SECRETARIA DE HACIENDA Y CREDITO PUBLICO

RESOLUCIÓN que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- HACIENDA.- Secretaría de Hacienda y Crédito Público.- Comisión Nacional Bancaria y de Valores.

La Comisión Nacional Bancaria y de Valores, previo acuerdo de su Junta de Gobierno, con fundamento en lo dispuesto por los artículos 46 Bis 1; 46 Bis 2; 52, párrafo octavo; 96 Bis, párrafo primero y 98 Bis de la Ley de Instituciones de Crédito, así como 4, fracciones XXXVI y XXXVIII; 12, fracción XV y 16, fracciones I y VI de la Ley de la Comisión Nacional Bancaria y de Valores, y

CONSIDERANDO

Que, en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de las presentes disposiciones, la Comisión Nacional Bancaria y de Valores, mediante la emisión de la "Resolución que modifica las Disposiciones de carácter general aplicables a los almacenes generales de depósito, casas de cambio, uniones de crédito y sociedades financieras de objeto múltiple reguladas" publicada en el Diario Oficial de la Federación el 26 de abril de 2018, dictaminada por la Comisión Nacional de Mejora Regulatoria mediante oficio COFEME/18/0413, contenido en el expediente 05/0006/020218 eliminó la obligación para las uniones de crédito de contar con la opinión sobre la recepción de préstamos de socios y reconocimiento de la obligación solidaria;

Que, las Disposiciones de carácter general aplicables a las instituciones de crédito establecen la posibilidad de que dichas instituciones celebren contratos de comisión con terceros que actúen a su nombre para ofrecer y realizar operaciones bancarias en los establecimientos de éstos últimos, lo cual realizan a través de operadores que interactúan de manera presencial con el público usuario;

Que, la red de comisionistas ha permitido la expansión de la cobertura geográfica del Sistema Financiero Mexicano, estando presentes en el 75 % de los municipios del país, lo que supera la cobertura tanto de sucursales bancarias como de cajeros automáticos;

Que, ya que la cobertura de redes de telecomunicación es mayor que la de los establecimientos físicos de los comisionistas, resulta conveniente que las instituciones de crédito, en especial aquellas que no poseen infraestructura física o aplicaciones de Internet, integren sus servicios a las plataformas digitales de los comisionistas y empresas especializadas, aprovechando la infraestructura de estos e incluso la base consolidada de clientes de los mismos. Lo anterior, se estima que mitigue algunas de las dificultades que presentan los canales presenciales como el riesgo y costo asociado al uso de efectivo, y el costo que representa para el usuario trasladarse a los establecimientos;

Que, asimismo, las autoridades financieras mexicanas han emitido regulación diversa que permite a las instituciones de crédito (i) ofrecer sus servicios y productos fuera de sus sucursales mediante el aprovechamiento de la tecnología disponible en los mercados y, (ii) mitigar los riesgos a los que se encuentran expuestas, con la finalidad de mantener y fomentar el sano y equilibrado desarrollo del Sistema Financiero Mexicano en su conjunto, en protección de los intereses del público;

Que, por todo lo anterior, la presente "Resolución que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito" regula la figura del comisionista de base tecnológica y busca permitir que las instituciones de crédito contraten con comisionistas, permitiendo que estos puedan ofrecer y realizar, en nombre de dichas instituciones, al público general algunos servicios y productos bancarios a través de canales de acceso digitales a efecto de ampliar el acceso a los mismos entre el público. En adición a lo anterior, dicha Resolución, además, busca establecer, entre otras, las obligaciones contractuales y responsabilidades que las instituciones de crédito tienen con dichos comisionistas, y

Que, a efecto de mitigar el robo de identidad, se establece la responsabilidad exclusiva de las instituciones de crédito en el proceso para autenticar las operaciones de los clientes, así como el establecimiento de un canal seguro de comunicación entre estos, para ejecutar las instrucciones de los clientes, ha resuelto expedir la siguiente:

RESOLUCIÓN QUE MODIFICA LAS DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO

ÚNICO. - Se **REFORMAN** los artículos 1, fracciones XXXI y LXXXIII; 318, párrafo primero, fracciones I, párrafo segundo, II, párrafo primero, III, párrafo primero, inciso a), numeral 3, inciso b), párrafo primero, numerales 1, 3 y 6, y VI; 320, párrafos primero y tercero; 321, párrafos primero, fracción II y segundo; 321 Bis 1, párrafos primero y tercero; 324 párrafo primero, fracciones VII, incisos a) en su primer párrafo y g), XII y XIII, y segundo; se **ADICIONA** al artículo 1 la fracción XLIV Bis; al artículo 318, párrafo primero, fracción III, párrafo primero, inciso a) los numerales 6 y 7; los artículos 319 Bis; 319 Bis 1; 319 Bis 2; 319 Bis 3; 319 Bis 4;

