como aquellos otros que la Comisión Nacional Bancaria y de Valores y el Banco de México, de manera conjunta, reconozcan como tales mediante disposiciones de carácter general.

Medios Electrónicos, significan los equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados y que utilicen las Entidades para prestar servicios a sus Socios o Clientes.

Mitigantes, significa la identificación de los controles, estructuras internas, medidas, criterios, políticas y procedimientos implementados por las Entidades, así como los recursos de cumplimento que constituyen a administrar, controlar y disminuir (no evitar o anular), la exposición de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo.

Nivel de Capitalización, significa la relación que guarda el capital neto de las SOFIPO y de las SOCAP respecto de los requerimientos de capitalización por riesgos de crédito y de mercado, de acuerdo a las disposiciones de carácter general emitidas por la CNBV.

Nivel de Operaciones, significa el nivel de operaciones asignado, de entre cuatro niveles, por la CNBV a las SOFIPO y a las SOCAP, de conformidad con la LACP, la LRASCAP y con las reglas generales emitidas por CNBV.

Operación, significan las actividades realizadas por las Entidades conforme a su ley específica cuando sean celebradas con Clientes o Usuarios e independientemente del nivel de operación de la Entidad.

Operación Monetaria, significa la transacción que implique transferencia o retiro de recursos dinerarios. Conforme a la regulación las operaciones monetarias podrán ser:

- Micro Pagos: operaciones de hasta el equivalente en moneda nacional a 70 UDIs.

- De Baja Cuantía: operaciones de hasta el equivalente en moneda nacional a 250 UDI diarias.

- De Mediana Cuantía: operaciones de hasta el equivalente en moneda nacional a 1,500 UDI diarias.

- Por montos superiores al equivalente en moneda nacional a 1,500 UDIs diarias.

Plan Estratégico de Negocios, significa el plan que debe presentarse por las Entidades que deseen contratar con comisionistas la prestación de ciertos servicios financieros en su nombre y representación.

Personas Políticamente Expuestas, significa Aquel individuo que desempeña o ha desempeñado funciones públicas destacadas en un país extranjero o en territorio nacional, considerando entre otros, a los jefes de estado o de gobierno, líderes políticos, funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales o funcionarios o miembros importantes de partidos políticos.
Se asimilan a las Personas Políticamente Expuestas, el cónyuge, la concubina, el concubinario y las personas con las que mantengan parentesco por consanguinidad o afinidad hasta el segundo grado, así como las personas morales con las que la Persona Políticamente Expuesta mantenga vínculos patrimoniales

PLD/FT, es el acrónimo que representa prevención de lavado de dinero y financiamiento al terrorismo.

POC, significa prueba de concepto.

Presentación de Proyecto, significa la presentación realizada en cualquier formato a través de la cual se establecen las características generales y demás detalles relacionados con un Proyecto para su difusión hacia terceros, incluyendo órganos de administración, directivos o reguladores.

Proveedores Relevantes, significa aquellos proveedores cuya contratación requiere del cumplimiento de requisitos específicos y, en su caso, de la notificación de su contratación o la solicitud de autorización para ello ante CNBV.

Redes de Medios de Disposición, significa la serie de acuerdos, protocolos, instrumentos, interfaces, procedimientos, reglas, programas, sistemas, infraestructura y demás elementos relacionados con el uso de Medios de Disposición.

PSS, significa el proveedor de servicios en la nube.

Servicios Básicos Móviles o Pago Móvil, significa el Servicio Electrónico en el cual el Dispositivo de Acceso se encuentra asociado con correspondencia unívoca al Identificador de Usuario, mediante cualquier información o datos únicos del propio Dispositivo de Acceso, debiendo la sociedad cooperativa de ahorro préstamo obtener la información o datos de manera automática del Dispositivo de Acceso correspondiente y únicamente se puedan realizar consultas de saldo respecto de las cuentas o tarjetas asociadas al servicio, Operaciones Monetarias limitadas a transferencias de recursos dinerarios y pagos de bienes o servicios, en ambos casos, de hasta el equivalente en moneda nacional a las Operaciones Monetarias de Mediana Cuantía por Usuario, con cargo a las tarjetas o cuentas bancarias que tenga asociadas.

