DISPOSICIONES DE CARÁCTER GENERAL RELATIVAS A LAS INTERFACES DE PROGRAMACIÓN DE APLICACIONES INFORMÁTICAS ESTANDARIZADAS A QUE HACE REFERENCIA LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA

Publicadas en el Diario Oficial de la Federación el 4 de junio de 2020.

La Comisión Nacional Bancaria y de Valores, con fundamento en lo dispuesto por los artículos 76, párrafos tercero, octavo, décimo primero, décimo segundo y décimo tercero de la Ley para Regular las Instituciones de Tecnología Financiera, así como los artículos 4, fracciones XXXVI y XXXVIII; 16, fracción I y 19 de la Ley de la Comisión Nacional Bancaria y de Valores, y

CONSIDERANDO

Que en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de las presentes disposiciones, la Comisión Nacional Bancaria y de Valores mediante resolución publicada en el Diario Oficial de la Federación el 22 de enero de 2018, reformó las "Disposiciones de carácter general aplicables a las instituciones de crédito", con el fin de flexibilizar el plazo para constituir requerimientos de capital y constituir dichos requerimientos de forma gradual;

Que el 9 de marzo de 2018 se publicó en el Diario Oficial de la Federación el "Decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de Organizaciones y Actividades Auxiliares del Crédito, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, de la Ley para Regular las Sociedades de Información Crediticia, de la Ley de Protección y Defensa al Usuario de Servicios Financieros, de la Ley para Regular las Agrupaciones Financieras, de la Ley de la Comisión Nacional Bancaria y de Valores y, de la Ley Federal para la Prevención e Identificación de Operaciones de Procedencia Ilícita";

Que el artículo 76 de la Ley para Regular las Instituciones de Tecnología Financiera establece la obligación para las entidades financieras, transmisores de dinero y las sociedades autorizadas para operar con Modelos Novedosos, de intercambiar datos a través del uso de interfaces de programación de aplicaciones estandarizadas a efecto de fomentar la competencia en los mercados, así como la inclusión financiera, al tiempo de facultar a la Comisión Nacional Bancaria y de Valores para emitir disposiciones de carácter general en dicha materia;

Que procurando que el intercambio de información se realice de una forma adecuada, transparente y equitativa, se establece el procedimiento para la autorización y registro de las contraprestaciones a cobrar por el uso de las interfaces de programación de aplicaciones estandarizadas;

Que tomando en cuenta que los datos financieros abiertos no contienen información de la considerada como confidencial, pues se trata de aquella de productos y servicios que se ofrecen al público en general, de la ubicación de oficinas y sucursales, así como de información de cajeros automáticos, entre otra; el compartirla libremente, no constituye un riesgo para quienes la generan;

Que con la finalidad de establecer formas de cumplimiento más sencillas que las previstas en la Ley, así como para evitar la creación de trámites innecesarios que representen costos adicionales a los destinatarios de la norma, se prevé una manera más expedita de obtener, de la Comisión Nacional Bancaria y de Valores, la autorización para acceder a los datos financieros abiertos a través de interfaces de programación de aplicaciones informáticas estandarizadas;

Que en ejercicio de la facultad a que alude el artículo 76 ya citado de la Ley para Regular las Instituciones de Tecnología Financiera y con el objeto de permitir que, ante algún incumplimiento por parte de las entidades financieras, transmisores de dinero y sociedades autorizadas para operar con Modelos Novedosos, se siga intercambiando la información a través de las interfaces de programación de aplicaciones estandarizadas, resulta indispensable normar los requisitos de los programas de regularización que deberán observarse en caso de incumplimientos; ha resuelto expedir las siguientes:

DISPOSICIONES DE CARÁCTER GENERAL RELATIVAS A LAS INTERFACES DE PROGRAMACIÓN DE APLICACIONES INFORMÁTICAS ESTANDARIZADAS A QUE HACE REFERENCIA LA LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGÍA FINANCIERA

Capítulo I
Disposiciones comunes

Artículo 1.- Para efectos de las presentes disposiciones, en adición a las definiciones previstas en la Ley, se entenderá, en singular o plural, por:

I. API, por sus siglas en inglés (*Application Programming Interface)*, a las interfaces de programación de aplicaciones informáticas estandarizadas que posibilitan el intercambio de Datos.

II. Autenticación, al conjunto de técnicas y procedimientos utilizados por el Proveedor de Datos para verificar la identidad de un Solicitante de Datos y su condición para acceder a los Datos disponibles a través de APIs.

III. Datos, a los datos abiertos a que hace referencia la fracción I del artículo 76 de la Ley.

IV. Evento de Seguridad de la Información, a cualquier suceso, interno o externo, relacionado con Clientes, terceros contratados por los Solicitantes de Datos o Proveedores de Datos, personas o procesos operativos, así como con componentes de la Infraestructura, u otros elementos que almacenen información, entre otros, que pueda suponer una afectación en la confidencialidad, integridad o disponibilidad de la información que dicho Proveedor de Datos o Solicitante de Datos gestione o conozca, o en la propia Infraestructura.