319 Bis 5; 321 la fracción III; 321 Bis 1 un párrafo segundo que incorpora las fracciones I, II, III, IV, V, VI,VII, y VIII y al artículo 324, párrafo primero, una fracción IV Bis; al Título Quinto, Capítulo XI, Sección Segunda, el título del Apartado A denominado “De los comisionistas con establecimientos presenciales”, que comprende el artículo 319; un Apartado B denominado “De los comisionistas de base tecnológica”, que comprende los artículos 319 Bis a 319 Bis 5, y el título del Apartado C denominado “Disposiciones complementarias”, que comprende los artículos 320 a 325, y se **SUSTITUYEN** los Anexos 57, 58 y 59 de las "Disposiciones de carácter general aplicables a las instituciones de crédito", publicadas en el Diario Oficial de la Federación el 2 de diciembre de 2005 y modificadas mediante resoluciones publicadas en el citado medio de difusión, para quedar como sigue:

RESOLUCIÓN QUE MODIFICA LAS DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE CRÉDITO

ÍNDICE

TÍTULO PRIMERO a **CUARTO . . .**

TÍTULO QUINTO . . .

Capítulo I a **X . . .**

Capítulo XI . . .

Sección Primera . . .

Sección Segunda . . .

Apartado A

De los comisionistas con establecimientos presenciales

Apartado B

De los comisionistas de base tecnológica

Apartado C

Disposiciones complementarias

Sección Segunda Bis a **Cuarta . . .**

Capítulo XII a **XV . . .**”

“Artículo 1.- . . .

I. a XXX. **. . .**

XXXI. Cifrado: al mecanismo que deberán utilizar las Instituciones y los comisionistas de base tecnológica a los que se refiere el Apartado B de la Sección Segunda, Capitulo XI del Título Quinto de estas Disposiciones para proteger la confidencialidad de información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.

XXXII. a XLIV. **. . .**

XLIV Bis. Criptografía Matemática Asimétrica: a los métodos de Cifrado que emplean una pareja de llaves de encriptación conocidas como llave pública y llave privada, las cuales, están relacionadas matemáticamente de tal forma que la información Cifrada con una de las llaves solo puede ser descifrada con la llave asociada.

XLV. a LXXXII. **. . .**

LXXXIII. Infraestructura Tecnológica: a los equipos de cómputo, instalaciones de procesamiento de datos y comunicaciones, equipos y redes de comunicaciones, sistemas operativos, bases de datos, aplicaciones y sistemas que utilizan las Instituciones para soportar su operación.

Asimismo, también se refiere a los equipos de cómputo, instalaciones de procesamiento de datos y comunicaciones, equipos y redes de comunicaciones, sistemas operativos, bases de datos, aplicaciones y sistemas que utilizan los comisionistas de base tecnológica a los que se refiere el Apartado B de la Sección

Segunda, Capitulo XI del Título Quinto de estas Disposiciones para soportar la operación pactada entre dichos comisionistas y las Instituciones.

LXXXIV. a CXCVII. **. . .**"

"TÍTULO QUINTO

. . .

Capítulo XI

. . .

Sección Primera

. . .

Artículos 317 y 317 Bis. - . . .

Artículo 318.- . . .

I. **. . .**

Asimismo, en ningún caso, dichos comisionistas podrán llevar a cabo aprobaciones y aperturas de cuentas de operaciones activas, pasivas y de servicios, salvo que se trate de operaciones de las previstas por el Artículo 319, fracciones IX y X y el Artículo 319 Bis de las presentes disposiciones.

II. Contar con un informe y flujograma que especifiquen los procesos operativos o de administración de bases de datos y sistemas informáticos, la información intercambiada en dichos procesos, la ubicación física de los servidores de la Institución y del comisionista de base tecnológica, así como el nombre, domicilio y el contrato que los comisionistas de base tecnológica pacten con terceros para la prestación de servicios de cómputo bajo demanda y de infraestructura tecnológica a través de Internet para soportar su operación que sean objeto de los servicios a contratar. Asimismo, deberán contar con las políticas y criterios para seleccionar al tercero, los cuales estarán orientados a evaluar la experiencia, capacidad técnica y recursos humanos del tercero con quien se contrate para prestar el servicio con niveles adecuados de desempeño, confiabilidad y seguridad, así como los efectos que pudieran producirse en una o más operaciones que realice la Institución.

. . .

. . .

III. **. . .**

a) **. . .**

1. y 2. **. . .**

3. Entregar, a solicitud de la Institución, al auditor externo de la propia Institución y a la Comisión o al tercero que dicha Comisión designe, libros, cifras de control, estructuras de información, informes, pruebas de operación, registros, manuales y documentos en general que acrediten y tomen evidencia en relación al cumplimiento de estas disposiciones, relacionados con la prestación del servicio o comisión de que se trate, los cuales podrán ser entregados digitalmente y firmados mediante Firma Electrónica Avanzada o Fiable. Asimismo, permitir el acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la prestación del servicio en cuestión.

