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

Publicadas en el Diario Oficial de la Federación el 28 de enero de 2021.

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 26 de diciembre de 2017, modificó las Disposiciones de carácter general aplicables a las instituciones de crédito, para flexibilizar el plazo al que estaban sujetas las instituciones de banca múltiple para constituir sus requerimientos de capital por riesgo operacional;

Que el 9 de marzo de 2018 fue publicado 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 con Recursos de Procedencia Ilícita";

Que la Ley para Regular las Instituciones de Tecnología Financiera incorpora. En el marco del sistema financiero nacional, a las instituciones de tecnología financiera, al tiempo que faculta al Banco de México y a la Comisión Nacional Bancaria y de Valores para emitir, de manera conjunta, las disposiciones de carácter general que deberán observar las instituciones de fondos de pago electrónico, las cuales se regirán bajo los principios de inclusión e innovación financiera, promoción de la competencia, protección al consumidor, preservación de la estabilidad financiera y neutralidad tecnológica;

Que, a fin de contar con una regulación adecuada para las instituciones de fondos de pago electrónico y en atención a los principios señalados en el Considerando inmediato anterior, se emiten las presentes disposiciones de carácter general como un marco normativo unificado, sistemático, coherente y claro que otorgue certeza jurídica a los participantes del mercado de tecnología financiera, fomente el crecimiento de las instituciones de fondos de pago electrónico y salvaguarde los intereses de los clientes de estas instituciones y del sistema financiero en su conjunto;

Que, para garantizar la seguridad de las operaciones celebradas con los clientes, se establecen los requisitos que deberán reunir la autenticación del propio cliente y notificación que a este se realice al momento de pactar o celebrar dichas operaciones, así como los términos y condiciones de la prestación de servicios a través de los canales de instrucción, al mismo tiempo que se establecen los requerimientos de seguridad de la información respecto de dichos canales de instrucción con el fin de garantizar la confidencialidad y evitar vulnerabilidades, de conformidad con las mejores prácticas y estándares internacionales;

Que, para salvaguardar la secuencia en las actividades y operaciones que llevan a cabo las instituciones de fondos de pago electrónico, resulta indispensable establecer la obligación de contar con un plan de continuidad de negocio que deberán implementar ante la verificación de cualquier evento que les dificulte, impida o limite realizar sus operaciones o procesos con afectación para sus clientes ante la eventualidad de que se presenten fallas por situaciones o eventos no previstos, lo cual se robustece con la obligación de tener mecanismos para la administración de contingencias operativas que reduzcan los riesgos a que están expuestas, tales como la designación de la persona responsable de la administración de contingencias y las certificaciones necesarias en la materia cuando las referidas instituciones financieras contraten los servicios de terceros para soportar su operación;

Que, tratándose de aquellas instituciones de fondos de pago electrónico que cuenten con un mayor volumen de cuentas o de operaciones y realicen sus procesos principales por medio de cómputo en la nube prestado por un tercero, resulta necesario que estas incluyan en sus respectivos planes de continuidad medidas especiales por razones prudenciales, con el fin de proteger los intereses de sus clientes, así como de mantener la seguridad e integridad operativa y financiera de dichas instituciones en lo individual, y la seguridad e integridad operativa del sistema de pagos en su conjunto, sin perjuicio de cualesquier otras medidas impuestas por las presentes y demás disposiciones aplicables;

Que, en protección de los intereses de los clientes de las instituciones de fondos de pago electrónico, resulta necesario establecer la obligación para estas instituciones de notificar a sus clientes la existencia de incidentes de seguridad de la información en los que se involucre la pérdida, extracción, eliminación o alteración de información personal o de información sensible de estos, ya sea que se encuentre en posesión de las propias instituciones de fondos de pago electrónico o de terceros que les presten servicios, señalando al efecto los plazos y términos de dicha notificación, las medidas que se implementarán para salvaguardar la información de los clientes y, en su caso, la reposición o sustitución de los medios de disposición o factores de autenticación que las propias instituciones de fondos de pago electrónico consideren necesario realizar;

Que, con el propósito de que los clientes tengan conocimiento del grado de eficiencia operativa que tienen las instituciones de fondos de pago electrónico con las que celebran operaciones, se considera relevante establecer que estas entidades financieras deberán hacer del conocimiento de la Comisión Nacional Bancaria y de Valores y del Banco de México aquellas contingencias operativas con una duración de, al menos 30 minutos, suscitadas en cualquiera de los canales de atención al público o al interior de la propia institución de fondos de pago electrónico, al mismo tiempo que se precisan los elementos que debe reunir dicha comunicación y el plazo en que deberá efectuarse una vez que la contingencia operativa de que se trate tenga lugar; aunado a lo anterior y en protección a los intereses de sus clientes o usuarios de medios de disposición, se establecen los elementos mínimos de la notificación que deberán realizar estas entidades financieras cuando se afecten uno o más canales de instrucción, como consecuencia de estas contingencias operativas;

Que, a fin de procurar una mayor certeza y seguridad jurídica a las operaciones de las instituciones de fondos de pago electrónico y con ello proteger los intereses de sus clientes, se considera indispensable señalar los términos y requisitos que deberán observar estas instituciones de tecnología financiera para contratar servicios con terceros y para celebrar comisiones mercantiles, estableciendo los supuestos en los que requerirá de la autorización de la Comisión Nacional Bancaria y de Valores y del Banco de México, para la celebración de dichos contratos;

Que, en aras de contar con transparencia en la información generada con motivo de las relaciones que las instituciones de fondos de pago electrónico tienen con terceros, se especifican las características del padrón de todos sus prestadores de servicios, incluyendo a los proveedores subcontratados por estos, así como a los administradores de comisionistas y comisionistas, con los cuales las instituciones de fondos de pago electrónico tengan celebrados contratos de prestación de servicios o comisiones mercantiles, previéndose también la difusión que darán estas instituciones financieras, a través de su página de Internet o aplicación móvil, del listado de los módulos o establecimientos de los comisionistas, en el cual indicarán las operaciones y los montos de operación permitidos, y

Que, a fin de contar con información financiera transparente, confiable y comparable, en beneficio de las propias instituciones de fondos de pago electrónico, de sus clientes y de las funciones de supervisión propias del Banco de México y de la Comisión Nacional Bancaria y de Valores, se establece que estas instituciones financieras deberán contratar los servicios de un tercero independiente para la evaluación del cumplimiento de los requerimientos de seguridad de la información, el uso de canales de instrucción y la continuidad operativa que deberán observar, señalando las características que debe reunir dicho tercero independiente; por lo que han resuelto expedir las siguientes:

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

CAPÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO II
DE LA SEGURIDAD DE LA INFORMACIÓN

Sección Primera
De la Infraestructura Tecnológica frente a los Clientes

Apartado A
De la celebración de contratos mediante Canales de Instrucción y las Operaciones a través de estos

Apartado B
De la Autenticación en los Canales de Instrucción

Apartado C
De los requerimientos de seguridad de información en los Canales de Instrucción

Sección Segunda
De la Infraestructura Tecnológica en los procesos internos

Sección Tercera
Disposiciones generales para la Infraestructura Tecnológica

CAPÍTULO III
DE LA CONTINUIDAD OPERATIVA

CAPÍTULO IV
DISPOSICIONES COMUNES DE SEGURIDAD DE INFORMACIÓN Y DE CONTINUIDAD OPERATIVA

CAPÍTULO V
DE LA CONTRATACIÓN DE SERVICIOS CON TERCEROS Y COMISIONISTAS

CAPÍTULO VI
DE LA EVALUACIÓN A TRAVÉS TERCEROS INDEPENDIENTES

CAPÍTULO VII
DISPOSICIONES COMPLEMENTARIAS

ANEXO 1 Indicadores de seguridad de la información.

ANEXO 2 Requerimientos mínimos para desarrollar el Plan de Continuidad de Negocio.

ANEXO 3 Incidentes en materia de seguridad de la información.

ANEXO 4 Informe de Incidentes de Seguridad de la Información.

ANEXO 5 Reporte en materia de Contingencias Operativas.

ANEXO 6 Características de Terceros Independientes.

ANEXO 7 Requerimientos técnicos para realizar Operaciones a través de comisionistas.

ANEXO 8 Especificaciones del sistema de información desarrollado por un tercero para el cifrado de información compartida con la Comisión Nacional Bancaria y de Valores y el Banco de México.

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Para efectos de las presentes Disposiciones, se entenderá, en singular o plural, además de los términos utilizados en la Ley para Regular las Instituciones de Tecnología Financiera, los siguientes:

Administrador de Comisionistas:	a la persona que, en términos del artículo 46 de estas Disposiciones, organiza una red de comisionistas y funge como intermediario entre estos y la institución de fondos de pago electrónico, para que dichos comisionistas celebren con los Clientes Operaciones y servicios.
Autenticación:	a la verificación de la identidad de (i) un Cliente, con el fin de permitirle la realización de las Operaciones que este requiera, o bien, (ii) un Usuario de la Infraestructura Tecnológica de la institución de fondos de pago electrónico de que se trate, con el fin de que aquel pueda acceder, utilizar u operar algún componente de dicha Infraestructura Tecnológica.
Canales de Instrucción:	a los equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones que forman parte de la Infraestructura Tecnológica de la institución de fondos de pago electrónico de que se trate y que, a través de ellos, esta permite al Cliente realizar Operaciones.
Cifrado:	al mecanismo que deberán utilizar las instituciones de fondos de pago electrónico para proteger la confidencialidad de la información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.
Cómputo en la Nube:	al modelo de servicios de cómputo prestados por un tercero, bajo demanda y en infraestructura compartida, privada o híbrida, independientemente de la ubicación física de la Infraestructura Tecnológica del tercero, que puede consistir, entre otros, en uno o más de los siguientes esquemas de servicios digitales: de infraestructura como servicio, de plataforma como servicio o de software como servicio.
Contingencia Operativa:	a cualquier evento que dificulte, limite o impida a una institución de fondos de pago electrónico realizar sus Operaciones, o aquellos procesos que pudieran tener una afectación a sus Clientes o a la propia institución de fondos de pago electrónico.
Cuenta:	a aquel registro contable en el que la institución de fondos de pago electrónico realiza, entre otros, las anotaciones de (a) abonos correspondientes a (i) la cantidad de fondos de pago electrónico que aquella emita a favor del Cliente a nombre de quien haya abierto dicho registro, de conformidad con el artículo 22, fracción I de la Ley, contra la recepción de una cantidad de dinero, en moneda nacional, o sujeto a la autorización del Banco de México,

en moneda extranjera, objeto de una Transferencia de Fondos, Transmisión de Dinero, por recepción de efectivo u operaciones con Tarjeta; (ii) la cantidad de fondos de pago electrónico objeto de las Transferencias de Fondos de Pago Electrónico que reciba a favor de dicho Cliente, así como (b) cargos que correspondan por (i) la disposición de fondos de pago electrónico con motivo de su redención, objeto de una Transferencia de Fondos, operaciones de pago con cualquier tipo de medio de disposición que la institución de fondos de pago electrónico haya permitido a su cliente realizar, domiciliaciones, Transmisión de Dinero, o la entrega de efectivo; (ii) la cantidad de fondos de pago electrónico objeto de las Transferencias de Fondos de Pago Electrónico de que se trate.

Evento de Seguridad de la Información: a cualquier suceso, interno o externo, relacionado, entre otros, con Clientes, terceros contratados por la institución de fondos de pago electrónico, personas o procesos operativos, así como con componentes de la Infraestructura Tecnológica, dispositivos, medios físicos, u otros elementos que almacenen información, que constituya algún indicio de la posible afectación en la confidencialidad, integridad o disponibilidad de la información que dicha institución gestione o a la cual tenga acceso en la propia Infraestructura Tecnológica.

Factor de Autenticación: al mecanismo de Autenticación, basado en las características físicas del Cliente, en dispositivos o información que solo el Cliente posea o conozca, conforme a lo previsto en el artículo 5 de las presentes Disposiciones.

Identificador de Cliente: a la cadena de caracteres alfanuméricos, o la información de un dispositivo, o cualquier otra información que conozca, tanto la institución de fondos de pago electrónico, como el Cliente titular de la respectiva Cuenta que esta administre, que permita identificarlo por medio del Canal de Instrucción de dicha institución de fondos de pago electrónico. Entre otros, el Identificador de Cliente podrá ser el número de la línea del teléfono móvil que el Cliente utilice para acceder a los Canales de Instrucción, la dirección de correo electrónico, el número de su Tarjeta u otro identificador único asociado al uso del Canal de Instrucción correspondiente.

Incidente de Seguridad de Información: a cualquier suceso, interno o externo, relacionado, entre otros, con Clientes, terceros contratados por la institución de fondos de pago electrónico, personas y procesos operativos, así como con componentes de la Infraestructura Tecnológica, dispositivos, medios físicos u otros elementos que almacenen información, que:

a) Comprometa la confidencialidad, integridad o disponibilidad de uno o más componentes de la Infraestructura Tecnológica con un efecto adverso para la institución de fondos de pago electrónico, sus Clientes, terceros, proveedores o contrapartes, entre otros.

b) Vulnere la Infraestructura Tecnológica de tal forma que comprometa la información que procesa, almacena o transmite.

c) Constituya una violación de las políticas y procedimientos de seguridad de la información.

d) Constituya la materialización de un menoscabo en la institución de fondos de pago electrónico, 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 o robo; por una interrupción de las actividades realizadas por la propia institución ocasionada por alguna acción; o por atentados contra las infraestructuras interconectadas conocidos como ciberataques.

Información Personal: a la conjunción del nombre, apellidos y otro elemento de información que permita identificar al Cliente o al receptor de Transferencias, tales como domicilio, números de teléfono o direcciones de correo electrónico, entre otros.

Información Sensible: a la conjunción del nombre, apellidos u otro elemento de información que permita identificar al Cliente o al receptor de Transferencias, así como la información del Identificador del Cliente, de las Cuentas, de los números de las Tarjetas respectivas, de la información de Operaciones previas, así como información que permita la Autenticación y demás datos de naturaleza financiera.

Órgano de Administración: al administrador único o al consejo de administración de una institución de fondos de pago electrónico, según sea el caso.

Plan de Continuidad de Negocio: al documento que integra el conjunto de estrategias, procedimientos y acciones previamente determinadas por la institución de fondos de pago electrónico que corresponda, para permitir, ante la ocurrencia de Contingencias Operativas, la continuidad en las Operaciones, actividades o en la realización de los procesos críticos de dicha institución de fondos de pago electrónico, o bien, su restablecimiento oportuno, así como la mitigación de las afectaciones producto de dichas Contingencias Operativas.

Plan Director de Seguridad: al documento que integra el conjunto de proyectos determinados por la institución de fondos de pago electrónico que corresponda, que deban ser ejecutados a corto, mediano y largo plazo, para establecer una correcta gestión de seguridad de la información y evitar que los Eventos de Seguridad de Información se materialicen en Incidentes de Seguridad de Información.

Política Estratégica de Continuidad de Negocio y de Seguridad de la Información: al documento que integra las estrategias de la institución de fondos de pago electrónico en materia de continuidad de negocio y seguridad de la información relacionadas con su operación de conformidad con las presentes Disposiciones, sin perjuicio de cualquier otro elemento en materia de administración de riesgos sujeto a las disposiciones de carácter general que, al efecto, emita la CNBV de conformidad con el artículo 48 de la Ley para Regular las Instituciones de Tecnología Financiera.