Participante de SPEI, significa Banco de México y a las entidades que hayan firmado con dicho Banco el contrato para participar en el SPEI en términos de la circular 17/2010 a fin de estar en posibilidades de enviar y recibir órdenes de transferencia.

Partes Responsables, significa aquellas partes involucradas en la realización de un proyecto de digitalización.

Proyecto, significa de manera indistinta cualquier proyecto de digitalización que se presentan en esta Guía Legal.

Proveedor Relevante, significa el comisionista o proveedor que previo a la prestación de servicios requiere dar aviso u obtener autorización de la autoridad competente.

RDP, significa el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

RECA, significa Registro de Contratos de Adhesión.

RECO, significa Registro de Comisiones.

Reguladores, significan en conjunto SHCP, CNBV, Banxico y Condusef.

Responsables, significa la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Riesgo, significa la probabilidad de que las Entidades puedan ser utilizadas por sus Clientes o Usuarios para realizar actos u Operaciones a través de los cuales se pudiesen actualizar los supuestos previstos en los artículos 139 Quáter o 400 Bis del Código Penal Federal.

Servicios Avanzados Móviles, significa el Servicio Electrónico, en el cual el Dispositivo de Acceso se encuentra asociado con correspondencia unívoca al identificador de Usuario, mediante cualquier información o datos únicos del propio Dispositivo de Acceso.

Servicios de Comisionistas o de Proveedor, significan aquellos servicios prestados por un Comisionista o Proveedor de servicios a la Entidad.

Servicios Electrónicos, significa conjunto de servicios y operaciones que la Entidad realiza con sus Usuarios a través de Medios Electrónicos.

Servicios Excluidos, significa aquellos servicios que no son prestados por Proveedores Relevantes.

Servicios Telefónicos Voz a Voz, significa Servicio Electrónico mediante el cual un Usuario instruye vía telefónica a través de un representante de la Entidad debidamente autorizado por esta, con funciones específicas a realizar operaciones a nombre del propio Usuario.

SIPRES, significa el Sistema de Registro de Prestadores de Servicios Financieros que lleva la Condusef.

Sistema Automatizado, significa una plataforma que ayuda a la Entidad a llevar de forma organizada el cumplimiento de tus obligaciones PLD/FT.

SHCP, significa la Secretaría de Hacienda y Crédito Público.

Sistema de Control Interno, significa el seguimiento y control de las actividades internas de la Entidad.

SOCAP, significa Sociedades Cooperativas de Ahorro y Préstamo.

Socio, significa, en singular o plural, a las personas físicas o morales que participen en el capital social de las Sociedades Cooperativas de Ahorro y Préstamo.

SPK, significa Sparkassenstiftung Alemana para la Cooperación Internacional (DSIK) für internationale Kooperation e.V.

SACP, significa el sector de ahorro y crédito popular mexicano.

Servicios Electrónicos: significa el conjunto de servicios y operaciones que la Entidad realiza con sus Usuarios a través de Medios Electrónicos.

SOFINCO, significa las Sociedades Financieras Comunitarias.

SOFIPO, significa las Sociedades Financieras Populares.

SOFOM, significa Sociedades Financieras de Objeto Múltiple, Entidades No Reguladas.

Tarjeta, significa tarjeta de débito y tarjeta de crédito.

Tarjetahabiente: significa el titular de la Tarjeta susceptible de utilizarse en la Red de Pagos con Tarjeta.

Terminal Punto de Venta o TPV, significan los medios de acceso a la red de pagos con Tarjeta, tales como dispositivos electrónicos, terminales, teléfonos móviles y programas de cómputo, operados por receptores de pagos para instruir el pago de bienes o servicios con cargo a una Tarjeta.