4. y 5. **. . .**

6. En caso de los empleados o funcionarios de los comisionistas a los que se refiere el Artículo 319 Bis, que tengan a su cargo ejecutar los procesos pactados en el contrato de comisión mercantil con la Institución de que se trate en términos de este Artículo y de los Artículos 319 Bis a 319 Bis 5 de estas Disposiciones, deberán ser identificados por el comisionista de base tecnológica en términos del Anexo 58 de las presentes Disposiciones.

Asimismo, las Instituciones deberán pactar con los comisionistas a los que se refiere el párrafo anterior, la entrega por escrito de un documento que contenga la siguiente información, previo a que opere con el Público Usuario a efecto de identificarlos:

i. Nombre completo sin abreviaturas.

ii. Número de empleado.

iii. Los procesos de los que estará a cargo el empleado o funcionario del comisionista en relación con los Artículos 319 Bis a 319 Bis 5.

iv. Correo electrónico institucional del empelado o funcionario.

Dicho documento deberá ser firmado por el empleado o funcionario del comisionista, para lo cual estos podrán utilizar su Firma Electrónica Avanzada.

Asimismo, en caso de que exista un cambio del empleado o funcionario del comisionista a que se refiere el primer párrafo del presente numeral, el comisionista deberá notificar a la Institución dicho cambio dentro de los dos días hábiles que se haya efectuado la designación correspondiente en los términos señalados en este numeral.

7. Intercambiar la información de los clientes con la Institución correspondiente a través de un canal seguro observando como mínimo los requisitos previstos en el Artículo 319 Bis 1 para aquellos comisionistas que se presenten ante el Público Usuario a través de sus páginas de Internet o aplicaciones informáticas.

. . .

b) . . .

1. Las restricciones y condiciones respecto a la posibilidad de que el tercero subcontrate, a su vez, la prestación del servicio.

En ningún caso, lo anterior, implicará que el tercero subcontratado podrá llevar a cabo Operaciones y funciones por cuenta propia o distintas a las que se pacten en el contrato de prestación de servicios o comisión respectivo para efectos de lo previsto en el presente Capítulo.

Asimismo, los terceros con los que las Instituciones contraten no podrán subcontratar los servicios o comisiones a que se refiere el Artículo 319 Bis de las presentes Disposiciones, con excepción de la contratación de servicios correspondientes a cómputo bajo demanda y de infraestructura tecnológica a través de Internet para soportar su operación.

2. . . .

3. Los mecanismos para la solución de disputas relativas al contrato de prestación de servicios o comisión mercantil. De la misma manera deberá prever los mecanismos para la solución de disputas relativas al contrato entre el comisionista y un tercero subcontratado.

4. y 5. . . .

6. Los términos, condiciones y procesos para que el comisionista o el prestador de servicios garantice a la Institución la transferencia, devolución y eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.

Tratándose de los comisionistas a que se refiere el Artículo 319 Bis, las Instituciones deberán requerir de éstos que observen los requerimientos para el manejo seguro de la información en términos de la Sección Octava Bis “De la seguridad de la información”, del Capítulo VI “Controles Internos” del Título Segundo “Disposiciones Prudenciales” a fin de proteger la información de los clientes, potenciales clientes y de la Institución.

7. . . .

. . .

IV. y V. . . .

VI. Verificar que los terceros, los accionistas de estos y, en su caso, subcontratados, así como los comisionistas y sus accionistas, en su caso, el Administrador de Comisionistas y los accionistas de estos últimos, no se encuentren dentro de las listas oficiales que emitan autoridades mexicanas, organismos internacionales, agrupaciones intergubernamentales o autoridades de otros países, de personas vinculadas o probablemente vinculadas con operaciones con recursos de procedencia ilícita, el terrorismo o su financiamiento, o con otras actividades ilegales. Para acreditar lo anterior, bastará con que la Institución, manifieste en el escrito de solicitud que presente que se aseguró que las personas señaladas en esta fracción no estaban relacionadas en dichas listas oficiales al momento de su contratación. Adicionalmente, la Institución deberá manifestar, en el propio escrito de solicitud, que conoce el negocio al que se dedica el comisionista.

VII. . . .

. . .

. . .

. . .

Artículo 318 Bis y 318 Bis 1. - . . .

Sección Segunda

. . .

Apartado A

De los comisionistas con establecimientos presenciales

Artículo 319.- . . .