Sesión: al periodo en el cual el Cliente, titular de una Cuenta que administre la institución de fondos de pago electrónico, podrá

	llevar a cabo consultas de saldos o de sus Operaciones realizadas o iniciar otras, una vez que haya ingresado al Canal de Instrucción con su Identificador del Cliente.
Tarjeta:	al medio de disposición de los fondos de pago electrónico registrados en la Cuenta de que se trate, constituido como el conjunto de datos que, al procesarse mediante sistemas determinados, permiten iniciar una instrucción de cargo a dicha Cuenta, distinta a aquella otra instrucción que se realice para ejecutar una Transferencia.
Tercero Independiente:	al profesionista competente para realizar labores de evaluación sobre el cumplimiento de los requisitos que las instituciones de fondos de pago electrónico deben cumplir conforme a estas Disposiciones, quien es externo a la institución de fondos de pago electrónico y que cumple, en lo conducente, con las características y requisitos previstos en el artículo 58 de estas Disposiciones.
Transferencia:	a las Transferencias de Fondos, Transferencias de Fondos de Pago Electrónico y Transmisiones de Dinero, indistinta o conjuntamente.
Transferencia de Fondos:	a aquella Operación a que se refiere el artículo 22, fracción III de la Ley para Regular las Instituciones de Tecnología Financiera realizada entre la institución de fondos de pago electrónico de que se trate y otra institución de fondos de pago electrónico, Entidad Financiera, entidad financiera del exterior o institución de fondos de pago electrónico del exterior, conforme al cual la primera realiza (i) el abono en una Cuenta por la cantidad equivalente de dinero a la indicada en la orden respectiva que reciba, derivada del cargo que esa otra institución de fondos de pago electrónico o entidad haga en la cuenta correspondiente, o bien (ii) el cargo en una Cuenta equivalente a aquella cantidad de dinero que el Cliente haya indicado en la orden que emita para que, una vez realizada la redención de los referidos fondos, dicha cantidad se acredite a favor de la otra institución de fondos de pago electrónico o entidad a quien se envíe dicha orden para su abono en la cuenta de depósito indicada en la propia orden. Para efectos de la presente definición se entenderá como instituciones de fondos de pago electrónico del exterior a las personas morales ubicadas fuera de territorio nacional que, conforme a la legislación aplicable en la jurisdicción de que se trate, realicen actividades similares a las de emisión, administración, redención y transmisión de instrumentos equivalentes a fondos de pago electrónico.
Transferencia de Fondos de Pago Electrónico:	a aquella Operación a que se refiere el artículo 22, fracción II de la Ley para Regular las Instituciones de Tecnología Financiera, realizada por una misma institución de fondos de pago electrónico de conformidad con los contratos celebrados con sus Clientes para la apertura de Cuentas, de acuerdo con la cual dicha institución abona una cantidad determinada de fondos de pago electrónico en una de dichas Cuentas, derivado del cargo por la referida cantidad en alguna otra de esas Cuentas.
Transmisión de Dinero:	a aquella Operación a que se refiere el artículo 25, fracción II de la Ley para Regular las Instituciones de Tecnología Financiera que realice la institución de fondos de pago electrónico autorizada para ello.

UDI:	a las unidades de cuenta llamadas "Unidades de Inversión" establecidas en el "Decreto por el que se establecen las obligaciones que podrán denominarse en Unidades de Inversión y reforma y adiciona diversas disposiciones del Código Fiscal de la Federación y de la Ley del Impuesto sobre la Renta", publicado en el Diario Oficial de la Federación el 1 de abril de 1995, tal como ese sea modificado o adicionado de tiempo en tiempo.
Usuario de la Infraestructura Tecnológica:	a la persona o componente de la Infraestructura Tecnológica de la institución de fondos de pago electrónico, que cuente con la autorización respectiva para que acceda, utilice u opere algún componente de esta. No quedarán comprendidos en esta definición los Clientes de la institución de fondos de pago electrónico.

CAPÍTULO II
DE LA SEGURIDAD DE LA INFORMACIÓN

Sección Primera
De la Infraestructura Tecnológica frente a los Clientes

Apartado A
De la celebración de contratos mediante Canales de Instrucción y las Operaciones a través de estos

Artículo 2.- Las instituciones de fondos de pago electrónico, al pactar la celebración de Operaciones y la prestación de servicios a través de Canales de Instrucción, deberán requerir el consentimiento expreso de sus Clientes para dichos efectos, el cual se podrá obtener a través del proceso de Autenticación referido en el artículo 7 de las presentes Disposiciones. Adicionalmente, las instituciones de fondos de pago electrónico deberán:

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

   a) Las Operaciones y servicios que podrán realizar y proporcionar a través de dichos Canales de Instrucción.

   b) Los mecanismos y procedimientos para la Autenticación del Cliente, así como las responsabilidades de este y de la institución de fondos de pago electrónico respecto de la celebración de Operaciones y la prestación de servicios a través del Canal de Instrucción respectivo.

   c) Los mecanismos y procedimientos para la notificación al Cliente de las Operaciones realizadas y servicios prestados por las instituciones de fondos de pago electrónico a través de los Canales de Instrucción.

   d) Los mecanismos y procedimientos de cancelación de la contratación de servicios, los cuales deberán ser similares a los de la propia contratación, considerando los canales de atención al Cliente, Mecanismos de Identificación del Cliente y procedimientos para su Autenticación.

   e) Las restricciones operativas aplicables de acuerdo con el Canal de Instrucción de que se trate, de conformidad con lo previsto en este Capítulo.

II. Informar a sus Clientes, previamente a la contratación, los términos y condiciones para el uso de los Canales de Instrucción, debiendo mantener dicha información disponible para su consulta en cualquier momento.

III. Informar a sus Clientes los riesgos inherentes a la utilización de los Canales de Instrucción respectivos, así como hacer de su conocimiento sugerencias para prevenir la realización de actos

no autorizados por ellos o cualesquier otros irregulares o ilegales, por los que se puedan llevar a cabo Operaciones referidas a las Cuentas de las que estos sean titulares.

Artículo 3.- Las instituciones de fondos de pago electrónico, en relación con los Canales de Instrucción, podrán:

I. Permitir a sus Clientes la contratación de Operaciones y servicios adicionales a los originalmente convenidos.

II. Modificar los términos y condiciones para la prestación de los servicios anteriormente convenidos que puedan tener una afectación financiera para sus Clientes, previo consentimiento expreso de estos, el cual podrá obtenerse por dichas instituciones a través del proceso de Autenticación referido en el artículo 7 de las presentes Disposiciones, desde el Canal de Instrucción de que se trate.

III. Permitir a sus Clientes contratar el uso de otro Canal de Instrucción, siempre y cuando la institución de fondos de pago electrónico requiera para ello, al menos, un Factor de Autenticación.

Artículo 4.- Las instituciones de fondos de pago electrónico deberán notificar a sus respectivos Clientes, por los medios pactados con ellos y en un periodo no mayor a cinco segundos, cuando a través de Canales de Instrucción, se ejecute cualquiera de las Operaciones que a continuación se indican o se solicite a las instituciones de fondos de pago electrónico alguno de los servicios siguientes:

I. Transferencias y entrega de cantidades de dinero derivado del cargo a la Cuenta del Cliente de que se trate, a partir de que el monto acumulado diario de las Operaciones realizadas supere el equivalente en moneda nacional a 60 UDI's, o bien, cuando cada una en lo individual supere el equivalente en moneda nacional a 25 UDI's.

II. Alta o modificación del medio de notificación al Cliente, en cuyo caso la institución de fondos de pago electrónico respectiva deberá enviar la notificación a que este artículo se refiere por el medio previamente pactado con el Cliente, así como por el nuevo medio.

III. Contratación de otro servicio provisto a través de Canales de Instrucción.

IV. Desactivación, bloqueo, reactivación y modificación de los Factores de Autenticación.

Las instituciones de fondos de pago electrónico deberán asegurarse de que la notificación que al efecto envíen conforme a este artículo, no contenga Información Personal o Información Sensible del Cliente. No obstante, las instituciones de fondos de pago electrónico deberán habilitar mecanismos para que sus Clientes puedan, a su elección, recibir la información del saldo de la Cuenta en virtud de los servicios prestados a través de los Canales de Instrucción.

Para efectos de la notificación a que se refiere el presente artículo, las instituciones de fondos de pago electrónico que emitan medios de disposición, deberán realizar la referida notificación, tanto a sus Clientes, como a los titulares de los medios de disposición emitidos.

Las instituciones de fondos de pago electrónico podrán deshabilitar las notificaciones cuando se ejecuten cualquiera de las Operaciones o servicios previstos en las fracciones I a IV del presente artículo, previa solicitud expresa de sus Clientes que deberá obtenerse por dichas instituciones a través del proceso de Autenticación referido en el artículo 7 de las presentes Disposiciones, y habiendo informado a sus Clientes, de manera previa, los riesgos asociados a dicha deshabilitación.

Apartado B
De la Autenticación en los Canales de Instrucción

Artículo 5.- Para efectos de las presentes Disposiciones, los Factores de Autenticación que deberán utilizar las instituciones de fondos de pago electrónico, solo podrán incluir la información perteneciente a cualquiera de las siguientes categorías:

I. Información que la institución de fondos de pago electrónico proporciona al Cliente o permite a dicho Cliente generar, bajo el entendido de que solamente dicha persona la conozca, para que la pueda ingresar al sistema autorizado por la institución de fondos de pago electrónico, a fin de iniciar Sesión y ejecutar la Operación de que se trate. Los Factores de Autenticación a que se refiere está fracción deberán cumplir con cualquiera de los siguientes esquemas:

a) Contraseñas que cumplan, cuando menos, con lo siguiente:

1. Deberá estar compuesta, al menos, por seis caracteres consecutivos e incluir caracteres alfanuméricos.

2. En ningún caso, se podrá utilizar como contraseñas, la información siguiente:

i) El Identificador de Cliente.

i). La denominación o marca comercial de la institución de fondos de pago electrónico.

ii). Más de tres caracteres idénticos en forma consecutiva.

iv) Más de tres caracteres numéricos o alfabéticos en forma secuencial.

b) Cuestionarios realizados a través de canales electrónicos de mensajería, de centros de atención telefónica o por agentes automatizados, siempre que observen lo siguiente:

1. Se requieran datos que el Cliente conozca y que las instituciones de fondos de pago electrónico puedan validar, manteniendo la debida confidencialidad de dicha información.

2. Se defina un conjunto de preguntas abiertas en cuestionarios de, al menos, tres preguntas y, en el evento de que la respuesta a una de ellas sea incorrecta, se podrá formular una pregunta adicional. Dicho conjunto de preguntas deberá ser único por medio a través del cual se presente el cuestionario, permitiéndose la repetición de solo una pregunta entre todos los medios. Asimismo, se deberán implementar mecanismos de aleatoriedad en la presentación de las preguntas al Cliente.

En ningún caso, las respuestas a estas preguntas podrán ser datos que se muestren en el Canal de Instrucción. Asimismo, la información o datos de la respuesta a dos o más preguntas no podrán ser enviadas por las instituciones de fondos de pago electrónico a sus Clientes, a través del mismo canal de comunicación, ya sea por medios impresos o electrónicos.

3. Se validen las respuestas proporcionadas por sus Clientes a través de herramientas informáticas, sin que el operador o sistema automatizado pueda consultar o acceder a los datos de Autenticación de los Clientes.

Las instituciones de fondos de pago electrónico permitirán a sus Clientes cambiar los Factores de Autenticación de esta categoría, cuando estos últimos así lo requieran, en los términos previstos en las presentes Disposiciones.

Las instituciones de fondos de pago electrónico podrán utilizar cuestionarios para desbloquear los Factores de Autenticación que previamente hayan sido bloqueados, siempre y cuando lo realicen en combinación con un segundo Factor de Autenticación distinto al cuestionario.

II. Información contenida, recibida o generada por medios o dispositivos electrónicos que solo posee el Cliente, incluida la obtenida por dispositivos o aplicativos generadores de contraseñas dinámicas que la institución de fondos de pago electrónico proporcione al Cliente, así como aquella que permita asociar medios o dispositivos electrónicos a un Cliente a través de mecanismos seguros de intercambio de credenciales o llaves criptográficas. Lo anterior, quedará sujeto a que la

información sea contenida, recibida o generada en dichos dispositivos electrónicos que solo posee el Cliente y cumpla con las características siguientes:

a) Contar con propiedades que impidan su duplicación o alteración.

b) Sea información dinámica que no pueda ser utilizada en más de una ocasión con una vigencia que no podrá ser mayor a dos minutos, o se trate de información dinámica generada para la realización de una operación, así como operaciones subsecuentes sin modificación alguna, en cuyo caso será considerada, para efectos del presente inciso, como un elemento independiente para autenticar las operaciones como autorizadas por el Cliente únicamente para la primera operación en que se utilice.

c) No sea conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes de la institución de fondos de pago electrónico o por terceros.

Las instituciones de fondos de pago electrónico podrán proporcionar a sus Clientes medios o dispositivos que generen contraseñas dinámicas de un solo uso que utilicen información de la Operación, mediante la captura de datos, de manera que dicha Contraseña únicamente pueda ser utilizada para la Operación solicitada. En este caso, no será aplicable la vigencia dispuesta en el inciso b) de la presente fracción.

III. Información derivada de características propias del Cliente, tales como aquellas de carácter biométrico, huellas dactilares, geometría de la mano o de la cara, patrones en iris o retina y reconocimiento de voz, entre otros. Para el uso de esta información, las instituciones de fondos de pago electrónico deberán contar con la previa autorización de la CNBV y del Banco de México.

En todo caso, se considerará que dos o más Factores de Autenticación son independientes si la vulneración de uno de los Factores de Autenticación no compromete la fiabilidad de los demás.

Artículo 6.- Las instituciones de fondos de pago electrónico podrán solicitar a la CNBV y al Banco de México que autoricen el uso de Factores de Autenticación referidos en las fracciones I y II del artículo 5 de las presentes Disposiciones con características distintas a las señaladas en dicho artículo, así como la utilización de la información señalada en la fracción III del mencionado artículo, siempre que acrediten que la tecnología utilizada, a juicio de ambas Autoridades Financieras, resulta fiable para autenticar a sus Clientes.

La solicitud para obtener la autorización indicada en el párrafo anterior deberá contener lo siguiente:

I. La descripción detallada del proceso, el cual deberá ser aprobado por el Órgano de Administración, así como la tecnología empleada en cada parte de este.

II. La descripción de los medios necesarios para la transmisión y resguardo de la información que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación, así como su adecuada conservación y disponibilidad.

Para el caso prescrito en la fracción III del artículo 5 de estas Disposiciones, la institución de fondos de pago electrónico que formule la solicitud de autorización a que se refiere el presente artículo, adicionalmente deberá presentar la evidencia recabada de pruebas controladas que demuestren que la solución tecnológica y los métodos utilizados son efectivos para autenticar a sus Clientes. Dicha evidencia podrá ser obtenida por la misma institución de fondos de pago electrónico o por una empresa especializada en certificación de Factores de Autenticación con la capacidad de presentar reportes.

Las instituciones de fondos de pago electrónico deberán contar con mecanismos y procedimientos para asegurar que, en el uso de los Factores de Autenticación a que se refiere la fracción III del artículo 5 de las presentes Disposiciones, la información transmitida para el proceso de Autenticación sea distinta cada vez que sea generada, mediante la incorporación de información adicional, tales como estampas de tiempo, números aleatorios y contadores, entre otros, en el proceso de encriptación del mensaje, de forma que en ningún caso se pueda utilizar nuevamente o duplicarse.

Las instituciones de fondos de pago electrónico deberán presentar las solicitudes de autorización y demás información a que se refiere el presente artículo al Banco de México y a la CNBV, de conformidad con lo establecido en el artículo 59 de estas Disposiciones.