Titular, significa la persona física a quien corresponden los datos personales.

UDI, significa Unidades de Inversión.

UNE, significa Unidad Especializada de Atención a Usuarios

Usuario, significa al Socio o el Cliente que haya suscrito un contrato de Servicios Electrónicos con una Entidad.

Normatividad utilizada para la realización de la Guía Legal

Circular 4/2019.

Circular 5/2019.

Circular 14/2017.

Circular 21/2009.

Circular 34/2010.

Código de Comercio.

Código Penal Federal.

Disposiciones de Carácter General Aplicables a las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo.

Disposiciones de Carácter General Aplicables a las Entidades de Ahorro y Crédito Popular, Organismos de Integración, Sociedades Financieras Comunitarias y Organismos de Integración Financiera Rural a que se refiere la Ley de Ahorro y Crédito Popular.

Disposiciones de Carácter General Aplicables a las Redes de Medios de Disposición.

Disposiciones de Carácter General Relativas a las Interfaces de Programación de Aplicaciones Informáticas Estandarizadas a las que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera.

Disposiciones de Carácter General a que se refieren los artículos 71 Y 72 de la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo.

Disposiciones de Carácter General a que se refiere el artículo 124 de la Ley de Ahorro y Crédito Popular

Disposiciones de Carácter General a que se refieren los artículos 115 de la Ley De Instituciones De Crédito en relación con el 87-D de la Ley General de Organizaciones y Actividades Auxiliares del Crédito y 95-Bis de este último ordenamiento, aplicables a las Sociedades Financieras De Objeto Múltiple.

Ley de Ahorro y Crédito Popular.

Ley del Mercado de Valores.

Ley de Transparencia y de Fomento a la Competencia en el Crédito Garantizado

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita

Ley General de Organizaciones y Actividades Auxiliares del Crédito.

Ley General de Sociedades Mercantiles.

Ley para Regular a las Instituciones de Tecnología Financiera.

Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo.

Ley para la Transparencia y Ordenamiento de los Servicios Financieros.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Bibliografía Consultada

(1) ¿De qué hablamos cuando hablamos de Big Data en el sector financiero? (Internet) 19 de febrero de 2020 Consultado en: https://www.empresaactual.com/big-data-sector-financiero/

(2) ¿Qué es y cómo hacer un manual de procedimientos? (Internet) Consultado en: https://softgrade.mx/manual-de-procedimientos/

(3) 10 steps to building an integrated Information management roadmap. (Internet) Consultado en: https://www.accesscorp.com/blog/10-steps-to-building-an-integrated-information-management-roadmap/

(4) 6 Tips for File Digitalization. (Internet) Consultado en: http://nimble.ca/6-Tips-for-File-Digitization

(5) A 7-year digital transformation for this Singapore bank enabled its survival success in the world's new normal (Internet) Consultado en: https://www.businessinsider.com/singaporean-banks-7-year-digital-transformation-enabled-its-survival-2020-9?r=MX&IR=T

(6) ALDIABAT, K., *et. al.* (2019). *The Effect of Mobile Banking Application on Customer Interaction in the Jordanian Banking Industry.*

(7) ALTALEB, H. & KOCAK, S. *The Risk of Using Biometrics*. Óbuda University, Institute of Mechatronics and Vehicle Engineering.

(8) Applied Legal Project Management (Internet) Consultado en: legalprojectmanagementelearning.com

(9) Banco de México. (2018) ¿Qué es y cómo funciona el SPEI? Consultado en: https://www.banxico.org.mx/spei/d/%7B44351472-054C-58EB-611D-153B1029C2A8%7D.pdf

(10) Banco de México. (2019). Informe Anual sobre las Infraestructuras de los Mercados Financieros.