Apartado B

De los comisionistas de base tecnológica

Artículo 319 Bis. – Las Instituciones podrán celebrar contratos de comisión mercantil con terceros que actúen en todo momento a nombre y por cuenta de aquéllas ante los clientes o potenciales clientes por medio de las páginas de Internet o aplicaciones informáticas de dichos comisionistas, con excepción de las páginas de Internet o aplicaciones informáticas que realizarán la Autenticación del cliente, cambio o actualización de los Factores de Autenticación y actualización del medio de contacto del cliente conforme a lo establecido en los Artículos 319 Bis 2, 319 Bis 3, 319 Bis 4 y 319 Bis 5, sin perjuicio de las demás obligaciones aplicables en términos del Artículo 318 de estas Disposiciones, así como de la presente Sección, debiendo observar adicionalmente los siguientes requisitos:

I. Las Instituciones únicamente podrán contratar con los comisionistas, a los que se refiere el presente artículo, la realización de las operaciones bancarias que se enlistan a continuación y que se ejecutarán en la sesión del cliente a la que se refiere el Artículo 319 Bis 2 de estas Disposiciones:

   a) Apertura de cuentas nivel 2 y transferencias de recursos asociadas a dichas cuentas.

   b) Otorgamiento de créditos por montos no mayores a tres mil UDIs.

   c) Pago de bienes y servicios.

   d) Consultas de saldos y movimientos de los productos y operaciones que el cliente haya contratado y celebrado con la Institución, respectivamente, a través del comisionista de base tecnológica.

   Todas estas operaciones deberán observar lo previsto en las disposiciones vigentes de la Secretaría, Comisión, Banco de México y demás regulación aplicable.

II. Las Instituciones deberán establecer mecanismos y procedimientos para asegurarse de que, a través de las páginas de Internet o aplicaciones informáticas del comisionista de que se trate, se le proporcione a los clientes o potenciales clientes de las Instituciones información personalizada, suficiente y clara en relación con lo siguiente:

   a) Las responsabilidades del comisionista y de la Institución frente a los clientes en relación con el uso de: (i) la información que el cliente les proporcione, y (ii) las páginas de Internet, aplicaciones informáticas e Infraestructura Tecnológica del comisionista.

   b) El reconocimiento de que el servicio de contratación es con las propias Instituciones y que el comisionista es un canal o medio para llevar a cabo las operaciones a que se refiere la fracción I del presente artículo, según corresponda.

   c) Los procesos de Autenticación a que se refieren los Artículos 319 Bis 2 y 319 Bis 3 que se seguirán a efecto de:

      1. Verificar la identidad del cliente o potencial cliente tanto en la apertura de cuenta como en la celebración de las operaciones a que se refiere la fracción I del presente artículo,

      2. Asociar los Factores de Autenticación correspondiente al cliente o potencial cliente.

      3. Identificar al comisionista para que el cliente o potencial cliente verifique que efectivamente está ante el comisionista de la Institución que corresponda.

   d) El derecho del cliente para utilizar el Factor de Autenticación de Categoría 2 definido por este en los términos del Artículo 319 Bis 2, para Autenticarse directamente en los servicios de Banca Móvil o Banca por Internet de la Institución que corresponda, a efecto de realizar operaciones o modificar su información de Autenticación.

III. Las Instituciones deberán estipular en el contrato que celebren con el comisionista que este último no podrá conocer, procesar, transmitir, guardar, modificar o copiar en ninguna circunstancia la información de los Factores de Autenticación asociados a los clientes de la Institución, por lo que deberá atender lo previsto en los Artículos 319 Bis 2, 319 Bis 3, 319 Bis 4 y 319 Bis 5.

IV. Las Instituciones deberán pactar con el comisionista que la información agregada y desagregada que se derive de la relación contractual con la Institución no podrá usarse, compartirse, venderse u otorgarse a algún tercero distinto a los previstos en el Artículo 318, fracción III, inciso a) numeral 7 de las presentes Disposiciones.

Sin perjuicio de lo anterior, las Instituciones podrán pactar las condiciones bajo las cuales el comisionista de base tecnológica utilizará, procesará y transmitirá a esta la información agregada de los clientes para su tratamiento.

V. Las Instituciones deberán contratar con los comisionistas que los periodos de inactividad de la sesión mencionada en el Artículo 319 Bis 2 no podrán durar más de cinco minutos y la duración total de la sesión no podrá exceder de los veinte minutos, ya sea que haya actividad o no por parte del cliente.

En estos casos, se deberá cerrar la sesión de forma automática, así como cualquier comunicación que haya entre la Institución y el cliente, debiendo revocar también los permisos otorgados al comisionista para el acceso a la información del cliente.

VI. Las Instituciones deberán contratar con el comisionista que las páginas de Internet o aplicaciones informáticas del comisionista proporcionen a los clientes, a través de su correo electrónico, un registro de todas las operaciones e instrucciones realizadas durante la sesión a la que se refiere el Artículo 319 Bis 2, el cual deberá mandarse de forma Cifrada al final de dicha sesión.

VII. Las Instituciones deberán publicar en su página de Internet la lista de los certificados y llaves públicas de sus comisionistas, previamente verificada, conforme a lo establecido en la fracción II del Artículo 319 Bis 1.