Artículo 7.- Las instituciones de fondos de pago electrónico, a efecto de permitir el acceso a los Canales de Instrucción, deberán llevar a cabo la Autenticación del Cliente. Para realizar dicha Autenticación, las instituciones de fondos de pago electrónico deberán recabar y validar, al menos, lo siguiente:

I. El Identificador de Cliente El Identificador de Cliente y

II. Un Factor de Autenticación.

El Identificador de Cliente deberá ser único para cada Cliente y deberá asociarse a todas las Operaciones realizadas por este último.

Asimismo, las instituciones de fondos de pago electrónico deberán guardar evidencia de la Autenticación, conforme a lo establecido en el artículo 29, fracción IV de las presentes Disposiciones.

Artículo 8.- Las instituciones de fondos de pago electrónico deberán solicitar, al menos, dos Factores de Autenticación independientes en cada ocasión en que se pretenda realizar lo siguiente:

I. Alta, baja o cualquier otra modificación relacionada con los beneficiarios de la Cuenta a que se refiere el séptimo párrafo del artículo 29 de la Ley para Regular las Instituciones de Tecnología Financiera.

II. Cambios respecto de los Factores de Autenticación.

III. Solicitud de estados de cuenta.

IV. Alta y modificación del medio de notificación al Cliente.

Las instituciones de fondos de pago electrónico quedarán sujetas a lo establecido en la Circular 12/2018 emitida por el Banco de México, para el caso en que reciban reclamaciones por cargos no reconocidos de sus Clientes por Operaciones que deriven de alguna de las operaciones descritas en las fracciones I, II y IV del presente artículo.

Para efectos de lo previsto en el presente artículo, las instituciones de fondos de pago electrónico podrán tomar en cuenta el Factor de Autenticación utilizado para el inicio de Sesión en los Canales de Instrucción de que se trate.

Artículo 9.- Las instituciones de fondos de pago electrónico deberán contar con políticas y procedimientos para asegurar que, en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Cliente quien los reciba, active, conozca, desbloquee y restablezca.

Tratándose de contraseñas definidas o generadas por las instituciones de fondos de pago electrónico durante el restablecimiento de los Factores de Autenticación a que se refiere el inciso a) de la fracción I del artículo 5 de estas Disposiciones, las propias instituciones deberán prever mecanismos y procedimientos por medio de los cuales el Cliente deba modificarlas inmediatamente después de iniciar la Sesión correspondiente, cuando así sea requerido según el tipo de Canal de Instrucción y previo a la realización de cualquier Operación, validando que los Factores de Autenticación a que se refiere este párrafo sean diferentes a las contraseñas definidas por las propias instituciones de fondos de pago electrónico.

Apartado C
De los requerimientos de seguridad de información en los Canales de Instrucción

Artículo 10.- Las instituciones de fondos de pago electrónico deberán establecer mecanismos y procedimientos para que sus Clientes, al acceder a los Canales de Instrucción, puedan reconocer a las propias instituciones, para lo cual estas deberán sujetarse a lo siguiente:

I. Proporcionar información personalizada y suficiente para que los Clientes puedan verificar, antes de realizar el procedimiento para su Autenticación, que se trata efectivamente de la institución de fondos de pago electrónico de la cual se es Cliente. Para ello, las instituciones de fondos de pago electrónico podrán utilizar la información siguiente:

   a) Aquella que el Cliente respectivo conozca o haya proporcionado a la institución de fondos de pago electrónico, o bien, que haya convenido con la institución de fondos de pago electrónico para este fin, tales como nombre, alias e imágenes, entre otros.

   b) Aquella que el Cliente respectivo pueda verificar a través de un medio pactado para este fin con la institución de fondos de pago electrónico.

II. Una vez que el Cliente acceda al Canal de Instrucción de que se trate, la institución de fondos de pago electrónico deberá poner a su disposición, al menos, la siguiente información:

   a) Fecha y hora del último acceso al Canal de Instrucción de que se trate y

   b) Nombre y apellido del Cliente.

Lo anterior no será aplicable cuando el Cliente utilice Canales de Instrucción que no requieran una interacción previa para la instrucción de Operaciones, tales como las terminales punto de venta.

Artículo 11.- Las instituciones de fondos de pago electrónico deberán prever lo necesario para que, una vez autenticado el Cliente en el Canal de Instrucción, la Sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las instituciones de fondos de pago electrónico establecerán, al menos, los mecanismos siguientes:

I. Dar por terminada inmediatamente la Sesión en forma automática e informar al Cliente el motivo en cualquiera de los siguientes casos:

   a) Cuando exista inactividad por más de 5 minutos.

   b) Cuando en el curso de una Sesión, la institución de fondos de pago electrónico identifique cambios relevantes en los parámetros de comunicación de dicha Sesión, tales como identificación del Canal de Instrucción, rango de direcciones de los protocolos de comunicación y ubicación geográfica, entre otros, que permitan a la propia institución inferir que pudiera tratarse de un robo de Sesión.

II. Impedir el acceso de forma simultánea en un mismo Canal de Instrucción, mediante la utilización de un mismo Identificador de Cliente y hacerlo del conocimiento del Cliente. Asimismo, las instituciones de fondos de pago electrónico deberán detectar los intentos de acceso al Canal de Instrucción con Factores de Autenticación incorrectos y, en caso de exceder tres intentos de acceso fallidos consecutivos, se deberá restringir temporalmente el acceso al Canal de Instrucción de que se trate, bloqueando el Factor de Autenticación del Cliente por un lapso de diez minutos, debiendo notificar al Cliente sobre dicho bloqueo por los medios pactados previamente con este.

   Transcurridos los diez minutos indicados en el párrafo anterior, el Cliente podrá tener un intento más para acceder al Canal de Instrucción y, en caso de que se ingrese un Factor de Autenticación incorrecto, dicho Factor de Autenticación se bloqueará de manera permanente hasta que el Cliente realice el proceso de desbloqueo al que hace referencia el artículo 9 de estas Disposiciones. La institución de fondos de pago electrónico deberá notificar al Cliente de este bloqueo permanente, a través de los medios pactados entre las partes.

III. En el evento de que las instituciones de fondos de pago electrónico ofrezcan servicios de terceros mediante enlaces, deberán comunicar a sus Clientes que, al momento de ingresar a dichos

servicios, se ingresará a otro enlace cuya seguridad no depende ni es responsabilidad de dicha institución.

En el caso en que la institución de fondos de pago electrónico pretenda establecer parámetros distintos a los establecidos en este artículo, deberá obtener previamente la autorización del Banco de México y de la CNBV. Las solicitudes de dichas autorizaciones deberán presentarse de conformidad con el artículo 59 de las presentes Disposiciones.

Artículo 12.- Las instituciones de fondos de pago electrónico, en el uso del Identificador de Cliente y los Factores de Autenticación, deberán cumplir con los requisitos siguientes:

I. Contar con los mecanismos necesarios para impedir la lectura o presentación en el Canal de Instrucción, de la información proporcionada por el Cliente y utilizada en los Mecanismos de Identificación y Autenticación.

II. Asegurar que, cuando se utilicen al menos dos Factores de Autenticación, estos sean independientes.

III. Contar con procedimientos para restablecer los Factores de Autenticación, de tal manera que no se comprometa la Información Personal o Información Sensible del Cliente.

IV. Contar con procedimientos para invalidar los Factores de Autenticación, a fin de impedir su uso en un servicio provisto por la institución de fondos de pago electrónico, cuando un Cliente o la misma institución de fondos de pago electrónico cancele el uso de dicho servicio o cuando el Cliente respectivo deje de ser Cliente de dicha institución.

Artículo 13.- Las instituciones de fondos de pago electrónico únicamente podrán almacenar información relativa a los Factores de Autenticación utilizados por sus Clientes en los Canales de Instrucción, cuando dicho almacenamiento se realice bajo protocolos criptográficamente seguros y no sea posible que:

I. Se obtenga la información original de los Factores de Autenticación a partir de la información almacenada.

II. Distintos conjuntos de datos generen la misma información almacenada.

Artículo 14.- Las instituciones de fondos de pago electrónico deberán establecer procedimientos y mecanismos para que sus Clientes, que realicen Operaciones o soliciten los servicios de estas a través de Canales de Instrucción, puedan en todo momento desactivar la realización de dichas Operaciones o la prestación de esos servicios de forma temporal, así como establecer procedimientos para reactivar el uso cuando los Clientes lo soliciten.

Las instituciones de fondos de pago electrónico deberán permitir a los Clientes desactivar de manera temporal la realización de las Operaciones y la prestación de los servicios mencionados en el párrafo anterior, a través de los Canales de Instrucción que al efecto hayan convenido con ellos solicitando, al menos, un Factor de Autenticación.

Para la reactivación de la realización de las Operaciones y la prestación de servicios que las instituciones de fondos de pago electrónico presten a través de Canales de Instrucción, dichas instituciones deberán permitir a los Clientes utilizar los Canales de Instrucción que convengan para este fin, para lo cual deberán requerir, al menos, un Factor de Autenticación. Las instituciones de fondos de pago electrónico deberán observar lo señalado en el artículo 7 de estas Disposiciones, a fin de que puedan permitir el acceso al Canal de Instrucción de que se trate una vez que se haya reactivado el servicio.

Sección Segunda
De la Infraestructura Tecnológica en los procesos internos

Artículo 15.- Las instituciones de fondos de pago electrónico, tratándose de componentes de comunicaciones y de cómputo, deberán establecer los aspectos de seguridad siguientes:

I. Segregación lógica, o lógica y física, de las diferentes redes en distintos dominios y subredes, dependiendo de la función que desarrollen o el tipo de datos que se transmitan, incluyendo segregación de los ambientes productivos de los de desarrollo y pruebas, así como componentes de seguridad perimetral y de redes que aseguren que solamente el tráfico autorizado es permitido. En particular, en aquellos segmentos con enlaces al exterior, tales como Internet, proveedores, autoridades, otras redes de la institución de fondos de pago electrónico o matriz y otros terceros, todo ello referido a aquellos servicios definidos como críticos por la propia institución, relacionados, al menos con sistemas de pagos, equipos de Cifrado, o autorizadores de Operaciones, entre otros, deberán considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (referidas como DMZ, por sus siglas en inglés).

II. Configuración segura de acuerdo con el tipo de componente considerando, al menos, puertos y servicios, conexiones entrantes y salientes a otras redes, incluyendo Internet, permisos otorgados bajo el principio de mínimo privilegio, uso de medios extraíbles de almacenamiento, listas de acceso, actualizaciones del fabricante y reconfiguración de parámetros de fábrica. 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 de cada Usuario de la Infraestructura Tecnológica.

III. Mecanismos de seguridad en las aplicaciones que procuren que, durante su ejecución se protejan de ataques o intrusiones, tales como inyección de código, manipulación de la sesión, fuga de información y alteración de privilegios de acceso, entre otros. Dichos mecanismos deberán de ser implementados, tanto para las aplicaciones proporcionadas por terceros, como para las aplicaciones desarrolladas, implementadas y mantenidas por la propia institución de fondos de pago electrónico.

Artículo 16.- Las instituciones de fondos de pago electrónico deberán cifrar la Información Personal y la Información Sensible recibida, generada, almacenada o transmitida en la Infraestructura Tecnológica propia o de terceros contratados, así como las imágenes de documentos de identificación expedidos por autoridades oficiales e información biométrica de los Clientes, y cualquier otra que determinen de acuerdo con sus políticas. En el caso de la Información Sensible, se exceptúa del cifrado la información relativa a las Operaciones, siempre y cuando dicha información esté almacenada en tablas o repositorios distintos a los utilizados para almacenar el resto de la Información Personal e Información Sensible, y se cuente con mecanismos de seguridad que permitan su disociación y eviten el acceso a dicha información, en caso de no estar autorizado para ello.

Los mecanismos y procedimientos para descifrar la información referida en este artículo, así como las claves criptográficas requeridas para tal fin, deberán estar bajo el control exclusivo del oficial en jefe de seguridad de la información de la institución de fondos de pago electrónico de que se trate.

Artículo 17- Las instituciones de fondos de pago electrónico deberán contar con procedimientos y mecanismos que permitan estructurar la Información Personal y la Información Sensible almacenada en la Infraestructura Tecnológica, de tal manera que los datos personales de los Clientes no puedan ser relacionados con la información relativa a sus Operaciones, incluyendo, entre otros, los montos, así como los nombres o denominaciones de los receptores o emisores de los pagos realizados por los Clientes. Esta relación solo podrá ser generada a través de procedimientos o aplicaciones informáticos para la consulta, diseñados por la institución de fondos de pago electrónico, que deberán ser ejecutados a demanda cada vez que sea necesario construir esta relación, ya sea por medio de mecanismos manuales o de los sistemas informáticos.

Artículo 18.- Las instituciones de fondos de pago electrónico, respecto de la información relativa a los Factores de Autenticación deberán cumplir con los requisitos siguientes:

I. Mantener procedimientos de seguridad de información para la custodia, distribución y asignación de los Factores de Autenticación de sus Clientes.

II. Establecer procedimientos y mecanismos con el fin de que la información relativa a los Factores de Autenticación no sea conocida por ninguno de sus funcionarios, empleados o representantes, o por algún tercero.

III. Establecer procedimientos y mecanismos que impidan solicitar a sus Clientes, a través de sus funcionarios, empleados, representantes o terceros, la información parcial o completa relativa a los Factores de Autenticación.

Artículo 19.- Las instituciones de fondos de pago electrónico deberán establecer procedimientos y mecanismos que aseguren que, al desechar o dar de baja componentes de almacenamiento o dispositivos físicos, conocidos como hardware, de la Infraestructura Tecnológica, la información de los Clientes contenida en dichos componentes o dispositivos sea irrecuperable.

Artículo 20.- Las instituciones de fondos de pago electrónico estarán obligadas a utilizar herramientas que permitan detectar virus informáticos y códigos maliciosos en la Infraestructura Tecnológica, así como procedimientos que permitan su actualización periódica.

Artículo 21.- Las instituciones de fondos de pago electrónico deberán realizar, previo al inicio de su operación y al menos cada dos meses, pruebas de escaneo de vulnerabilidades de la totalidad de los componentes de la Infraestructura Tecnológica propia, o de terceros y comisionistas contratados, en la que almacenen, procesen o transmitan información de las instituciones de fondos de pago electrónico y de sus Clientes. Adicionalmente, en caso de presentarse modificaciones o actualizaciones en la Infraestructura Tecnológica, las instituciones de fondos de pago electrónico deberán realizar las pruebas de escaneo de vulnerabilidades sobre los componentes actualizados o modificados, antes de poner en ambiente productivo las modificaciones o actualizaciones mencionadas, debiendo realizar las acciones necesarias para subsanar, cuando menos, las vulnerabilidades clasificadas como críticas y altas. El director general o, en su caso, el administrador único, será responsable de vigilar que dichas pruebas se lleven a cabo, ya sea a través de la propia institución o de un tercero contratado al efecto.

Las instituciones de fondos de pago electrónico deberán generar un plan de remediación documentado para atender las vulnerabilidades detectadas en las pruebas mencionadas en el párrafo anterior, en el que se deberá priorizar su atención de acuerdo con la criticidad de dichas vulnerabilidades, conforme a la clasificación que realice la propia institución.

Los planes de remediación a que se refiere el párrafo anterior deberán ser validados por el oficial en jefe de seguridad de la información. Asimismo, dichos planes deberán contener, al menos, la indicación del personal responsable de su implementación y ejecución, detalle de las actividades definidas, fecha de inicio y de fin de estas, al igual que los recursos técnicos, materiales y humanos requeridos. Los referidos planes de remediación deberán elaborarse dentro de los diez días hábiles siguientes a que se identifiquen las vulnerabilidades y estar disponibles para la CNBV y el Banco de México, cuando dichas autoridades lo requieran.