(11) Banco de México. ¿Qué es un activo virtual? [Internet] Consultado en: Activos virtuales, definición, Banco de México (banxico.org.mx) el 25 de enero de 2021.

(12) Banco Interamericano de Desarrollo. Sandbox Regulatorio en América Latina y el Caribe para el ecosistema Fintech y el sistema financiero.

(13) Banxico. Sistema de Pagos Electrónicos (Internet) Consultado en: https://www.banxico.org.mx/servicios/sistema-pagos-electronicos-in.html

(14) Becoming more than a bank: Digital transformation at DBS (Internet) Consultado en: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/becoming-more-than-a-bank-digital-transformation-at-dbs#

(15) BIS. The supertech generations. (Internet) Consultado en: https://www.bis.org/fsi/publ/insights19.htm

(16) BURKE, Brian A. (2019). *How Cloud Computing Is Transforming and Benefiting Financial Institutions*. DePaul University.

(17) CAPCO CENTER OF REGULATORY INTELLIGENCE. (2018) *Exploring Partnerships in Fintech*. Regulatory Intelligence Briefing.

(18) CECOBAN, Reporte Open Banking MX-2019.

(19) CEMLA. The Role Payments Systems (Internet) Consultado en: https://www.cemla.org/PDF/forodepagos-TheRolePaymentSystems.pdf

(20) CHUNG, Chang-ho. *Legal Issues Arising from the Use of Mobile Devices in Electronic Commerce*.

(21) CNBV. Descripción del Sector (Internet) Imagen obtenida de: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/PARTICIPANTES EN REDES DE MEDIOS DE DISPOSICI%C3%93N/Paginas/DescripcionDelSector.aspx

(22) CNBV. Modelos de negocio para la inclusión financiera 1. (Internet) Consultado en: https://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Modelos%20de%20Negocio%20para%20la%20IF/1%20Corresponsales%20Bancarios.pdf

(23) CNR. 10 future cloud computing trends to watch in 2021. (Internet) Consultado en: https://www.crn.com/news/cloud/10-future-cloud-computing-trends-to-watch-in-2021

(24) Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros. (2020). México: *Cifras relevantes de Banco de México en Comercio Electrónico*. (Internet) Consultado en: https://www.condusef.gob.mx/?p=estadisticas

(25) CRYPTOMATHIC. *Adopting a Global eSignature Strategy for Large Banks and Financial Services*.

(26) D.A. Reed, J. (2015) Dongarra Exascale Computing and Big Data. Communications of the ACM New York, NY, USA: ACM, 58 (7), pp. 56-68

(27) DAWSON, Steve. (2015). *Internal Control/Anti-Fraud Program Design for the Small Business*.

(28) DE MAN, Ard-Pieter. (2013). *Alliances*. Wiley.

(29) DI CASTRI, Simone. (2013). *Enabling Mobile Money Policies in Sri Lanka the Rise of eZ Cash*. Mobile Money for the Unbanked.

(30) DURÁN DÍAZ, O.J. (2018). Código de Comercio y Medios Electrónicos. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.

(31) ERNST & YOUNG. (2020) *FinTech partnerships*.

(32) ERNST & YOUNG. (2020) *Navigating Joint Ventures*.

(33) ESQUIVEL MARTÍNEZ, H. (2008). Situación actual del Sistema de Ahorro y Crédito Popular en México.

(34) FIGUEROA-HERNÁNDEZ, *et. al*. Las sociedades de ahorro y crédito popular de México.

(35) Gawer, A. (2009) Platforms, Markets and Innovation. Edward Elgar.

(36) GIONES-VALLS, Aina. La gestión de la identidad digital: una nueva habilidad información digital. (Internet) Consultado en: http://bid.ub.edu/24/giones2.htm

(37) GlobalDots. Cloud computing types of clouds. (Internet) Consultado en: https://www.globaldots.com/blog/cloud-computing-types-of-cloud

(38) Gómez Giovanny. (Internet). *Manual de procedimientos: qué es, objetivos, estructura y su justificación frente al control interno*. Consultado en https://www.gestiopolis.com/manuales-procedimientos-uso-control-interno/

(39) Guía para la Contratación Comisionistas SOFIPO y SOFINCOS.