Además, las Instituciones deberán proporcionar a la Comisión el enlace directo a dicha lista, a fin de que la Comisión lo ponga a disposición del Público Usuario para su consulta en su página de Internet. Para efectos de lo anterior, las Instituciones deberán verificar de forma periódica la validez de los certificados y llaves públicas que estén contenidas en dicha lista.

Asimismo, las Instituciones deberán avisar a la Comisión sobre cualquier cambio o actualización que se realice al enlace o en el contenido de dicha lista.

No será aplicable lo previsto en el Artículo 318, fracción III, inciso b), numeral 1, así como el Artículo 321 Bis 2, ambos de las presentes Disposiciones, a excepción de la contratación con terceros para la prestación de servicios de cómputo bajo demanda y de infraestructura tecnológica a través de Internet para soportar su operación, en virtud de que las operaciones a que se refiere el presente Apartado, no podrán subcontratarse.

Artículo 319 Bis 1. – Las Instituciones deberán estipular con los comisionistas a que se refiere el Artículo 319 Bis de estas Disposiciones, la identificación y segregación de la Infraestructura Tecnológica, páginas de Internet y aplicaciones informáticas que son propiedad de la Institución y las del comisionista, respectivamente, a efecto de que establezcan un canal seguro para el intercambio de información de Autenticación de los clientes y sus operaciones, dicho canal deberá cumplir con, al menos, los siguientes requisitos:

I. El intercambio de información entre las Infraestructuras Tecnológicas de las Instituciones y comisionistas deberá ir Cifrada utilizando, al menos, un método de la Criptografía Matemática Asimétrica cumpliendo con lo establecido en los Artículos 93, 93 Bis, 97 y 107 del Código de Comercio.

II. Previo a que los comisionistas ofrezcan las operaciones de la Institución ante los clientes o potenciales clientes, el comisionista y la Institución que corresponda, deberán proporcionarse recíprocamente (i) un listado con las llaves y certificados públicos asociadas a la Infraestructura Tecnológica que sean de su propiedad o tengan en control, respectivamente, a través de los cuales cada parte procesará el intercambio de los permisos asociados a la Autenticación del cliente y sus operaciones, y (ii) la información que permita identificar a la Infraestructura Tecnológica tanto de la Institución como del comisionista, a efecto de que la Institución y el comisionista se autentiquen recíprocamente para permitir el intercambio de los permisos asociados a la Autenticación del cliente y sus operaciones. Asimismo, la Institución deberá verificar la fiabilidad de las llaves y certificados públicos del comisionista de base tecnológica a fin de identificar aquellas que pudiera resultar apócrifas.

III. Las Infraestructuras Tecnológicas de la Institución y del comisionista deberán llevar a cabo un protocolo de autenticación mutua para permitir el intercambio de los permisos asociados a la Autenticación del cliente y sus operaciones, esto con la finalidad de que solamente el comisionista y la Institución tengan acceso a dicha información.

IV. Una vez que se lleve a cabo el intercambio de información de Autenticación de los clientes y sus operaciones, la información respectiva que se intercambie entre la Infraestructura Tecnológica de la Institución y la del comisionista, deberá ser firmada utilizando la llave privada del emisor de la información y, posteriormente, Cifrada con la llave pública del receptor de la información. En este caso, dependiendo del sentido del flujo de la información, tanto la Institución como el comisionista, tendrán el carácter de emisor o receptor.

Artículo 319 Bis 2. – Las Instituciones que pacten con los comisionistas a que se refiere el Artículo 319 Bis de estas Disposiciones, la apertura de cuentas nivel 2 y otorgamiento de crédito por montos no mayores a tres mil Unidades de Inversión, sin perjuicio del cumplimiento de las obligaciones previstas en otras disposiciones, deberán observar lo siguiente para efectos de Autenticación de los potenciales clientes:

I. Mediante la página de Internet o aplicación informática de los comisionistas, se deberá informar al cliente o potencial cliente que su Autenticación se realizará por la Institución correspondiente, para lo cual esta última le solicitará un Factor de Autenticación Categoría 2 y un Factor de Autenticación Categoría 3, conforme a lo previsto por el Artículo 310 de estas Disposiciones.

   Asimismo, se deberá informar al cliente que para que se lleve a cabo dicha Autenticación, se le redireccionará a la Infraestructura Tecnológica de la Institución, a efecto de que el cliente pueda definir su Factor de Autenticación Categoría 2 e ingresar su Factor de Autenticación Categoría 3.

II. Una vez que el cliente se encuentre en la Infraestructura Tecnológica de la Institución, se deberá solicitar al cliente que:

   i. Defina su Factor de Autenticación Categoría 2.

   ii. Proporcione su correo electrónico o un medio de contacto de mensajería instantánea que utilice protocolos de comunicación Cifrada, a efecto de que la Infraestructura Tecnológica de la Institución envíen a dicho medio de contacto uno de los Factores de Autenticación Categoría 3.

   iii. Ingrese el Factor de Autenticación Categoría 3 en la Infraestructura Tecnológica de la Institución a efecto de que este sea verificado y se asocie al cliente el Factor de Autenticación Categoría 2.