Artículo 22.- Las instituciones de fondos de pago electrónico deberán contar con procedimientos y mecanismos para impedir la instalación de cualquier servicio, aplicación o software, salvo los que:

I. Sean necesarios para la operación de la institución de fondos de pago electrónico.

II. Estén autorizados por el oficial en jefe de seguridad de la información de la institución de fondos de pago electrónico, en cada uno de los elementos de su Infraestructura Tecnológica.

Artículo 23.- Las instituciones de fondos de pago electrónico que cuenten con infraestructura propia para su operación y el resguardo de la información, deberán establecer procedimientos y mecanismos para restringir el acceso, tanto a los puertos físicos de conexión y dispositivos periféricos, como a la infraestructura de cómputo o de telecomunicaciones.

Asimismo, cuando las instituciones de fondos de pago electrónico contraten con un tercero la infraestructura necesaria para su operación y el resguardo de la información, deberán asegurar que dicho tercero cuente con los procedimientos y mecanismos referidos en el párrafo anterior.

Artículo 24.- Las instituciones de fondos de pago electrónico deberán contar con procedimientos y mecanismos de control de acceso a la Infraestructura Tecnológica que sean robustos y seguros, para lo cual deberán cumplir, al menos, con los requisitos siguientes:

I. Controles de acceso lógico a la infraestructura de cómputo y telecomunicaciones, así como su Infraestructura Tecnológica y la infraestructura de software como base de datos, sistemas operativos y contenedores de software.

II. Controles para la gestión de Usuarios de la Infraestructura Tecnológica y contraseñas.

III. Controles que aseguren el seguimiento y monitoreo del acceso a los sistemas utilizados para el almacenamiento de la información de los Clientes, incluyendo auditorías automáticas que permitan la revisión del acceso a nivel individual a la información de los Clientes, las acciones que se realizaron tras el acceso a tal información, los intentos de acceso inválidos, los cambios de Identificación del Cliente y Autenticación para el acceso de los datos de los Clientes, así como todos los cambios realizados al sistema de almacenamiento.

En el caso de que la institución de fondos de pago electrónico pretenda utilizar cualquier práctica o estándar distintos que no contengan los elementos antes mencionados, deberá obtener previamente la autorización del Banco de México y de la CNBV, para lo cual deberá presentar la solicitud respectiva de acuerdo con lo establecido en el artículo 59 de estas Disposiciones. La CNBV y el Banco de México podrán publicar en sus páginas de Internet los estándares que cumplen con los requisitos anteriores.

Artículo 25.- Las instituciones de fondos de pago electrónico deberán establecer políticas de seguridad de información que su personal esté obligado a observar, que incluyan el correcto uso de los recursos utilizados para el almacenamiento de datos de los Clientes, la revisión previa a la contratación de los perfiles del personal que pretenda contratar la institución de fondos de pago electrónico, así como los procesos de evaluación de riesgos que se realicen por lo menos cada año.

Sección Tercera
Disposiciones generales para la Infraestructura Tecnológica

Artículo 26.- Las instituciones de fondos de pago electrónico deberán establecer y documentar políticas y mecanismos para que los Canales de Instrucción solo utilicen aquellos protocolos de comunicación que garanticen la confidencialidad de la información en la comunicación punto a punto, con base en las mejores prácticas y estándares internacionales de seguridad informática en esta materia que, previo acuerdo entre la CNBV y el Banco de México, sean publicadas, en sus respectivos sitios de Internet. Los mecanismos de cifrado implementados para dichos protocolos de comunicación deberán estar vigentes, no contar con vulnerabilidades conocidas y contemplar que la longitud de las claves de cifrado sea robusta.

En caso de que alguna institución de fondos de pago electrónico pretenda utilizar cualquier práctica o estándar distinto a los señalados anteriormente, deberá obtener previamente autorización del Banco de México y de la CNBV. Para estos efectos, las instituciones de fondos de pago electrónico deberán presentar las solicitudes a que se refiere a este artículo, de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones.

Artículo 27.- Las instituciones de fondos de pago electrónico deberán contar con medidas de validación para garantizar la autenticidad de los procesos ejecutados por los diferentes componentes de la Infraestructura Tecnológica, incluyendo las Operaciones realizadas por los Clientes, considerando, al menos, lo siguiente:

I. La verificación de la veracidad e integridad de la información sin importar que se encuentre estática o en tránsito.

II. La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan solo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro.

III. Los protocolos de mensajería, comunicaciones y Cifrado, los cuales deben procurar la integridad y confidencialidad de la información.

IV. La identificación de procesos atípicos, previendo que se cuenten con herramientas de monitoreo o medidas de alerta automática para su atención, por parte de las áreas operativas correspondientes.

V. La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados a los procesos de ejecución.

Las medidas a que alude este artículo deberán establecerse acorde con el grado de riesgo que las instituciones de fondos de pago electrónico definan para cada tipo de proceso.

Artículo 28.- Las instituciones de fondos de pago electrónico, para la implementación y el desarrollo de sus sistemas informáticos, ya sea por parte de la propia institución o por medio de un tercero especializado en el desarrollo de programas de cómputo contratado por esta, deberán cumplir con lo siguiente:

I. Documentar sus procesos, funcionalidades y configuraciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones y el inventario detallado de cada componente de la Infraestructura Tecnológica.

El proceso de desarrollo deberá implementar aspectos de seguridad de la información, al menos, en las siguientes etapas:

a) Elaboración de requerimientos.

b) Diseño del sistema informático.

c) Desarrollo o adquisición del sistema informático conforme al diseño a que se refiere el inciso b) anterior.

d) Validación de funcionalidades, propósito, capacidad y calidad del sistema informático.

e) Pruebas de vulnerabilidades y análisis de código previas a su liberación.

f) Liberación o instalación del sistema informático.

g) Control de cambios en el sistema informático.

h) Destrucción segura de información al término de la vida útil de componentes o sistemas.

i) En caso de que el software sea desarrollado por una empresa externa especializada, la institución de fondos de pago electrónico deberá solicitar que el software entregado contenga mecanismos para validar su integridad y autenticidad al momento de instalarlo en su Infraestructura Tecnológica.

II. Los sistemas informáticos deberán considerar las siguientes funcionalidades durante todo su proceso de operación:

a) Mecanismos de Autenticación entre los diferentes componentes utilizados para la operación de la institución de fondos de pago electrónico.

b) Uso de firmas electrónicas para garantizar la integridad y el no repudio de la información operativa de la institución de fondos de pago electrónico, con independencia de que sea información estática o en tránsito.

c) Gestión de Usuarios de la Infraestructura Tecnológica y sus privilegios.

d) Uso de comunicaciones cifradas para la comunicación de los diferentes sistemas informáticos y sus componentes.

III. Revisar de forma estática, al menos a través de herramientas automatizadas, la seguridad del sistema informático cada vez que se realice una actualización de este.

Artículo 29.- Las instituciones de fondos de pago electrónico deberán mantener la solidez de su Infraestructura Tecnológica, para lo cual deberán contar con:

I. Controles que permitan revisar, al menos una vez al año, que los componentes que brindan seguridad a su Infraestructura Tecnológica se encuentren vigentes y, en su caso, actualizar los componentes que ya no lo sean.

II. Procedimientos y herramientas para la detección de la alteración o falsificación de la información contenida en la Infraestructura Tecnológica.

III. Registros que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes Usuarios de la Infraestructura Tecnológica de los sistemas informáticos, con independencia del nivel de privilegios que se establezca para su acceso y el medio o protocolo de comunicación de acceso. Estos registros deberán incluir, al menos, la siguiente información:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los Usuarios de la Infraestructura Tecnológica.

b) Elementos que permitan identificar al Usuario de la Infraestructura Tecnológica que realiza dichas actividades.

c) Datos de identificación del punto de acceso utilizado por el Usuario de la Infraestructura Tecnológica para realizar la operación de que se trate.

d) Direcciones de los protocolos de Internet o similares, de acuerdo con el medio electrónico utilizado por el Usuario de la Infraestructura Tecnológica.

La información generada deberá ser almacenada de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

IV. Registros que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes Clientes. Estos registros deberán incluir, al menos, la siguiente información:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los Clientes.

b) Números de las Cuentas involucradas en la Operación, incluyendo aquella Cuenta perteneciente al ordenante de la Operación y, en su caso, la de los receptores, y demás información que permita identificar las Operaciones realizadas por los Clientes o quienes hayan usado el medio de disposición respectivo.

c) Datos de identificación del Canal de Instrucción utilizado por el Cliente o por quien haya usado el medio de disposición respectivo para realizar la Operación de que se trate, así como los Factores de Autenticación utilizados para su instrucción.

d) Direcciones de los protocolos de Internet o similares, el número de la línea de teléfono o demás datos, de acuerdo con el Canal de Instrucción utilizado por el Cliente o usuario del medio de disposición.

La información generada deberá ser almacenada de forma segura por un periodo mínimo de ciento ochenta días naturales a partir de su generación, mediante mecanismos previamente determinados para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Dicha información deberá ser proporcionada a los Clientes o usuarios del medio de disposición que así lo requieran expresamente a la institución de fondos de pago electrónico mediante sus canales de atención al Cliente, en un plazo que no exceda de diez días hábiles, siempre que se trate de Operaciones realizadas en las propias Cuentas de los Clientes o usuarios del medio de disposición durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate.

V. Registros que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos, así como bloquear transmisiones que no cumplan con los criterios de seguridad establecidos. Estos registros deberán incluir lo siguiente:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los sistemas informáticos.

b) Datos de identificación del punto de acceso utilizado por el sistema informático, para realizar la operación de que se trate.

c) Direcciones de los protocolos de Internet o similares, de acuerdo con el medio electrónico utilizado por el sistema informático.

La información generada, incluyendo la de otros medios, deberán ser almacenadas de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Artículo 30.- Las instituciones de fondos de pago electrónico deberán contar con una Política Estratégica de Continuidad de Negocio y de Seguridad de la Información, la cual deberá ser aprobada por su Órgano de Administración.

Artículo 31.- Las instituciones de fondos de pago electrónico deberán contar con un Plan Director de Seguridad el cual deberá ser aprobado por el director general o, a falta de este, por el administrador único. El Plan Director de Seguridad deberá estar alineado con la estrategia de negocio de la institución de fondos de pago electrónico y con lo establecido en la Política Estratégica de Continuidad de Negocio y de Seguridad de la Información, así como definir y priorizar los proyectos en materia de seguridad de la información, con el objetivo de reducir la exposición a los riesgos tecnológicos y la materialización de Incidentes de Seguridad de la Información hasta niveles aceptables en los términos que defina el Órgano de Administración, a partir de un análisis de la situación actual.

Para la aprobación del Plan Director de Seguridad, el director general o, en su caso, el administrador único, deberá verificar que este contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes y contemple los controles requeridos conforme a las disposiciones aplicables. Las modificaciones al Plan Director de Seguridad deberán ser aprobadas por el director general o, en su caso, por el administrador único.

Tratándose de instituciones de fondos de pago electrónico que cuenten con director general y consejo de administración, el primero deberá informar a dicho consejo el contenido y modificaciones al Plan Director de Seguridad, y deberá contar con evidencia de su aprobación e implementación.

Artículo 32.- Las instituciones de fondos de pago electrónico deberán implementar procedimientos y mecanismos que deberán seguir para la atención de Incidentes de Seguridad de Información en su Infraestructura Tecnológica, en los que se comprendan la identificación, contención y la adecuada recolección y resguardo de evidencias de dichos incidentes.

Artículo 33.- Las instituciones de fondos de pago electrónico deberán evaluar o auditar, al menos una vez al año, la seguridad informática de la Infraestructura Tecnológica. Además, entre los trabajos de dicha evaluación o auditoría, las instituciones de fondos de pago electrónico deberán presentar al Órgano de Administración, en el plazo referido, los siguientes documentos:

I. Reporte que especifique el nivel de riesgo informático para la Infraestructura Tecnológica.

II. Plan de remediación para atender las observaciones clasificadas con criticidad alta y muy alta, encontradas en la referida evaluación o auditoría.

III. Evidencia de la implementación de las medidas de remediación conforme al plan indicado en la fracción II de este artículo.

IV. Evidencia de la mitigación de las observaciones referidas conforme al plan mencionado en la fracción II del presente artículo.

Las instituciones de fondos de pago electrónico, previo al inicio de operaciones, deberán realizar la evaluación o auditoría a que se refiere el párrafo anterior, sobre aquellos elementos o componentes de la Infraestructura Tecnológica propia o de terceros contratados, utilizada para realizar la emisión, administración, redención o transmisión de fondos de pago electrónico, incluyendo los servicios que presten a sus Clientes para realizar dichas actividades, así como el almacenamiento de la Información Personal y la Información Sensible.

Para efectos de lo establecido en el primer y segundo párrafos del presente artículo, las instituciones de fondos de pago electrónico que utilicen Infraestructura Tecnológica de terceros deberán contar, por parte de estos, con los siguientes documentos:

I. Resultados de la evaluación o auditoría realizadas al menos una vez al año y previo al inicio de operaciones a dichos terceros.

II. Plan de remediación para atender las observaciones clasificadas con criticidad alta y muy alta, encontradas en la evaluación o auditoría a que se refiere la fracción I anterior.

III. Evidencias de la implementación del plan de remediación y de la mitigación de las observaciones señaladas en la fracción II que precede.

Las instituciones de fondos de pago electrónico deberán presentar al Órgano de Administración lo referido en las fracciones anteriores.

Los documentos a que se refiere el presente artículo deberán estar disponibles para consulta del Banco de México y la CNBV, cuando dichas Autoridades Financieras lo requieran y, en este caso, deberán ser enviadas conforme a lo establecido en el artículo 59 de las presentes Disposiciones.

Artículo 34.- Las instituciones de fondos de pago electrónico deberán contratar a una persona moral, con personal que cuente con capacidad técnica comprobable mediante certificaciones de la industria en la materia, para que, al menos, cada dos años, se realicen pruebas de penetración en los diferentes sistemas y aplicativos de la Infraestructura Tecnológica, con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los Clientes y de la propia institución de fondos de pago electrónico.

La institución de fondos de pago electrónico deberá enviar al Banco de México y a la CNBV, dentro de los veinte días hábiles, contados a partir de la fecha en que hayan finalizado las pruebas correspondientes, un informe con las conclusiones de dichas pruebas, de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones. El informe deberá firmarse digitalmente por el director general o, en su caso, por el administrador único, y deberá cifrarse conforme a lo dispuesto en el artículo 59 de las presentes Disposiciones.

En el caso de que, de las pruebas de penetración realizadas, se deriven observaciones de alta o muy alta criticidad, la institución de fondos de pago electrónico de que se trate deberá presentar un plan de remediación documentado para subsanar dichas observaciones, al Banco de México y a la CNBV, en un plazo no mayor a 20 días hábiles de haber finalizado las pruebas de penetración. El plan de remediación deberá firmarse digitalmente por el director general o, en su caso, por el administrador único, y cifrarse conforme a lo dispuesto en el artículo 59 de las presentes Disposiciones. La CNBV y el Banco de México podrán efectuar observaciones a dicho plan de remediación, en cualquier tiempo.

Una vez concluidas las actividades de remediación de las observaciones de alta o muy alta criticidad a que se refiere el párrafo anterior, la institución de fondos de pago electrónico deberá realizar nuevamente, en un plazo no mayor a dos meses posteriores a la fecha de conclusión de dichas actividades, pruebas de penetración para verificar que se han mitigado las vulnerabilidades respectivas.

Las instituciones de fondos de pago electrónico deberán documentar en manuales las metodologías utilizadas para clasificar la criticidad y el riesgo de los hallazgos de las pruebas de seguridad de la información, incluyendo las de penetración y vulnerabilidades.