(40) Guía para la Contratación de Servicios SOCAP.

(41) ICBA & HUNTINGTON & WILLIAMS. (2018). *Fintech Strategy Roadmap for Comminity Banks*.

(42) IMF. Pandemic Preparedness for Financial Institutions. (Internet) Consultado en: https://www.imf.org/~/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-pandemic-preparedness-for-financial-institutions.ashx.

(43) KASSA, Dawit. (2015) Document control. *Lifecycle and the governance challenge*.

(44) KELLY, S., *et. al*. *How Financial Institutions and Fintechs Are Partnering for Inclusion: Lessons from the Frontlines*. Institute of International Finance & Center for Financial Inclusion.

(45) KNÖL, Esteban. Objetivos SMART: qué son y cómo utilizarlos. (Internet) Consultado en: https://www.titular.com/blog/objetivos-smart-que-son-y-como-utilizarlos.

(46) LAL, R. & SACHDEV, I. (2015) *Mobile Money Services – Design and Development for Financial Inclusion*. Harvard Business School.

(47) LARSEN, Warren. *Blockchain Tecnology Explained* 2021.

(48) LEONOVICH, P. (2020) *Monetary and Capital Markets: Pandemic Preparedness for Financial Institutions*. International Monetary Fund.

(49) MARTÍNEZ SÁNCHEZ, J.F. & PÉREZ LECHUGA, G. (2015). Evaluación de un sistema de *credit scoring* para instituciones de ahorro y crédito popular. Facultad de Contaduría y Administración de la Universidad Nacional Autónoma de México.

(50) MAS. Guidelines on Outsourcing for financial institutions. (Internet) Consultado en: https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

(51) MATCHI BIZ. *Fintech to Fintech Partnerships: The Way of the Future*.

(52) MATYAS, M. & RIHA, Zdenek. (2002). *Biometric Authentication – Security and Usability*.

(53) Microsoft Azure. What is cloud computing. (Internet) Consultado en: *https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/*

(54) MIREKU KWAKYE, M., *et. al.* (2015). *Adoption of Biometric Fingerprint Identification as an Accessible, Secured form of ATM Transaction Authentication*. Ghana Technology University College.

(55) Monetary Authority of Singapore. (2016). *Guidelines on Outsourcing*.

(56) MORALES, R., *et. al. The Role of Payment Sustems and Services in Financial Inclusion. Latin American and Caribbean Perspective*. Center for Latin American Monetary Studies.

(57) MORENO Y GUTIÉRREZ, F.J., *et. al*. Sistemas de pagos en México.

(58) OPUSRESEARCH. *Guidelines for Deploying Mobile Biometrics in Financial Services*.

(59) PERDANA, P.A. & SUHARJITO (2017). *Cloud Computing Implementation Using Rocca Model in PT Matrica Consulting Service*. Bina Nusantara University.

(60) PÉREZ-SOTO, F., *et. al*. Matemáticas Aplicadas a la Economía. *Handbook T-1*. ECORFAN.

(61) PINTO, Jeffrey K. & SLEVIN, Dennis P. (2006). *Critical Success Factors in Effective Project Implementation*.

(62) PriceWaterhouseCoopers Australia. *Fraud: A guide to its prevention, detection and investigation*. (Internet) Consultado en: https://www.pwc.com.au/consulting/assets/risk-controls/fraud-control-jul08.pdf

(63) Ramachandran, S., Yousif, N., et. al. (2019). Boston Consulting Group. A Smarter Way to Quantify Cybersecurity Risk. (Internet) Consultado en: https://www.bcg.com/capabilities/digital-technology-data/smarter-way-to-quantify-cybersecurity-risk

(64) Rodríguez P, Palomino N, Mondaca J. (2017) El uso de datos masivos y sus técnicas analíticas para el diseño e implementación de políticas públicas en Latinoamérica y el Caribe.