III. Después de haber establecido el Factor de Autenticación de Categoría 2 e ingresado el Factor de Autenticación Categoría 3 a los que se refiere la fracción I del presente artículo, la Institución le otorgará al comisionista los permisos necesarios para poder acceder a la información del cliente y al cliente se le redirigirá a la página de Internet o aplicación informática del comisionista para que dicho cliente pueda realizar la apertura de la cuenta a que se refiere el Artículo 319 Bis, fracción I de las presentes Disposiciones.

En el caso de los redireccionamientos a que se refiere el presente artículo, tanto la Infraestructura Tecnológica de los comisionistas como los de las Instituciones, según sea el caso, deberán informar en un mensaje explícito, claro y visible para el cliente, los motivos por los cuáles se está llevando el redireccionamiento respectivo y en qué paso del proceso de Autenticación se encuentra el cliente.

Los permisos otorgados al comisionista para el acceso a la información del cliente a que se refiere la fracción III del presente artículo, serán revocados una vez que se finalice la sesión en la página de Internet o aplicación informática del comisionista para llevar a cabo las operaciones a que se refiere el Artículo 319 Bis de estas Disposiciones.

Se entenderá por sesión a la interacción entre clientes y las páginas de Internet o aplicaciones informáticas del comisionista de base tecnológica, iniciada por la Autenticación del cliente y finalizada transcurrido el intervalo al que se refiere el Artículo 319 Bis fracción V, durante la cual se podrán llevar a cabo las operaciones a las que hace referencia el Artículo 319 Bis fracción I.

Las Instituciones deberán permitir a sus clientes que utilicen el Factor de Autenticación de Categoría 2 definido por estos en los términos del presente artículo, para Autenticarse en los servicios de Banca Móvil o Banca por Internet de la Institución que corresponda.

Artículo 319 Bis 3. – Las Instituciones que pacten con los comisionistas a que se refiere el Artículo 319 Bis de estas Disposiciones, la celebración de las operaciones referidas en dicho artículo, deberán informar a los clientes, previo a la ejecución de la operación respectiva, que se le solicitará el Factor de Autenticación

Categoría 2 que definió previamente con la Institución y que ingrese un Factor de Autenticación Categoría 3, para que este pueda ser Autenticado por la Institución.

En este caso, las Instituciones deberán proporcionar la Infraestructura Tecnológica para que el cliente ingrese el Factor de Autenticación Categoría 2 y se genere y envíe el Factor de Autenticación Categoría 3 que se le solicitará al cliente para Autenticarlo.

Una vez que el cliente se encuentre en la Infraestructura Tecnológica de la Institución, se le deberá solicitar al cliente que:

i. Ingrese su Factor de Autenticación Categoría 2 para que sea verificado con la información almacenada por la Institución.

ii. Ingrese el Factor de Autenticación Categoría 3 en los Medios Electrónicos de la Institución que reciba en el correo electrónico o el medio de contacto de mensajería instantánea que proporcionó a la Institución previamente.

Después de que la Institución haya realizado la Autenticación del cliente, la Institución le otorgará al comisionista los permisos necesarios para poder acceder a la información del cliente y al cliente se le redirigirá a la página de Internet o aplicación informática del comisionista para que este pueda realizar las operaciones previstas en la fracción I, del Artículo 319 Bis de las presentes Disposiciones.

En caso de los redireccionamientos a que se refiere el presente artículo, tanto la Infraestructura Tecnológica de los comisionistas como los de las Instituciones, según sea el caso, deberán informar en un mensaje explícito, claro y visible al cliente, los motivos por los cuáles se está llevando la redirección respectiva y en qué paso del proceso de Autenticación se encuentra el cliente.

Una vez realizada la Autenticación del cliente, la Institución le deberá permitir al comisionista el acceso a la información del cliente a efecto de que el cliente pueda realizar las operaciones previstas en el Artículo 319 Bis a través de los Infraestructura Tecnológica del comisionista, exclusivamente para la sesión, entendiendo por sesión a lo establecido en el Artículo 319 Bis 2.

Los permisos otorgados al comisionista para el acceso a la información del cliente a que se refiere el párrafo cuarto del presente artículo, serán revocados una vez que se finalice la sesión en la interfaz gráfica que defina el comisionista en su página de Internet o aplicación informática para llevar a cabo las operaciones a que se refiere el Artículo 319 Bis de estas Disposiciones.

Artículo 319 Bis 4.- Las instrucciones de los clientes para la ejecución de operaciones que reciba la Infraestructura Tecnológica del comisionista a que se refiere el Artículo 319 Bis deberán ir Cifradas.