Artículo 35.- Las instituciones de fondos de pago electrónico deberán contar con una persona que, entre sus funciones, se desempeñe como oficial en jefe de seguridad de la información, conocido como CISO por sus siglas en inglés de *Chief Information Security Officer*. Dichas funciones podrán ser realizadas por un tercero, siempre que se ajuste a lo señalado en el presente artículo.

El oficial en jefe de seguridad de la información deberá ser designado por el director general o, en su caso, por el administrador único, y no deberá tener conflictos de interés respecto del responsable de las funciones de auditoría y tecnologías de la información de la institución de fondos de pago electrónico. Asimismo, no podrá realizar las funciones relacionadas con la operación de la seguridad de la información de la propia institución de fondos de pago electrónico.

El oficial en jefe de seguridad de la información podrá apoyarse, para el ejercicio de sus funciones, en representantes de las diferentes unidades de negocio.

Las instituciones de fondos de pago electrónico podrán designar como oficial en jefe de seguridad de la información al director general o, en su caso, al administrador único, durante un plazo máximo de doce meses contados a partir de la fecha en que obtengan la autorización para actuar como instituciones de fondos de pago electrónico.

Artículo 36.- El oficial en jefe de seguridad de la información de la institución de fondos de pago electrónico deberá, al menos:

I. Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad de la información señalados en las presentes Disposiciones.

II. Elaborar el Plan Director de Seguridad, el cual deberá contener, por cada proyecto que se defina, nombre del proyecto, objetivo, alcance, fechas de inicio y fin, áreas involucradas y la inversión proyectada. El plan a que se refiere la presente fracción deberá revisarse y actualizarse, al menos anualmente.

III. Verificar, al menos anualmente, la definición de los perfiles de acceso a la Infraestructura Tecnológica de la institución de fondos de pago electrónico, ya sea propia o provista por terceros, de acuerdo con los perfiles de puestos, conocido como segregación funcional, incluyendo aquellos con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos.

IV. Asegurarse, al menos anualmente o antes en caso de presentarse un Incidente de Seguridad de la Información, de la correcta asignación de los perfiles de acceso a los Usuarios de la Infraestructura Tecnológica. La función a que se refiere esta fracción podrá realizarse mediante muestras representativas y aleatorias.

    Asimismo, el oficial en jefe de seguridad de la información será responsable de la autorización temporal de los accesos por excepción, tales como los de Usuarios de la Infraestructura Tecnológica de ambientes de desarrollo con accesos a ambientes de producción, accesos por eventos de contingencia o cualquier otro acceso privilegiado que no corresponda con la política determinada por la institución de fondos de pago electrónico. Igualmente, deberá contar con un registro que contenga el nombre del Usuario de la Infraestructura Tecnológica, aplicación asociada, ambiente, motivo de la excepción y fecha de inicio y de fin de la asignación.

V. Aprobar y verificar el cumplimiento de las medidas que se hayan adoptado para subsanar deficiencias detectadas con motivo de las funciones a que se refieren las fracciones III y IV de este artículo, así como de los hallazgos, tanto de auditoría interna, como externa relacionada con la Infraestructura Tecnológica y de seguridad de la información.

VI. Gestionar las alertas de seguridad de la información comunicadas por la CNBV u otros medios, así como los Incidentes de Seguridad de la Información, considerando las etapas de identificación, protección, detección, respuesta y recuperación.

VII. Presidir el equipo que se conforme para la detección y respuesta de Incidentes de Seguridad de la Información en la institución de fondos de pago electrónico.

VIII. Informar al Órgano de Administración, o al comité de auditoría y al comité de riesgos en caso de contar con ellos, en la sesión inmediata siguiente, según resulte aplicable, a la verificación del Incidente de Seguridad de la Información, respecto de las acciones tomadas y del seguimiento a las medidas para prevenir o evitar que se presenten nuevamente los mencionados incidentes.

IX. Verificar que se implementen programas anuales de capacitación dirigidos a todo el personal, así como de concientización en materia de seguridad de la información hacia los Clientes incluyendo, en su caso, a terceros que les presten servicios, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de Infraestructura Tecnológica tengan al respecto.

X. Presentar mensualmente al director general o, en su caso, al administrador único, el informe de gestión en materia de seguridad de la información. Este reporte deberá efectuarse al comité de auditoría y al comité de riesgos o, en ausencia de estos, al consejo de administración de la institución de fondos de pago electrónico, en su sesión inmediata siguiente.

XI. Considerar, al menos, los indicadores de riesgo en materia de seguridad de la información establecidos en el Anexo 1 de estas Disposiciones, e informar del resultado de la evaluación de dichos indicadores al Órgano de Administración, y en su caso, al comité de auditoría o comité de riesgos.

XII. Responder a los requerimientos formulados por el Banco de México y la CNBV y al interior de la institución de fondos de pago electrónico, en materia de seguridad de la información.

Las instituciones de fondos de pago electrónico deberán asegurarse de que el oficial en jefe de seguridad de la información tenga a su disposición los registros de las personas que cuenten con acceso a la información relacionada con las operaciones en las que interviene la propia institución de fondos de pago electrónico, incluyendo aquellas que se encuentren en el extranjero, así como de los Usuarios de la Infraestructura Tecnológica que cuenten con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos, así como de sus prestadores de servicios.

Las instituciones de fondos de pago electrónico que pertenezcan a un grupo financiero sujeto a la supervisión de la CNBV, o bien, que formen parte de Consorcios o Grupos Empresariales que cuenten con una entidad financiera sujeta a la supervisión de la propia CNBV, podrán asignar las funciones del oficial en jefe de seguridad de la información a la persona que desempeñe dichas actividades en la entidad financiera supervisada por la CNBV, siempre y cuando dicha persona cumpla con lo establecido en el artículo 35 de estas Disposiciones.

CAPÍTULO III
DE LA CONTINUIDAD OPERATIVA

Artículo 37.- Las instituciones de fondos de pago electrónico deberán contar con un Plan de Continuidad de Negocio que se obliguen a cumplir e incluyan los requerimientos mínimos establecidos en el Anexo 2 de las presentes Disposiciones, el cual deberá de estar alineado con la Política Estratégica de Continuidad de Negocio y de Seguridad de la Información.

El Plan de Continuidad de Negocio deberá ser aprobado por el director general o, en su caso, por el administrador único, debiendo verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes, conforme a las presentes Disposiciones. Las modificaciones al Plan de Continuidad de Negocio deberán ser aprobadas por el director general o, en su caso, por el administrador único, siendo responsabilidad del director general ajustarse a los principios establecidos por el consejo de administración en el manual de continuidad de negocio y seguridad de la información.

Tratándose de instituciones de fondos de pago electrónico que cuenten con director general y consejo de administración, el primero deberá informar a dicho consejo el contenido del Plan de Continuidad de Negocio, o de sus modificaciones, y contar con evidencia de su aprobación e implementación.

Artículo 38.- Cada institución de fondos de pago electrónico deberá contar con los mecanismos necesarios para la continuidad operativa y la administración de Contingencias Operativas de la propia institución, que incluyan su identificación, evaluación, monitoreo y mitigación.

Artículo 39.- Las instituciones de fondos de pago electrónico deberán contar con metodologías para estimar los impactos cuantitativos y cualitativos de las posibles Contingencias Operativas que, en términos de estas Disposiciones, determine el responsable de la administración de Contingencias Operativas para su utilización en el análisis a que hace referencia el Anexo 2 de estas Disposiciones. El Órgano de Administración de cada institución de fondos de pago electrónico deberá aprobar dichas metodologías, sin perjuicio de las facultades del director general para realizar las modificaciones al Plan de Continuidad de Negocio, de conformidad con los principios establecidos por el respectivo Órgano de Administración en la Política Estratégica de Continuidad de Negocio y Seguridad de la Información.

Artículo 40.- El Órgano de Administración de la institución de fondos de pago electrónico deberá designar a una persona responsable de la administración de Contingencias Operativas, que cuente con conocimientos en la materia y quien podrá ser la misma persona que sea designada como administrador integral de riesgos de conformidad con las disposiciones de carácter general que emita la CNBV. El responsable de la administración de Contingencias Operativas podrá auxiliarse de otras áreas de la propia institución de fondos de pago electrónico o de terceros contratados al efecto, que sean especialistas en la materia. Dicha persona deberá tener, como mínimo, las funciones siguientes:

I. Elaborar, revisar y, en su caso, actualizar el Plan de Continuidad de Negocio.

II. Evaluar, por lo menos una vez al año, el alcance y efectividad, así como el cumplimiento de los requerimientos mínimos establecidos en el Anexo 2 de las presentes Disposiciones, así como del Plan de Continuidad de Negocio establecido, e informar los resultados de dicha evaluación al Órgano de Administración y a las áreas responsables de los procesos operativos críticos, identificando, en su caso, los ajustes necesarios para su actualización, fortalecimiento y cumplimiento. En caso de que la institución de fondos de pago electrónico cuente con un comité de auditoría, las funciones previstas en esta fracción serán realizadas por dicho comité.

III. Coordinar y verificar la ejecución de las pruebas del funcionamiento y suficiencia del Plan de Continuidad de Negocio e informar al Órgano de Administración, cuando menos una vez al año, sobre los resultados de dichas pruebas.

IV. Definir y presentar al Órgano de Administración, la metodología para la administración de Contingencias Operativas, en los términos establecidos en las disposiciones correspondientes a la administración de eventos operativos. Para efectos de lo anterior, el responsable de la administración de eventos operativos podrá auxiliarse de otras áreas de la propia institución de fondos de pago electrónico o de terceros contratados al efecto, que sean especialistas en la materia.

V. Definir y presentar para aprobación del Órgano de Administración, las metodologías para estimar los impactos cuantitativos y cualitativos de las Contingencias Operativas. Para efectos de lo anterior, el responsable de la administración de Contingencias Operativas podrá auxiliarse de otras áreas de la propia institución de fondos de pago electrónico o de terceros contratados al efecto que sean especialistas en la materia.

VI. Verificar la efectividad de la metodología para estimar los impactos cuantitativos y cualitativos de las posibles Contingencias Operativas, al menos una vez al año y, en su caso, corregir dicha metodología dentro del mismo plazo. Asimismo, comparar sus estimaciones contra las Contingencias Operativas efectivamente observadas y, de ser el caso, llevar a cabo las correcciones necesarias.

En el supuesto de que las instituciones de fondos de pago electrónico contraten con terceros los servicios necesarios para soportar su operación, en sustitución de lo previsto en las fracciones II y III del presente artículo, y únicamente respecto de los servicios prestados por dichos terceros, las instituciones deberán contar con la documentación que acredite que tales terceros cuentan con una certificación vigente emitida conforme a estándares internacionales respecto de su capacidad para mantener la continuidad de sus servicios. Lo anterior, deberá observarse sin perjuicio del cumplimiento de lo previsto en el Capítulo V de las presentes Disposiciones.

CAPÍTULO IV
DISPOSICIONES COMUNES DE SEGURIDAD DE INFORMACIÓN Y DE CONTINUIDAD OPERATIVA

Artículo 41.- Las instituciones de fondos de pago electrónico deberán llevar un registro en bases de datos de los Eventos de Seguridad de la Información calificados como relevantes, Incidentes de Seguridad de la Información, Contingencias Operativas, así como fallas o vulnerabilidades detectadas en la Infraestructura Tecnológica, que incluya, según sea el caso, la información relacionada con la detección de fallas, errores operativos, intentos de ataques informáticos y de aquellos efectivamente llevados a cabo, así como de pérdida, extracción, alteración, extravío o uso indebido de información de los Usuarios de la Infraestructura Tecnológica o de los Clientes, en donde se contemple la fecha del suceso y una breve descripción de este, su duración, servicio o el elemento de la Infraestructura Tecnológica afectado, Clientes afectados y montos, así como las medidas correctivas implementadas.

La información de los Eventos de Seguridad de la Información calificados como relevantes e Incidentes de Seguridad de la Información, así como Contingencias Operativas, deberá estar respaldada en los medios que las instituciones de fondos de pago electrónico determinen y conservarse por, al menos, diez años.

Artículo 42.- En caso de que se presente un Incidente de Seguridad de la Información, o bien, un Evento de Seguridad de Información en los componentes de la Infraestructura Tecnológica de la institución de fondos de pago electrónico; en los Canales de Instrucción, o en la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la institución de fondos de pago electrónico, el director general o, en su caso, el administrador único deberá llevar a cabo lo siguiente:

I. Prever lo necesario para hacer del conocimiento del Banco de México y de la CNBV de forma inmediata, los Incidentes de Seguridad de la Información, mediante correo electrónico que se envíe a las cuentas ifpe@banxico.org.mx y Ciberseguridad-CNBV@cnbv.gob.mx, o a través de otros medios que el propio Banco de México o la CNBV señalen. 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 evento o incidente, así como una evaluación inicial del impacto o gravedad.

   Adicionalmente, las instituciones de fondos de pago electrónico deberán enviar a las cuentas ifpe@banxico.org.mx y Ciberseguridad-CNBV@cnbv.gob.mx, o a través de otros medios que el propio Banco de México o la CNBV señalen, dentro de los cinco días hábiles siguientes a la identificación del Incidente de Seguridad de la Información de que se trate, la información que se determina en los Anexos 3 y 4 de las presentes Disposiciones.

   En el caso de Eventos de Seguridad de la Información, deberán reportarse a través de los medios señalados en el primer párrafo de esta fracción solo aquellos que, de acuerdo con las políticas y procedimientos establecidos por la propia institución de fondos de pago electrónico, se califiquen como relevantes por tener potencial afectación para la institución de fondos de pago electrónico, sus Clientes, contrapartes, proveedores u otras entidades del sistema financiero, además de los relacionados con Información Personal o Información Sensible, imágenes de identificaciones

oficiales e información de los Factores de Autenticación a los que se refiere la fracción III del artículo 5 de estas Disposiciones. Este reporte únicamente deberá contener la fecha y hora de inicio, así como la descripción del evento de que se trate.

II. Llevar a cabo una investigación inmediata sobre las causas que generaron el Incidente de Seguridad de la Información y establecer un plan de trabajo que describa las acciones a implementar para eliminar o mitigar las vulnerabilidades que propiciaron el mencionado incidente. Dicho plan deberá indicar, al menos, el personal responsable de su diseño, implementación, ejecución y seguimiento; plazos para su ejecución, así como los recursos técnicos, materiales y humanos; y enviarse al Banco de México y a la CNBV en un plazo no mayor a quince días hábiles posteriores a que concluyó el Incidente de Seguridad de la Información.

III. Cuando el Incidente de Seguridad de la Información consista en que la Información Personal o Información Sensible que se encuentre en custodia de la institución de fondos de pago electrónico o de terceros que le presten servicios, fue extraída, extraviada, eliminada, alterada, o bien, las instituciones de fondos de pago electrónico sospechen de la realización de algún acto que involucre accesos no autorizados a dicha información, el director general o, en su caso, el administrador único o la persona que alguno de estos designe, deberá notificar a los Clientes la posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información, dentro de las siguientes veinticuatro horas a que ocurrió el Incidente de Seguridad de la Información o a que se tuvo conocimiento de este, a través de los medios de notificación que el Cliente haya señalado para tal efecto, a fin de prevenirlo de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada, eliminada, o alterada. De igual forma, se informará al Cliente las medidas que deberá tomar y, en su caso, efectuar la reposición de los medios de disposición que correspondan o la sustitución de Factores de Autenticación necesarios.