V. Incidente de Seguridad de la Información, al Evento de Seguridad de la Información del Proveedor de Datos cuando se actualice alguno de los siguientes supuestos:

   a) Haya comprometido la confidencialidad, integridad o disponibilidad de uno o más componentes de la Infraestructura utilizada por un Solicitante de Datos o Proveedor de Datos, o bien, de los Datos que se envíen o reciban a través de dicha Infraestructura, con un efecto adverso para cualquiera de ellos, o bien, para terceros contratados por el Proveedor de Datos para administrar o desarrollar APIs, entre otros.

b) Vulnere la Infraestructura, comprometiendo los Datos que procesa, almacena o transmite.

c) Constituya una violación de las políticas y procedimientos de seguridad a que hace referencia el artículo 5 de las presentes disposiciones.

d) Constituya la materialización de un menoscabo, ya sea por extracción, alteración o extravío de la información; por fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información; por accesos no autorizados que deriven en el uso indebido de la información o de los sistemas; por fraude, robo o en interrupción de los servicios, atentados contra las infraestructuras interconectadas, conocidos como ciberataques.

VI. Infraestructura, a 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 los Solicitantes de Datos o Proveedores de Datos para soportar la operación de las APIs.

VII. Ley, a la Ley para Regular las Instituciones de Tecnología Financiera.

VIII. Proveedores de Datos, a las Entidades Financieras, ITF, sociedades autorizadas por la CNBV para operar con Modelos Novedosos y transmisores de dinero, que conforme al primer párrafo del artículo 76 de la Ley, estén obligados a establecer APIs con el fin de compartir Datos.

IX. Solicitantes de Datos, a las Entidades Financieras, ITF, sociedades autorizadas para operar con Modelos Novedosos, transmisores de dinero y terceros especializados en tecnologías de información.

X. Usuarios, a las personas que utilicen los productos o servicios que ofrezcan los Solicitantes de Datos.

Capítulo II
De los Solicitantes de Datos

Artículo 2.- Los Solicitantes de Datos cuyas APIs desarrolladas o administradas por estos cumplan con lo establecido en los Anexos 1, 2 y 3 de las presentes disposiciones, se tendrán por autorizados por la CNBV, sin necesidad de declaración alguna, para acceder a los Datos de los distintos Proveedores de Datos a los que solicite su acceso a través de dichas APIs.

Capítulo III
De los Proveedores de Datos

Artículo 3.- Los Proveedores de Datos en el desarrollo o administración de sus APIs deberán cumplir con los Anexos 1, 2 y 3 de las presentes disposiciones.

Los Proveedores de Datos publicarán, de forma clara, precisa y en idioma español, en su página de Internet o cualquier otro medio de comunicación electrónica, aplicaciones informáticas o digitales, el proceso que deberán seguir los Solicitantes de Datos para acceder a los Datos a través de APIs y las contraprestaciones que, en su caso, deberán pagar por el intercambio de Datos.

Los términos y condiciones que establezcan los Proveedores de Datos con los Solicitantes de Datos para llevar a cabo el intercambio de Datos a través de APIs, 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.

Artículo 4.- Los Proveedores de Datos deberán contar con una política de seguridad de la información que proteja en todo momento la Infraestructura, propia o de terceros contratados por estos, así como la confidencialidad e integridad de los Datos que, en su caso, compartan a través de APIs. La mencionada política de seguridad deberá contener procedimientos continuos, mecanismos y controles considerando, al menos, lo siguiente:

I. Configuración segura de los componentes tecnológicos de su Infraestructura, incluyendo, entre otros, cierre de puertos y servicios, instalación de mecanismos para detección y prevención de virus, códigos maliciosos y detección de intrusos, así como actualizaciones del fabricante.

II. Mecanismos de identificación y autenticación del personal responsable del manejo de APIs 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.

III. Cifrado de la información almacenada y de los canales a través de los que se envíen los Datos, así como mecanismos de identificación y autenticación, que cumplan con los Anexos 1 y 2 de las presentes disposiciones.

IV. Procesos de gestión para la atención de Incidentes de Seguridad de la Información que se presenten en la operación de las APIs, que aseguren la detección, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, solución, seguimiento y reporte a la CNBV a que hace referencia el artículo 6 de estas disposiciones.

V. Programa de pruebas de escaneo de vulnerabilidades y amenazas en el acceso y administración de las APIs, el cual podrá ser realizado por un tercero. El mencionado programa deberá considerar la realización de dichas pruebas al menos una vez cada 3 meses, así como con un plan de remediación para las vulnerabilidades críticas detectadas.

VI. Programa de pruebas de penetración, el cual establezca que se realizarán al menos dos pruebas al año sobre sistemas y aplicativos que estén relacionados o conectados con APIs, o bien, cuando lo ordene la CNBV. Dichas pruebas se deberán realizar por un tercero independiente que cuente con personal con capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia. Asimismo, se deberá contar con un plan de remediación para las vulnerabilidades críticas detectadas.