Por lo anterior, la página de Internet o aplicación informática del comisionista deberá realizar el Cifrado con, al menos, la llave o el certificado público del comisionista, la cual (i) deberá estar previamente cargada en las páginas de Internet o aplicaciones informáticas del comisionista o (ii) deberá actualizarse por una instrucción de la Infraestructura Tecnológica del comisionista.

Artículo 319 Bis 5. – Las Instituciones deberán permitir a los clientes modificar el Factor de Autenticación Categoría 2, así como su correo electrónico o medio de contacto de mensajería instantánea que utilice protocolos de comunicación Cifrados por el cual recibe el Factor de Autenticación Categoría 3, que definió en términos del Artículo 319 Bis 2, para lo cual, la página de Internet o la aplicación informática del comisionista deberá prever una opción o enlace explícito, claro y visible que realice el redireccionamiento hacia la Infraestructura Tecnológica de la Institución, a fin de modificar dichos Factores de Autenticación, correo electrónico o medio de contacto de mensajería instantánea que utilice protocolos de comunicación Cifrados.

Para que se lleve a cabo la modificación respectiva, se deberá cumplir con lo previsto en el Artículo 319 Bis 2.

Apartado C

Disposiciones complementarias

Artículo 320.- Las Instituciones que celebren comisiones mercantiles que tengan por objeto llevar a cabo las operaciones a que se refieren los Artículos 319 y 319 Bis de las presentes disposiciones a través de comisionistas, requerirán presentar para autorización de la Comisión, previo a la firma del contrato de comisión mercantil y por única ocasión, un plan estratégico de negocios que contemple la totalidad de las operaciones previstas en los referidos artículos que podrían realizar, y deberá incluir el modelo de contrato de comisión mercantil que servirá de base para los contratos que se celebren con cada uno de los comisionistas con los que se pretenda contratar. Tratándose de instituciones de banca de desarrollo, la autorización del plan estratégico podrá solicitarse una vez obtenida la excepción a que se refiere el Artículo 47 de la Ley.

. . .

El plan estratégico a que se refiere el primer párrafo del presente artículo deberá prever el cumplimiento de los requisitos señalados en el Artículo 318, fracciones I, III, V y VII de las presentes disposiciones, estableciendo las fechas de implementación de cada una de las operaciones en éste señaladas. Asimismo, el referido plan deberá contener los siguientes aspectos:

I. a V. **. . .**

. . .

Artículo 321.- Cuando las Instituciones pretendan realizar operaciones distintas a las señaladas en el plan estratégico que les fue autorizado de conformidad con el Artículo 320 anterior, o bien, pretendan operar con nuevos comisionistas no previstos en el plan autorizado o implementar una nueva tecnología para operar con comisionistas o Administradores de Comisionistas previamente autorizados, deberán sujetarse a lo siguiente:

I. **. . .**

II. Tratándose de las operaciones a que se refieren las fracciones I, IV y XII del Artículo 319 de las presentes disposiciones, deberán presentar un aviso a la Comisión, debiendo manifestar en el mismo que la operación se realizará al amparo del contrato a celebrar entre la Institución y el comisionista, en los términos autorizados por la Comisión, señalando en su caso, si el contrato que pretende celebrar con el comisionista presenta alguna variación que recaiga en un convenio modificatorio respecto del modelo de contrato, en cuyo caso deberá remitir dicho proyecto. El aviso a que se refiere esta fracción deberá enviarse a la Comisión, pudiendo iniciar las operaciones a que se refiere esta fracción al día siguiente de presentado el aviso correspondiente, en el entendido de que la Comisión podrá en cualquier momento requerir que las operaciones no se lleven a cabo a través de algún o algunos comisionistas en particular cuando estos incumplan las presentes disposiciones. Asimismo, las Instituciones podrán incorporar en un mismo aviso todas las operaciones de las señaladas en esta fracción, que se efectuarán con un mismo comisionista.

. . .

III. Tratándose de las operaciones a que se refiere la fracción I del Artículo 319 Bis de las presentes Disposiciones, deberán solicitar autorización a la Comisión, acompañando a su escrito de solicitud lo siguiente:

a) Los requerimientos técnicos que señala el Anexo 59 de las presentes disposiciones y, en su caso, la descripción de la nueva tecnología y su implementación.

b) El proyecto de contrato de comisión mercantil para operar con el comisionista, el cual contemple los aspectos a que se refieren los Artículos 318, fracción III y 324, con excepción del párrafo segundo de la fracción I, de las presentes disposiciones, de conformidad con el plan estratégico de negocios autorizado.

Adicionalmente, para las operaciones referidas en las fracciones I, II y III anteriores, las Instituciones deberán presentar junto con la solicitud de autorización o aviso, según corresponda, el Formato de Certificación Interna de Comisionistas (FCIC) con información de pruebas preoperativas, debidamente llenado en función de la nueva operación que pretendan realizar. Para ello deberán descargar el formato actualizado de dicho reporte disponible en el sitio de Internet de la Comisión.