La notificación a que se refiere esta fracción deberá incluir, al menos, la naturaleza del evento, su fecha y hora de inicio, duración y, en caso de existir, delimitar y señalar las afectaciones individuales a cada Cliente La evidencia de esta notificación deberá incluirse en el resultado de la investigación señalada en la fracción II del presente artículo.

Artículo 43.- Las instituciones de fondos de pago electrónico deberán hacer del conocimiento del Banco de México y la CNBV las Contingencias Operativas que se presenten en cualquiera de los canales de atención al público o al interior de la propia institución de fondos de pago electrónico, mediante correo electrónico que se envíe a las cuentas ifpe@banxico.org.mx, contingencias@cnbv.gob.mx y supervisionfintech@cnbv.gob.mx, o a través de otros medios que el propio Banco de México o la CNBV dispongan, debiéndose generar un acuse de recibo electrónico. Lo anterior, siempre que estas interrupciones tengan una duración de, al menos, treinta minutos.

La notificación señalada en el párrafo anterior, deberá efectuarse dentro de los sesenta minutos siguientes a que haya tenido lugar la Contingencia Operativa de que se trate, debiendo incluir la fecha y hora de inicio de la Contingencia Operativa; la indicación de si continúa o si ha concluido y su duración; los procesos, sistemas y canales afectados; una descripción del evento que se haya registrado, y una evaluación inicial del impacto o gravedad.

Asimismo, en caso de que se presente una Contingencia Operativa, la institución de fondos de pago electrónico de que se trate deberá realizar una investigación inmediata sobre las causas que generaron el evento, y enviar los resultados de dicha investigación al Banco de México y a la CNBV, en un plazo no mayor a cinco días hábiles conforme a las especificaciones del Anexo 5 de las presentes Disposiciones.

Por su parte, en caso de que, producto de una Contingencia Operativa, se afecten uno o a más Canales de Instrucción, la institución de fondos de pago electrónico de que se trate deberá hacer del conocimiento de sus Clientes o usuarios respecto del medio de disposición que esté siendo afectado por esta, en un plazo no mayor a cinco segundos contados a partir de que se presente la Contingencia Operativa y conforme a la información con la que cuenten al momento de esta, sobre la intermitencia o imposibilidad del uso de los Canales de Instrucción, a través de los medios de notificación pactados con los propios Clientes o usuarios y deberá mantener evidencia de ello.

Adicionalmente a lo previsto en el párrafo anterior, la institución de fondos de pago electrónico deberá poner a disposición del público en general, en el sitio de Internet que previamente hubiese hecho del conocimiento de sus Clientes, la información relativa a la Contingencia Operativa de que se trate, incluyendo, al menos, la naturaleza del evento, su fecha y hora de inicio y duración, así como una descripción general de las afectaciones que tuvieron sus Clientes, en un plazo máximo de sesenta minutos contados a partir de la materialización del evento y, en caso de existir, deberá delimitar y señalar las afectaciones individuales a cada Cliente o usuario del medio de disposición, las cuales deberá hacer del conocimiento de sus Clientes por los medios previamente pactados para este fin, en un plazo máximo de veinticuatro horas, contadas a partir de la materialización del evento.

En su caso el director general o administrador único será el responsable de llevar a cabo lo previsto en el presente artículo.

CAPÍTULO V
DE LA CONTRATACIÓN DE SERVICIOS CON TERCEROS Y COMISIONISTAS

Artículo 44.- Las instituciones de fondos de pago electrónico requerirán autorización del Banco de México y de la CNBV, para contratar la prestación de servicios con cualquier tercero que cumpla con alguna de las siguientes características:

I. Preste servicios que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de Información Personal o Información Sensible, imágenes de documentos de identificación expedidos por autoridades oficiales o información biométrica de los Clientes, siempre y cuando el tercero de que se trate tenga privilegios de acceso para conocer dicha información o la información de configuración de seguridad, o bien, a la administración de control de accesos.

II. Realice procesos en el extranjero relacionados con la contabilidad o tesorería.

III. Funja como el proveedor primario de aquellos servicios cuya interrupción, parcial o permanente, imposibilite a la institución de fondos de pago electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico, conforme a los actos a los que refieren las fracciones II, III, IV y V del artículo 22 de la Ley para Regular las Instituciones de Tecnología Financiera.

Las instituciones de fondos de pago electrónico únicamente podrán contratar los servicios referidos en las fracciones anteriores, así como cualquier otro, cuando las personas que proporcionen los servicios respectivos queden obligadas a guardar la debida confidencialidad de la información referente a las Operaciones celebradas con sus Clientes, así como la relativa a estos últimos, en caso de tener acceso a ella, al menos en los mismos términos y condiciones en que las instituciones de fondos de pago electrónico queden obligadas a guardar dicha confidencialidad. En todo caso, las instituciones de fondos de pago electrónico serán responsables por las violaciones a la confidencialidad de la información bajo su resguardo o en custodia de los terceros referidos.

El director general o, en su caso, el administrador único de la institución de fondos de pago electrónico será responsable de aprobar la contratación de los prestadores de servicios a que se refiere este Capítulo.

Las instituciones de fondos de pago electrónico deberán mantener los datos de quienes les proporcionen servicios, en el padrón a que se refiere el artículo 52 de las presentes Disposiciones.

La autorización a que se refiere este artículo no será necesaria cuando las instituciones de fondos de pago electrónico contraten a otras entidades financieras sujetas a disposiciones de carácter general substancialmente similares a las presentes Disposiciones.

Artículo 45.- Las instituciones de fondos de pago electrónico deberán presentar al Banco de México y a la CNBV un aviso con veinte días hábiles de antelación a la contratación de terceros, cuando dicho tercero:

I. 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, así como de aquellos servicios cuya interrupción, parcial o permanente, imposibilitarían a la institución de fondos de pago electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico, conforme a los actos a los que refieren las fracciones II, III, IV y V del artículo 22 de la Ley, en cuyo caso el aviso referido deberá cumplir con los requerimientos a que se refiere el artículo 49 de las presentes Disposiciones.

II. Corresponda a una entidad financiera legalmente facultada y sujeta a regulación substancialmente similar a lo dispuesto en la presentes Disposiciones, en el ámbito federal, en materia financiera.

El Banco de México y la CNBV, durante el plazo de veinte días hábiles anteriormente referido, podrán requerir a la institución de fondos de pago electrónico de que se trate, que la prestación de dicho servicio no se realice a través del tercero señalado en el aviso a que se refiere el presente artículo, cuando cualquiera de las dos autoridades considere que, por los términos y condiciones de contratación del servicio, las políticas y procedimientos de control interno, o por la infraestructura tecnológica o de comunicaciones materia del servicio que utilice dicho tercero, este no estará en posibilidad de cumplir con las disposiciones aplicables a la institución de fondos de pago electrónico y, en su caso, pueda verse afectada la estabilidad financiera o continuidad operativa de la propia institución, a juicio del Banco de México o la CNBV.

Artículo 46.- Las instituciones de fondos de pago electrónico podrán celebrar contratos de comisión mercantil con terceros que actúen frente al público en general a nombre y por cuenta de las respectivas instituciones de fondos de pago electrónico, únicamente para la realización de las siguientes Operaciones:

I. Retiros de efectivo efectuados por el propio Cliente titular de la cuenta respectiva.

II. Recepción de efectivo para abono en cuentas propias o de terceros.

III. Consultas de saldos y movimientos de cuentas.

IV. Puesta en circulación instrumentos para la disposición de fondos de pago electrónico.

V. Apertura de cuentas de fondos de pago electrónico, observando en todo momento lo establecido en las disposiciones de carácter general a que se refiere el artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera, emitidas por la Secretaría, o aquellas que las sustituyan.

VI. Transferencias con cargo a cuentas de fondos de pago electrónico, incluidos los pagos de servicios.

Para efectos del presente artículo, las instituciones de fondos de pago electrónico deberán solicitar autorización a la CNBV, de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones.

Las operaciones previstas en las fracciones anteriores deberán efectuarse en moneda nacional y a nombre y por cuenta de la institución de fondos de pago electrónico. En caso de que la institución de fondos de pago electrónico pretenda realizar operaciones distintas a las señaladas a través de comisionistas, deberá solicitar autorización a la CNBV, previo a su realización, de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones.

Tratándose de aquellas instituciones de fondos de pago electrónico que realicen las operaciones señaladas en las fracciones I y II del presente artículo, a través de una institución de crédito, estarán exceptuadas de presentar la solicitud de autorización a que se refiere el párrafo anterior. Adicionalmente, las instituciones de fondos de pago electrónico deberán observar, en todo momento, los límites establecidos en el artículo 9 de las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera emitidas por la CNBV o las que la sustituyan, y establecer en el manual de cumplimiento previsto en las Disposiciones de carácter general a que se refiere el artículo 58 de la Ley

para Regular las Instituciones de Tecnología Financiera emitidas por la Secretaría, o aquellas que la sustituyan, mecanismos de monitoreo para dar cumplimiento a los límites antes mencionados.

Las instituciones de fondos de pago electrónico, en la celebración de los contratos a que se refiere este artículo, deberán cuidar en todo momento que los terceros que les proporcionen los servicios guarden la debida confidencialidad de la información referente a las Operaciones celebradas con sus Clientes, así como la relativa a estos últimos, en caso de tener acceso a ella.

El director general o, en su caso, el administrador único de la institución de fondos de pago electrónico será responsable de aprobar la contratación de comisionistas.

Artículo 47.- Las instituciones de fondos de pago electrónico que pretendan celebrar los contratos de comisión mercantil a que se refiere el artículo anterior, deberán presentar en la solicitud de autorización, lo siguiente:

I. Plan general de funcionamiento que contenga lo siguiente:

   a) Descripción detallada y diagrama de flujo de los procesos de cada una de las operaciones a contratar considerando, en su caso, el proceso de conciliación y liquidación de cada una de ellas, los terceros involucrados y la Infraestructura Tecnológica a utilizar en la Operación de que se trate.

   b) Mecanismos que incluyan los controles automatizados que utilizará la institución de fondos de pago electrónico para evitar que los comisionistas o el Administrador de Comisionistas excedan los límites de operación establecidos en el artículo 48 de las presentes Disposiciones.

   c) Mecanismos de vigilancia del desempeño del comisionista o del Administrador de Comisionistas, que deberán considerar, cuando menos, el cumplimiento de sus obligaciones contractuales.

      Para efectos de lo anterior, la institución de fondos de pago electrónico deberá contar con planes para evaluar y reportar al Órgano de Administración o, en su caso, al comité de auditoría, el desempeño de los comisionistas o del Administrador de Comisionistas contratados y el cumplimiento de la regulación aplicable relacionada con dicha contratación.

   d) Requerimientos técnicos para realizar operaciones a través de comisionistas, ajustándose a lo señalado en el Anexo 7 de las presentes Disposiciones.

Las instituciones de fondos de pagos electrónico, para la realización de operaciones adicionales a las manifestadas en el plan general de funcionamiento a que se refiere esta fracción, deberán solicitar autorización a la CNBV, en un plazo no mayor a veinte días hábiles previo al inicio de la realización de las mencionadas operaciones. Asimismo, cuando lleven a cabo reformas a dicho plan que impliquen cambios sustanciales en los términos en los que realizarían las Operaciones con los Clientes o usuarios del medio de disposición, deberán solicitar autorización a la CNBV con, por lo menos, veinte días hábiles de anticipación a la fecha en que se pretenda que surtan efectos.

II. Proyecto de contrato en el que deberá señalarse la fecha probable de su celebración y los derechos y obligaciones de la institución de fondos de pago electrónico y del comisionista o del Administrador de Comisionistas. Asimismo, dentro del contrato se deberá prever lo siguiente:

   a) Operaciones que el comisionista o el Administrador de Comisionistas realizarán a nombre y por cuenta de la institución de fondos de pago electrónico.

      Tratándose de Operaciones que se realicen a través de Administradores de Comisionistas, las instituciones de fondos de pago electrónico deberán prever en el contrato las Operaciones que el Administrador de Comisionistas contratará a nombre y por cuenta de la institución de

fondos de pago electrónico con los Comisionistas que este administrará, así como, en su caso, las Operaciones y servicios que realizará el propio Administrador de Comisionistas.

b) Límites que aplicarán a cada una de las Operaciones, conforme a las disposiciones aplicables.

c) Derechos y obligaciones que tendrán, tanto la institución de fondos de pago electrónico, como el comisionista o el Administrador de Comisionistas, así como las respectivas consecuencias legales y sanciones aplicables en caso de incumplimiento a los términos del contrato.

d) Facultad de la institución de fondos de pago electrónico para suspender la realización de operaciones o dar por terminado el respectivo contrato, ambas sin responsabilidad, en caso de que el comisionista o el Administrador de Comisionistas incumplan la normatividad aplicable o el contrato, o bien, presenten cambios en su operación que afecten las condiciones del servicio contratado.

e) Medidas correctivas que la institución de fondos de pago electrónico implementaría por el incumplimiento del comisionista o el Administrador de Comisionistas a las disposiciones aplicables.

f) Prohibición para el comisionista o Administrador de Comisionistas de:

1. Condicionar la realización de la operación a la adquisición de un producto o servicio.

2. Publicitarse o promocionarse de cualquier forma a través de la papelería o en el anverso de los comprobantes que proporcionen a los Clientes a nombre de la institución de fondos de pago electrónico de que se trate.

3. Realizar las Operaciones objeto de la comisión en términos distintos a los pactados con la institución de fondos de pago electrónico correspondiente.

4. Subcontratar la comisión mercantil. Lo previsto en esta fracción no será aplicable al Administrador de Comisionistas en la contratación a nombre y por cuenta de la institución de fondos de pago electrónico de los comisionistas que este administrará, salvo por lo que se refiere a aquellas operaciones y servicios que realizará el propio Administrador de Comisionistas.

5. Cobrar comisiones, por cuenta propia, a los 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.

6. Llevar a cabo Operaciones con los Clientes a nombre propio.

7. Pactar en exclusiva con la institución de fondos de pago electrónico, la realización de las Operaciones y actividades consistentes en la recepción de pagos de servicios con cargo a cuentas de fondos de pago electrónico.

g) Constancia, dentro del contrato, de la aceptación expresa por parte del comisionista o Administrador de Comisionistas de las obligaciones siguientes:

1. Apegarse a lo previsto en el artículo 54 de la Ley para Regular las Instituciones de Tecnología Financiera.

2. Entregar, en el desarrollo de la auditoría y a solicitud de la institución de fondos de pago electrónico, al auditor externo independiente de la propia institución de fondos de pago electrónico y a la CNBV, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate, así como permitir al auditor externo independiente o al personal de la CNBV el acceso

a sus oficinas e instalaciones en general, relacionadas con la prestación del servicio en cuestión.

3. Informar a la institución de fondos de pago electrónico respecto de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar las operaciones objeto de la contratación con, por lo menos, treinta días de anticipación a que suceda dicha modificación o cambio.

4. Guardar confidencialidad respecto de la información que haya sido recibida, transmitida, procesada o almacenada durante la realización de las operaciones. Asimismo, aceptar que dicha información solamente podrá usarse y explotarse para los fines pactados en el contrato.

5. Manifestar la aceptación de la responsabilidad directa por el uso indebido de la información de la institución de fondos de pago electrónico y, en su caso, pagar las indemnizaciones por daños y perjuicios causados por cualquier incumplimiento a lo señalado en el numeral anterior.

6. Cumplir con los términos, condiciones y procesos para garantizar a la institución de fondos de pago electrónico la transferencia, la devolución y eliminación segura de la información sujeta a la comisión contratada cuando el contrato se dé por terminado.

7. Prevenir el uso indebido de los factores de autenticación de los Clientes y empleados que operen el servicio contratado.