(65) Sociedades Financieras Populares (Internet) Consultado en: https://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/SECTOR-POPULAR/Preguntas-Frecuentes/Paginas/Sociedades-Financieras-Populares.aspx

(66) Sweeney L. Simple Demographics Often Identify People Uniquely (Internet). Consultado en: https://dataprivacylab.org/projects/identifiability/paper1.pdf

(67) Thales Group. Digital identity and security. (Internet) Consultado en: https://www.thalesgroup.com/en/markets/digital-identity-andsecurity/government/inspired/biometrics

(68) The Central Bank of The Bahamas. (2006) *Supervisory and regulatory Guidelines: Electronic Banking.*

(69) The Data Deluge. The Economist [Internet]. 25 de febrero del 2010 [consultado el 1 de agosto del 2018]. Recuperado de: https://www.economist.com/leaders/2010/02/25/the-data-deluge.

(70) TORRES GRIMALDO, J.A. & CANO MORALES, A. María (2019). Importancia del Gobierno Corporativo en las sociedades financieras populares en México. Universidad Autónoma de Tamaulipas, México y Universidad de Medellín, México.

(71) U.S. GLOBAL DEVELOPMENT LAB. *Making the Journey from Cash to Electronic Payments*: *A Toolkit for USAID Implementing Partners and Development Organizations.*

(72) UNCITRAL. Detección y prevención del fraude comercial: indicadores de fraude comercial. (Internet) Consultado en: https://www.uncitral.org/pdf/spanish/texts/fraud/Recognizing-and-preventing-commercial-fraud-s.pdf

(73) UNESCO, Carta para la preservación del patrimonio digital, 2003. (en línea). http://www.r020.com.ar/enlaces/ir.php?ir_id=665 (Consulta: 26 de agosto de 2004).

(74) Unidad de Inteligencia Financiera. Evaluación Nacional de Riesgos de Lavado de Dinero y Financiamiento al Terrorismo en México 2019-2020. (Internet) Consultado en: https://www.uif.gob.mx/work/models/uif/comunicados/imp/ENR2019-2020/

(75) VENKATRAMAN, S. & DELPACHITRA, I. *Biometrics in banking security: a case study.*

(76) WISCONSIN HISTORICAL SOCIETY. *Digitalization Project Guidance for State Agencies.* Division of Library, Archives and Museum Collections.

(77) YouGov. Breaking the Banks? Revolut, Starling and the rise of “challenger” firms. (2020) Consultado en: https://yougov.co.uk/topics/finance/articles-reports/2020/08/14/breaking-banks-revolut-starling-and-rise-challenge

(78) YouGov. Future Banking. (2015) Consultado en: Results-for-Pinsent-Mason-Future-Banking-221015.pdf

Miembros de Grupo de Trabajo

Caja Popular Cerano, S.C. de A.P. de R.L. de C.V.

Lic. Eduardo Gómez Villagómez

Federación de Cajas Populares Alianza SC de RL de CV.

Ing. Carlos Salvador Jesús Arévalo

C.P. José Francisco Ramírez Ávila

Caja Depac Poblana, SC de AP de RL de CV

Lic. Rocío Nayeli Pérez Ramírez

Administradora de Caja Bienestar, S.A. de C.V., S.F.P.

Ing. Edgar Guerrero Ibarra

Ing. Takenobu Yamaguchi Carranza

Ing. Pablo Rodríguez Fajardo

Consultores

VITE ABOGADOS

Eliseo Vite

Pablo Rueda

Natalia Gastélum

implementada por:

Sparkassenstiftung Alemana
LATINOAMÉRICA Y EL CARIBE

https://sparkassenstiftung-latinoamerica.org/
https://www.sparkassenstiftung.de/es/