VII. Mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación.

VIII. Registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por el Solicitante de Datos con la información obtenida. La información a que se refiere el presente numeral deberá conservarse por, al menos, un año.

Tratándose de Proveedores de Datos cuyo régimen normativo establezca disposiciones en materia de seguridad de la información, lo previsto en este artículo deberá ser incorporado en las políticas y procedimientos que deban establecer conforme a dicho régimen.

Artículo 5.- Los Proveedores de Datos, deberán asegurar que su Infraestructura para compartir Datos por medio de APIs cumpla con lo siguiente:

I. Contar con una configuración que garantice que el acceso a los Datos compartidos sea solamente de lectura.

II. Que la Infraestructura se encuentre segregada de aquella que soporte cualquier operación y que cuente con mecanismos de seguridad que limiten el acceso desde el servicio de APIs hacia este último, 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 responsable del manejo de APIs.

III. Cuenten con procedimientos que garanticen la disponibilidad del servicio relacionado con el intercambio de Datos.

IV. Registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada en la Infraestructura.

Artículo 6.- 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 y, a través del correo electrónico ciberseguridad-cnbv@cnbv.gob.mx. En dicha notificación se deberá indicar, al menos, la fecha y hora de inicio del Incidente de Seguridad de la Información de que se trate y, en su caso, la indicación de si continúa o ha concluido y su duración; una descripción de dicho incidente, así como una evaluación del mismo.

Artículo 7.- Los Proveedores de Datos, en los casos en que interrumpan el acceso de información por el incumplimiento del Solicitante de Datos a los términos y condiciones pactados para el intercambio de Datos, deberán notificarlo, vía correo electrónico, a la dirección general de la CNBV encargada de su supervisión. En dicha notificación se deberán señalar las razones que justifiquen la interrupción del acceso a la información y los supuestos de incumplimiento a los términos y condiciones pactados, adjuntando la evidencia de tales incumplimientos.

Artículo 8.- Los Proveedores de Datos deberán presentar ante la CNBV, para su autorización, registro y, en su caso, modificación, las contraprestaciones que pretendan cobrar a los Solicitantes de Datos por el intercambio de Datos, debiendo proporcionar, por cada tipo de API, el método, la información y las variables empleadas para determinar las contraprestaciones, así como cualquier otra consideración utilizada en tal determinación.

Los Proveedores de Datos para efectos de realizar el registro de las contraprestaciones, deberán presentar la siguiente información:

I. Nombre, denominación o razón social, sin abreviaturas.

II. En su caso, nombre comercial.

III. Registro Federal de Contribuyentes.

IV. Nombre de la API a la cual aplicará la contraprestación.

V. Descripción del método empleado para determinar la contraprestación.

VI. Monto de la contraprestación, en moneda nacional.

VII. Número telefónico de las personas encargadas de implementar la API.

VIII. Correo electrónico de las personas encargadas de implementar la API.

IX. Periodicidad con la que la contraprestación será exigible, o bien, algún otro parámetro utilizado.

El procedimiento para la autorización de las contraprestaciones, así como para su incremento o reducción, se ajustará a lo establecido en el artículo 76 de la Ley.

Capítulo IV
De los programas de regularización

Artículo 9.- Las Entidades Financieras, las ITF, las sociedades autorizadas por la CNBV para operar con Modelos Novedosos y los transmisores de dinero, en el supuesto previsto en el párrafo décimo segundo del artículo 76 de la Ley y al ejercer su derecho de audiencia, podrán presentar, para aprobación de la CNBV, un programa de regularización, el cual deberá contemplar, cuando menos, los requisitos siguientes:

I. Señalar las acciones que habrán de implementar para observar las obligaciones previstas en las presentes disposiciones que hayan incumplido.

II. Especificar las etapas y plazos de cada una de las acciones a implementar, así como las personas responsables de llevar a cabo tales acciones. En ningún caso la ejecución y cumplimiento del programa de regularización deberá exceder de 3 meses contados a partir de su autorización.

III. Las medidas tendientes a prevenir nuevos incumplimientos.

La CNBV tendrá 20 días hábiles, contados a partir de que reciba el programa de regularización respectivo, para resolver al respecto. La CNBV podrá prevenir al interesado, por una sola ocasión y dentro de los 10 días hábiles al plazo que tiene para resolver, de la falta de requisitos en el contenido del programa o para solicitar mayor información; por lo que, en estos casos, se ampliará por 5 días hábiles más, el plazo para que la CNBV resuelva lo conducente.

El interesado tendrá 5 días hábiles contados a partir de que reciba la prevención de la CNBV, para atender el requerimiento de información; de lo contrario, la CNBV resolverá con la información con la que cuente.

TRANSITORIO

ÚNICO. - Las presentes disposiciones entrarán en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.