8. Observar las medidas que deberá instrumentar la institución de fondos de pago electrónico para apegarse a las disposiciones de carácter general a que se refiere el artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera., emitidas por la Secretaría, o aquellas que las sustituyan.

9. Capacitar al personal respecto del proceso para realizar Operaciones, el uso de la infraestructura tecnológica del comisionista y la seguridad de la información.

Las instituciones de fondos de pago electrónico deberán presentar a la CNBV la solicitud de autorización a que se refiere el presente artículo, de conformidad con el artículo 59 de las presentes Disposiciones, con una anticipación de, por lo menos, veinte días hábiles a la fecha en que pretendan realizar la contratación.

Las instituciones de fondos de pago electrónico podrán facultar a terceros, a través de un mandato o comisión, para que contraten a su vez con otras personas a nombre y por cuenta de la propia institución, las comisiones o servicios a que se refiere el presente artículo, designándose tales representantes, para efectos de las presentes disposiciones, como Administrador de Comisionistas.

En este caso, las instituciones de fondos de pago electrónico deberán establecer que corresponderá a los Administradores de Comisionistas asegurarse de que los comisionistas que contraten cumplan con lo establecido en el presente artículo y en el Anexo 7 de las presentes Disposiciones.

Lo previsto en este artículo se observará sin perjuicio de la autorización que podrá obtener la institución de fondos de pago electrónico para que su propio Administrador de Comisionistas sea a su vez comisionista.

Artículo 48.- Las instituciones de fondos de pago electrónico, en la realización de las Operaciones a través de comisionistas a que se refieren las fracciones I y II del artículo 46 de estas Disposiciones, deberán sujetarse a los límites que a continuación se indican:

I. Tratándose de las Operaciones a que se refiere la fracción I del artículo 46, el límite por comisionista no podrá exceder de un monto diario equivalente en moneda nacional a 1,500 UDIs, por Cuenta de Cliente.

II. Tratándose de las Operaciones a que se refiere la fracción II del artículo 46, el límite por comisionista no podrá exceder de un monto diario equivalente en moneda nacional a 4,000 UDIs, por Cuenta de Cliente.

Artículo 49.- Las instituciones de fondos de pago electrónico deberán acompañar a la solicitud de autorización a que se refiere el artículo 44 o, en su caso, al aviso a que se refiere la fracción I del artículo 45 de las presentes Disposiciones, lo siguiente:

I. Descripción detallada y diagramas de flujo de los procesos de los servicios a contratar, considerando las actividades que se pretendan realizar por la institución de fondos de pago electrónico, así como por el prestador del servicio; las áreas de la propia institución de fondos de pago electrónico y del tercero que participan en el flujo del servicio; nombre, descripción y funcionalidad de los sistemas que, en su caso, serán contratados para la prestación del servicio, o los sistemas de la institución de fondos de pago electrónico que serán utilizados por el proveedor respectivo.

II. Proyecto de contrato de prestación de servicios, en el que deberá señalarse la fecha contemplada de su celebración, los derechos y obligaciones de la institución de fondos de pago electrónico y del tercero, incluyendo la determinación sobre la propiedad intelectual respecto de los diseños, desarrollos o procesos utilizados para la prestación del servicio. Dicho proyecto de contrato deberá ser presentado en idioma español.

Asimismo, deberá quedar constancia dentro del contrato, de la aceptación expresa por parte del tercero de las obligaciones siguientes:

a) Apegarse a lo previsto en el artículo 54 de la Ley para Regular las Instituciones de Tecnología Financiera.

b) Entregar en el desarrollo de la auditoría y a solicitud de la institución de fondos de pago electrónico, al Tercero Independiente de la propia institución de fondos de pago electrónico, así como al Banco de México y a la CNBV, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitir al Tercero Independiente o al personal del Banco de México o de la CNBV el acceso a sus oficinas e instalaciones en general, relacionadas con la prestación del servicio en cuestión.

c) Informar a la institución de fondos de pago electrónico respecto de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar la prestación del servicio objeto de la contratación con, por lo menos, treinta días de anticipación a que suceda dicha modificación o cambio.

d) Guardar confidencialidad respecto de la información que haya sido recibida, transmitida, procesada o almacenada durante la prestación de los servicios. Asimismo, aceptar que dicha información solamente podrá usarse para los fines pactados en la prestación del servicio.

e) En caso de que el tercero realice la subcontratación para la prestación parcial o total de alguno de los servicios prestados a las instituciones de fondos de pago electrónico, deberá notificar a la propia institución respecto de dicha subcontratación; asimismo, establecerá los mecanismos para que el subcontratado cumpla con las obligaciones pactadas y proporcione la información para los efectos del artículo 52 de las presentes Disposiciones.

f) Cumplir con los términos, condiciones y procesos para que el tercero garantice a la institución de fondos de pago electrónico la transferencia, devolución y eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.

g) Mantener registros de auditoría íntegros que incluyan la información detallada de los accesos o intentos de acceso y la operación o actividad efectuadas por los Usuarios de la Infraestructura Tecnológica. Dichos registros deberán estar a disposición del personal autorizado de la institución de fondos de pago electrónico.

h) Contar con controles de acceso a la información de acuerdo con los niveles de acceso y perfiles determinados por la institución de fondos de pago electrónico.

i) Permitir a la institución de fondos de pago electrónico realizar las revisiones de seguridad que se señalan en los artículos 21, 33 y 34 de las presentes Disposiciones a los servicios contratados, o bien, proporcionar evidencia de la realización de estas revisiones.

III. Documentación respecto de la Infraestructura Tecnológica que a continuación se indica:

a) Descripción de los enlaces de comunicación utilizados por la institución de fondos de pago electrónico para conectarse con el proveedor de servicios, que incluya el nombre del proveedor, el ancho de banda y el tipo de servicio prestado, entre otros.

b) Diagrama de telecomunicaciones en donde se muestre la conexión existente entre cada uno de los participantes en la prestación del servicio, tales como proveedores, centros de datos, e institución de fondos de pago electrónico, entre otros, incluyendo los esquemas de redundancia.

c) Dirección completa del lugar en donde se realizarán cada uno de los servicios, así como de los centros de datos, primario y secundario, en donde se almacenará y procesará la información. En caso de que el lugar señalado se encuentre en territorio nacional, debe incluirse por lo menos, calle, número exterior e interior, colonia, alcaldía o municipio, código postal y entidad federativa. Tratándose de un sitio localizado en el extranjero, deberán incluirse datos similares que permitan ubicar con certeza el lugar señalado. Tratándose de servicios de Cómputo en la Nube, solamente deberá proporcionarse lo señalado en el artículo 50 de las presentes Disposiciones.

d) En su caso, el esquema de interrelación de aplicaciones o sistemas objeto de la contratación, incluyendo los sistemas propios de la institución de fondos de pago electrónico.

e) Mecanismos de continuidad del servicio contratado.

IV. Mecanismos que permitirán a la institución de fondos de pago electrónico mantener bajo su resguardo, ya sea en Infraestructura Tecnológica propia o de terceros en territorio nacional, los registros detallados de todas las Operaciones que se realicen, así como de sus registros contables de forma que se asegure la continuidad operativa en todo momento. Dichos registros deberán mantenerse en un formato que permita su consulta, operación y uso, con independencia de que el servicio contratado con el tercero no se encuentre disponible.

V. Evidencia de los controles que el tercero mantendrá para garantizar la confidencialidad, integridad y disponibilidad de esta información, cuando este tenga privilegios de acceso a las imágenes de identificaciones oficiales o información biométrica de los Clientes.

VI. Descripción de los mecanismos para vigilar el desempeño del tercero contratado y el cumplimiento de sus obligaciones contractuales incluyendo, al menos, las previstas en las presentes Disposiciones.

VII. Planes para evaluar y reportar al Órgano de Administración o, en su caso, al comité de auditoría de la institución de fondos de pago electrónico, según la importancia del servicio contratado, el desempeño del tercero y el cumplimiento de la regulación aplicable relacionada con dicho servicio.

VIII. 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 institución de fondos de pago electrónico cumplir con las disposiciones legales que la rigen en la materia.

Tratándose de servicios que se procesen, proporcionen o ejecuten total o parcialmente fuera de territorio nacional, las instituciones de fondos de pago electrónico deberán acompañar la

documentación que acredite que los terceros residen en países cuyo derecho interno proporciona protección a los datos de las personas, resguardando su debida confidencialidad, o bien, que dichos países mantengan suscritos con México acuerdos internacionales en dicha materia, o de intercambio de información entre los organismos supervisores, tratándose de Entidades Financieras.

Adicionalmente, las instituciones de fondos de pago electrónico deberán:

a) Contar con la aprobación del Órgano de Administración respecto a que no habrá impacto en la continuidad de la operación de la institución de fondos de pago electrónico, con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizará en la prestación del servicio.

b) Contar con esquemas de soporte técnico que permitan solucionar problemas e incidencias, con independencia de las diferencias que, en su caso, existan en husos horarios y días hábiles.

Asimismo, en el evento de que alguna autoridad del país de origen del tercero a que se refiere esta fracción le requiera información relacionada con los servicios que le presta a la institución de fondos de pago electrónico, el tercero deberá, tan pronto como sea jurídicamente posible, informar de ello a la institución, así como proporcionarle copia de la información que haya entregado a dicha autoridad. En este caso, la institución de fondos de pago electrónico deberá informar de tal situación al Banco de México y a la CNBV de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones, inmediatamente después de que tenga conocimiento de ello, así como proporcionarles copia de la información referida.

El Banco de México y la CNBV contarán con un plazo de veinticinco días hábiles para resolver respecto de la solicitud de autorización a que se refiere el presente artículo; transcurrido este plazo sin pronunciamiento alguno, se entenderá la resolución en sentido positivo. Cualquier requerimiento de información adicional que realice el Banco de México o la CNBV, interrumpirá el plazo señalado en este párrafo.

Artículo 50.- Las instituciones de fondos de pago electrónico que se ubiquen en alguno de los supuestos previstos en los incisos a) y b) de este artículo deberán observar las medidas establecidas a continuación por razones prudenciales.

Las instituciones que estarán obligadas a adoptar las medidas a que se refiere este artículo serán aquellas que contraten a un tercero como proveedor primario de los servicios correspondientes al Cómputo en la Nube para llevar a cabo cualquiera de los actos de emisión, administración, redención o transmisión de fondos de pago electrónico conforme a lo señalado en las fracciones II, III, IV y V del artículo 22 de la Ley para Regular las Instituciones de Tecnología Financiera, cuando los servicios prestados por dicho tercero, con independencia de la nacionalidad de este último o de las personas que ejerzan Control sobre él, sean susceptibles de interrumpirse, temporal o permanentemente, por causa de alguna disposición, orden, instrucción, mandato o acto equivalente de una autoridad extranjera que vaya dirigida de manera directa a impedir, limitar, prohibir o bloquear la prestación de los servicios de Cómputo en la Nube por parte del proveedor primario, ya sea por el lugar en el que este o las personas que ejerzan Control sobre él se encuentren o se hayan constituido o bien, en que mantengan activos o realicen sus operaciones, así como por la relación que dicho tercero guarde con la institución de fondos de pago electrónico respectiva, y que ello imposibilite a dicha institución llevar a cabo los referidos actos de emisión, administración, redención o transmisión de fondos de pago electrónico antes señalados.

Las instituciones de fondos de pago electrónico que se ubiquen en el supuesto a que se refiere el párrafo anterior deberán incluir en sus respectivos Planes de Continuidad de Negocio alguno de los mecanismos indicados a continuación, con la finalidad de garantizar que mantendrán la capacidad de cómputo y procesamiento necesarias para que, a partir de un periodo no mayor a dos horas, se implementen los mecanismos referidos y se puedan realizar, al menos, los procesos respectivos para llevar a cabo todos los actos de emisión, administración, redención o transmisión de fondos de pago electrónico referidos anteriormente, durante el periodo que dure la interrupción del Cómputo en la Nube primario:

I. Un mecanismo que, además del Cómputo en la Nube primario referido en el presente artículo, permita a las instituciones de fondos de pago electrónico contar con la disponibilidad de servicios de Cómputo en la Nube prestados por un proveedor secundario, siempre y cuando ese otro proveedor adicional no esté sujeto al mismo riesgo al que se encuentra el Cómputo en la Nube primario, conforme a lo contemplado en el segundo párrafo del presente artículo, por estar sujeto a una jurisdicción distinta de aquella en la que pueda ocurrir el riesgo que dé lugar a la interrupción de los servicios prestados por el proveedor primario, así como por estar bajo el Control de una persona distinta al proveedor primario o a cualquier otra persona que pertenezca al mismo Grupo Empresarial de dicho proveedor primario o bien, de un Grupo de Personas en el que participe dicho proveedor primario o persona del mismo Grupo Empresarial.

   Lo anterior no deberá entenderse en el sentido de que los servicios correspondientes al Cómputo en la Nube secundario se deban llevar a cabo de manera simultánea a los del Cómputo en la Nube primario referido utilizado por la institución en su operación normal, mientras no ocurra la interrupción referida.

II. Un mecanismo que, además del Cómputo en la Nube primario que utilice la institución de que se trate y se ubique en el supuesto descrito en el segundo párrafo del presente artículo, permita a la institución de que se trate contar con infraestructura propia que le permita realizar, en un territorio distinto a aquel de la jurisdicción extranjera en la que pueda ocurrir el riesgo a que refiere el segundo párrafo del presente artículo, los procesos referidos en dicho párrafo, siempre y cuando la ejecución de dichos procesos no se lleve a cabo por el proveedor primario de Cómputo en la Nube o dependa de este o de las personas que ejerzan Control sobre él o bien, dependa de alguna otra persona que tanto ella como quienes ejerzan Control sobre ella estén sujetas a la misma jurisdicción en la que pueda ocurrir el riesgo indicado.

   La implementación del mecanismo señalado en esta fracción no implicará la operación de manera simultánea con el Cómputo en la Nube del proveedor primario utilizado por la institución en su operación normal, mientras no ocurra la interrupción referida.

III. Cualquier otro mecanismo distinto a los contemplados en las fracciones I y II anteriores que, a solicitud de la institución de fondos de pago electrónico, autoricen el Banco de México y la CNBV, con independencia de aquella otra autorización que, de conformidad con la fracción III del artículo 44 de estas Disposiciones, dichas autoridades otorguen para la contratación del proveedor primario del Cómputo en la Nube referido en el segundo párrafo del presente artículo, siempre y cuando la institución de fondos de pago electrónico demuestre que dicho mecanismo puede asegurar la continuidad en la realización de los actos señalados en el segundo párrafo citado, en caso de que ocurra la interrupción prevista en dicho párrafo por las causas indicadas ahí mismo.

   La solicitud de autorización referida en esta fracción deberá presentarse en los términos establecidos en el artículo 59 de las presentes Disposiciones.

   Las instituciones de fondos de pago electrónico que se ubiquen en los supuestos del presente artículo quedarán obligadas al cumplimiento de lo prescrito en este mismo artículo, sin perjuicio de su facultad para celebrar, en los términos y bajo las condiciones establecidas en las presentes y demás disposiciones aplicables, los contratos que les permitan obtener y conservar los servicios relativos al Cómputo en la Nube prestados por terceros del país o del exterior, con instalaciones informáticas ubicadas dentro o fuera del territorio nacional, con el fin de llevar a cabo los procesos correspondientes a sus Operaciones que estén autorizadas a realizar.

   Lo establecido en el presente artículo únicamente resultará aplicable a aquellas instituciones de fondos de pago electrónico que, derivado de la evaluación que se realice con información al cierre de cada trimestre, se ubiquen en alguno de los siguientes supuestos:

   a) Durante un periodo de doce meses calendario lleve a cabo alguna de las actividades siguientes:

      1. Realicen más de tres millones quinientas mil Operaciones de Transferencias.

2. Envíen o reciban Transferencias por un monto total superior al equivalente en moneda nacional a seis mil millones de UDI's.

b) En cualquier momento hayan contado con más de un millón de Cuentas que, durante un periodo de doce meses calendario consecutivos, hayan registrado, en cualquier momento, un saldo positivo o con respecto a las cuales se haya enviado, al menos, una Transferencia en dicho periodo, o hayan contado con un saldo total en las Cuentas superior al equivalente en moneda nacional a cuatrocientos millones de UDI's.

Las instituciones de fondos de pago electrónico a las cuales les resulte aplicable el presente artículo, tendrán un plazo de ciento ochenta días naturales contados a partir del primer día del mes calendario inmediato posterior a aquel en el que se actualice el supuesto contemplado en los incisos a) o b) anteriores que corresponda, para dar cumplimiento a lo establecido en este artículo.

Artículo 51.- Las instituciones de fondos de pago electrónico, para la contratación de servicios con terceros que sean objeto de autorización en términos del artículo 44 de estas Disposiciones, así como aquellos relacionados con procesos operativos y con administración de bases de datos y sistemas informáticos, deberán dar cumplimiento a lo siguiente:

I. Tratándose de terceros que proporcionen servicios relacionados con procesos operativos y con administración de bases de datos y sistemas informáticos, prever lo señalado en la fracción II, inciso g), numerales 1 al 6 del artículo 47 de las presentes Disposiciones y conservar el contrato respectivo.

II. 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.

III. Mantener en sus oficinas donde se realicen las funciones de administración de la institución de fondos de pago electrónico, al menos, la documentación e información relativa a las evaluaciones, resultados de auditorías y, en su caso, los planes de trabajo que correspondan, así como los reportes de desempeño de los terceros contratados, incluyendo documentación respecto del cumplimiento de lo señalado en la fracción I de este artículo.

IV. Actualizar la descripción o documentación respectiva cuando existan modificaciones que se consideren que tienen un impacto relevante en cuanto al servicio proporcionado o que estén relacionadas con los sistemas, equipos y aplicaciones objeto de la contratación o con sus características técnicas.

V. Respecto de la Infraestructura Tecnológica y seguridad de la información, además de la información determinada en el artículo 49, fracción III, incisos b) y d) de estas Disposiciones, contar con la siguiente documentación:

a) Descripción de las características técnicas de los sistemas, equipos y aplicaciones objeto de la contratación.

b) Aquella en donde se detallen los mecanismos para asegurar la transmisión y almacenamiento de la Información Personal o Información Sensible en forma Cifrada, en su caso, incluyendo la versión de los protocolos de Cifrado y componentes de seguridad en la Infraestructura Tecnológica.

En el caso de la Información Sensible, se exceptúa del Cifrado la información relativa a las Operaciones, siempre y cuando dicha información esté almacenada en tablas o repositorios distintos a los utilizados para almacenar el resto de la Información Personal e Información Sensible y se cuente con mecanismos de seguridad que impidan la integración de dichos repositorios separados en caso de no estar autorizado para ello.

c) La que contenga el detalle del tipo de información de la institución de fondos de pago electrónico y Clientes precisando, en su caso, el tipo de Información Personal o Información Sensible que será almacenada por el tercero en sus equipos o instalaciones, o a la que podrá tener acceso.

d) La descripción de los mecanismos de control y vigilancia del acceso a los sistemas informáticos y a la Información Personal o Información Sensible transmitida, almacenada, procesada, resguardada o custodiada en dichos sistemas, así como de las bitácoras, bases de datos y configuraciones de seguridad que se establezcan al efecto.

e) La evidencia de los controles y de los mecanismos de control a que se refiere la fracción V del artículo 49 de estas Disposiciones.

VI. Contar con la evidencia a que alude la fracción VIII del artículo 49 de las presentes Disposiciones.

Artículo 52.- Las instituciones de fondos de pago electrónico deberán contar con un padrón de todos los prestadores de servicios, incluyendo aquellos proveedores subcontratados por estos, así como de los Administradores de Comisionistas y comisionistas contratados, que contenga al menos la siguiente información:

I. Prestadores de servicios:

a) Nombre, denominación o razón social del prestador de servicios.

b) Nombre del representante legal del prestador de servicios.

c) Descripción del servicio contratado con el tercero, incluyendo los datos o información que, en su caso, son almacenados, procesados o transmitidos por este.

d) En su caso, información de los sistemas que soportan el servicio contratado con el tercero que incluya, al menos, el nombre, versión y función o propósito.

e) En su caso, interfaces con otros sistemas y el propósito de estas, incluyendo el detalle de la información que intercambia.

f) Ubicación en donde se realiza el servicio y en donde se encuentra el personal responsable de llevarlo a cabo.

g) En su caso, ubicación o jurisdicción del centro de datos principal en donde se encuentran los equipos de procesamiento del sistema contratado.

h) En su caso, ubicación o jurisdicción del centro de datos alterno en donde se encuentran los equipos de procesamiento, tratándose de la recuperación del servicio contratado.

i) En su caso, número y fecha del oficio con el que el Banco de México y la CNBV otorgaron la autorización para fungir como prestador de servicios.

II. Administrador de Comisionistas o comisionistas:

a) Nombre, denominación o razón social del comisionista o del Administrador de Comisionistas.

b) Nombre del representante legal del comisionista o del Administrador de Comisionistas.

c) Nombre comercial del comisionista o del Administrador de Comisionistas, así como detalle de la modalidad comercial bajo la que opera, ya sea que se trate de una cadena comercial o franquicia.

d) Número de establecimientos del comisionista en los que se realizan las comisiones mercantiles, y de cada uno de ellos su domicilio completo, incluyendo la clave de la localidad geoestadística conforme al Catálogo Único de Claves de Áreas Geoestadísticas Estatales, Municipales, y Localidades del Instituto Nacional de Estadística y Geografía, o el que lo sustituya.

e) Tipo de Operación que realiza el comisionista a nombre y por cuenta de la institución de fondos de pago electrónico.

f) Límites de las Operaciones pactadas con el comisionista o con el Administrador de Comisionistas.

g) Dispositivos de acceso utilizados para ofrecer los servicios a los Clientes, tales como teléfono móvil, tabletas electrónicas y terminales punto de venta, entre otros.

h) En su caso, número de oficio y fecha en la que se otorgó la autorización para la contratación del comisionista o Administrador de Comisionistas.

Las instituciones de fondos de pago electrónico deberán difundir a través de su página de Internet o aplicación, el listado de los módulos o establecimientos que los comisionistas o el Administrador de Comisionistas tengan habilitados para realizar las Operaciones referidas en el artículo 47 de las presentes Disposiciones, especificando las Operaciones que se pueden llevar a cabo en cada uno de ellos y los montos máximos autorizados por Operación.

Las instituciones de fondos de pago electrónico deberán mantener actualizado el padrón a que se refiere este artículo.

Artículo 53.- La institución de fondos de pago electrónico deberá realizar, al menos anualmente, por sí misma o a través de un tercero, auditorías que tengan por objeto verificar el grado de cumplimiento de las presentes Disposiciones. En caso de que el comisionista o Administrador de Comisionistas cuente con resultados de auditoría que con el mismo objeto se haya realizado previamente, con vigencia máxima de un año, podrán presentarlos a la institución de fondos de pago electrónico. Sin perjuicio de lo anterior, la CNBV podrá ordenar la realización de auditorías cuando a su juicio existan condiciones de riesgo en materia de operación y seguridad de la información.

Artículo 54.- Las instituciones de fondos de pago electrónico, en todo momento, deberán mantener plenamente identificadas las Operaciones que realicen a través del comisionista o del Administrador de Comisionistas, de manera independiente de las que realicen a través de sus plataformas.
Asimismo, las instituciones de fondos de pago electrónico deberán verificar que los comisionistas o Administrador de Comisionistas informen por cualquier medio a los Clientes de las propias instituciones de fondos de pago electrónico, que actúan a nombre y por cuenta de la institución de fondos de pago electrónico de que se trate.

Artículo 55.- Las instituciones de fondos de pagos electrónico responderán en todo momento, tanto por el servicio que sus comisionistas o Administrador de 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.
En caso de incumplimiento por parte de los comisionistas o Administrador de Comisionistas a las disposiciones aplicables, las instituciones de fondos de pago electrónico deberán implementar las medidas correctivas necesarias.

Lo establecido en los dos párrafos anteriores será sin perjuicio de las responsabilidades civiles, administrativas o penales en que los comisionistas o Administrador de Comisionistas o sus empleados, puedan incurrir por las violaciones de las disposiciones legales aplicables.

Lo señalado en el párrafo anterior, deberá establecerse en el contrato que se celebre entre la institución de fondos de pago electrónico y el comisionista o el Administrador de Comisionistas.

CAPÍTULO VI
DE LA EVALUACIÓN A TRAVÉS TERCEROS INDEPENDIENTES

Artículo 56.- Las instituciones de fondos de pago electrónico deberán contratar los servicios de un Tercero Independiente o de la persona moral por medio de la cual dicho Tercero Independiente preste sus servicios, para realizar la evaluación del nivel de cumplimiento de los requerimientos de seguridad de información, del uso de Canales de Instrucción y de la continuidad operativa que dichas instituciones deben observar conforme a lo previsto en los capítulos II, III, IV y V de las presentes Disposiciones.

Artículo 57.- La evaluación del nivel de cumplimiento realizado por el Tercero Independiente a que se refiere el artículo anterior, deberá realizarse cada dos años.

El informe de la evaluación de cumplimiento deberá ser entregado por el Tercero Independiente al Órgano de Administración de la institución de fondos de pago electrónico y presentado al comité de auditoría de dicha institución, cuando cuente con este.

Las instituciones de fondos de pago electrónico no podrán contratar los servicios de un Tercero Independiente, ni de las personas morales por medio de las cuales presten los servicios respectivos, para obtener la evaluación de cumplimiento a que se refiere este artículo por más de dos periodos de evaluación consecutivos. Sin perjuicio de lo anterior, la institución de fondos de pago electrónico podrá designar nuevamente al mismo Tercero Independiente o persona moral referida, después de una interrupción mínima de cinco años contados a partir de la última evaluación de cumplimiento que hubiere otorgado respecto de dicha institución.

En el caso que de la evaluación realizada se deriven observaciones que, a juicio del Tercero Independiente, representen violaciones graves, la institución de fondos de pago electrónico de que se trate deberá presentar el informe de la evaluación de cumplimiento a su Consejo de Administración dentro de los veinte días hábiles siguientes al de finalizada la evaluación por el Tercero Independiente, o en cinco días hábiles en caso de tratarse de Administrador Único.

El informe indicado en el párrafo anterior deberá entregarse al Banco de México y a la CNBV, de conformidad con lo establecido en el artículo 59 de las presentes Disposiciones, dentro de un plazo de cinco días hábiles contados a partir del día siguiente al de la presentación a su Órgano de Administración de dicho informe. El informe deberá firmarse digitalmente por el director general o, en su caso, el administrador único, y ser cifrado conforme a lo dispuesto en el artículo 59 citado.

Además, la institución de fondos de pago electrónico deberá presentar, de conformidad con lo establecido en el artículo 59 de estas Disposiciones, y dentro de un plazo de veinte días hábiles siguientes al de la finalización de la evaluación realizada por el Tercero Independiente, un plan de remediación para subsanar dichas observaciones. El plan de remediación deberá firmarse digitalmente por el director general o, en su caso, el administrador único, y ser cifrado de conformidad con lo dispuesto en el mencionado artículo 59. La CNBV y el Banco de México podrán efectuar observaciones a dicho plan de remediación, en cualquier tiempo.

Artículo 58.- Los Terceros Independientes que evalúen el nivel de cumplimiento de las instituciones de fondos de pago electrónico a las normas contenidas en las presentes Disposiciones, así como las personas morales por medio de las cuales estos presten los servicios respectivos, deberán ser independientes a la fecha de celebración del contrato de prestación de servicios, durante el desarrollo de la evaluación de cumplimiento y hasta la emisión del reporte de la evaluación de cumplimiento de que se trate, y deberán cumplir con lo señalado en el Anexo 6 de las presentes Disposiciones.

CAPÍTULO VII
DISPOSICIONES COMPLEMENTARIAS

Artículo 59.- Tratándose de los documentos que contengan solicitudes, informes, reportes y planes de trabajo o de remediación que las instituciones de fondos de pago electrónico deban presentar a través del sitio de Internet que la CNBV y el Banco de México pongan a disposición de las mencionadas instituciones en el momento en el que obtengan la autorización para organizarse como tales, para los fines establecidos en los artículos 6, 11, 24, 26, 33, 34, 43, 44, 45, 46 y 57 de las presentes Disposiciones, deberán presentarse con las respectivas firmas electrónicas de los representantes que correspondan y, en los casos que se indique, cifrarse conforme a lo siguiente:

I. Uso de claves criptográficas, conocidas como llaves, asimétricas pública y privada por cada firma electrónica, a fin de garantizar confidencialidad y no repudio, evitando compartir la llave privada.

II. Uso de un certificado digital validado por una agencia certificadora reconocida o por un prestador de servicios de certificación acreditado ante la Secretaría de Economía.

III. Incorporación de firma electrónica que permita garantizar la integridad de la información proporcionada.

La información de las claves criptográficas públicas que se deberán utilizar para realizar el cifrado del mensaje de datos que constituya el documento respectivo, será publicada en el sitio de Internet que las Autoridades Financieras referidas en el primer párrafo de este artículo pondrán a disposición de las instituciones de fondos de pago electrónico. Para realizar el cifrado, dichas instituciones podrán utilizar el sistema de información del Banco de México denominado "WebSec" o aquel otro desarrollado por un tercero que cumpla con lo previsto en el Anexo 8 de las presentes Disposiciones.

En los casos en que el sitio de Internet a que se refiere el primer párrafo de este artículo no se encuentre disponible o que las instituciones de fondos de pago electrónico no cuenten con los elementos necesarios para poder emplear las firmas electrónicas en los documentos a que refiere el presente artículo, las referidas instituciones deberán presentar dichos documentos mediante el Módulo de Atención Electrónica, conocido como MAE, del Banco de México, en términos de las disposiciones aplicables emitidas por el propio Banco de México para dichos efectos, o a falta de dicho módulo, por los medios que este disponga.

Las resoluciones emitidas respecto de la documentación ingresada al sitio de Internet de las mencionadas Autoridades Financieras, de conformidad con lo establecido en el presente artículo, se entregarán de manera conjunta por parte de dichas autoridades, a través del mencionado sitio de Internet.

TRANSITORIOS

PRIMERO.- Las presentes Disposiciones entrarán en vigor a los noventa días naturales siguientes al de su publicación en el Diario Oficial de la Federación.

SEGUNDO.- Las instituciones de fondos de pago electrónico tendrán un plazo máximo de seis meses, contados a partir de la entrada en vigor de estas Disposiciones, para dar cumplimiento a lo establecido en el artículo 15 del presente instrumento.

TERCERO.- Las instituciones de fondos de pago electrónico contarán con un plazo de nueve meses, contados a partir de la entrada en vigor de las presentes Disposiciones, para dar cumplimiento a lo establecido en los artículos 16 y 17 de este instrumento.

CUARTO.- Las personas a que se refiere la disposición OCTAVA Transitoria de la Ley para Regular las Instituciones de Tecnología Financiera publicada en el Diario Oficial el 9 de marzo de 2018, tendrán un plazo de seis meses contados a partir de la obtención de su autorización para actuar como institución de fondos de pago electrónico, para cumplir con lo establecido en los artículos 44, 45, 46 y 47 de las presentes Disposiciones.