Artículo 321 Bis.- **. . .**

Artículo 321 Bis 1.- Las Instituciones deberán proporcionar al Público Usuario y al público en general, a través de su página de Internet o en sus sucursales, según corresponda, la información de los comisionistas que tengan habilitados para realizar las operaciones referidas en el Artículo 319 y Artículo 319 Bis de las presentes disposiciones, especificando las operaciones que puede realizar en cada uno de ellos y los montos máximos autorizados por operación.

Asimismo, las Instituciones deberán informar respecto de los comisionistas, siempre que sea aplicable, lo siguiente:

I. Los domicilios legales del comisionista, comprendiendo al menos, su domicilio fiscal y comercial;

II. El listado de los módulos físicos de atención con su dirección física;

III. Las páginas de Internet a través de su nombre de dominio de Internet, tales como los denominados URL (“Uniform Resource Locator”);

IV. Los nombres y logos de las aplicaciones móviles, el nombre del administrador y propietario de la aplicación móvil y las tiendas digitales en donde están disponibles, en su caso;

V. La lista de todos los números telefónicos oficiales que utilizan los comisionistas mismos que deberán estar habilitados para recibir llamadas del público, además de esto, deberán existir la opción de ofrecer la atención telefónica por medio de un empleado del comisionista de base tecnológica;

VI. La lista de correos electrónicos oficiales de contacto;

VII. Las redes sociales utilizadas para realizar promoción, y

VIII. Cualquier otro canal de comunicación que se utilice para interactuar con el público y no esté contemplado en las fracciones anteriores.

Asimismo, las Instituciones deberán verificar que los comisionistas informen a los clientes, a través de los recibos o comprobantes de las operaciones que realizan, anuncios visibles en los establecimientos, plataformas tecnológicas o por cualquier otro medio que utilicen para promocionar con el Público Usuario sus operaciones como comisionista, que actúan en nombre y por cuenta de la propia Institución representada.

Artículos 321 Bis 2 al 323. - . . .

Artículo 324.- . . .

I. a IV. **. . .**

IV. Bis. Tratándose de los comisionistas que se presenten ante los clientes o potenciales clientes a través de sus páginas de Internet o aplicaciones informáticas, se deberá cumplir con lo previsto en los Artículos 319 Bis, 319 Bis 1, 319 Bis 2, 319 Bis 3, 319 Bis 4 y 319 Bis 5.

V. y VI. **. . .**

VII. **. . .**

a) Condicionar la realización de la operación bancaria a la adquisición de un producto o servicio, tratándose de las operaciones a que se refieren las fracciones I a X y XII del Artículo 319 y la fracción I del Artículo 319 Bis de estas disposiciones.

. . .

b) a f) **. . .**

g) Contratar condiciones de exclusividad con la Institución de que se trate, sin perjuicio de los deberes de confidencialidad de la información por parte del comisionista frente a cada Institución con la que pacte los servicios a que se refiere el presente artículo.

VIII. a XI. **. . .**

XII. Tratándose de las operaciones a que se refieren las fracciones IX y X del Artículo 319 y el Artículo 319 Bis, fracción I de las presentes disposiciones, la obligación del comisionista para recabar del cliente la información necesaria y transmitirla en tiempo y forma a la Institución, a fin de dar cumplimiento a lo previsto en el Artículo 115 de la Ley y las “Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones de Crédito”, emitidas por la Secretaría, o las que las sustituyan.

XIII. La obligación del comisionista de elaborar planes de remediación respecto de los hallazgos de las revisiones y pruebas de seguridad efectuadas a las que se refiere la fracción IX del presente artículo y entregarlos a la Institución.

Las Instituciones, en la realización de las operaciones a que se refiere la presente Sección Segunda del Capítulo XI, no podrán contratar comisionistas de forma que les presten de manera exclusiva sus servicios.

Artículo 325.- . . .”

TRANSITORIOS

PRIMERO. - La presente Resolución entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación, salvo lo previsto en el siguiente artículo transitorio.

SEGUNDO. – Las Instituciones contarán con dieciocho meses contados a partir de la entrada en vigor de esta Resolución, para modificar los contratos que tengan celebrados con los terceros a que se refiere el Capítulo XI de estas Disposiciones y dar cumplimiento simultáneamente con las obligaciones derivadas de la

modificación de dichos contratos, por lo que respecta a las reformas aplicables previstas en los Artículos 318, fracciones II y III, inciso a), numeral 3 e inciso b), numeral 1, párrafo segundo y numeral 3; Artículo 321 Bis 1; Artículo 324, fracción VII, inciso g); Anexo 58, fracción I, numeral 5, párrafo segundo, fracción III, numeral 2, segundo párrafo, inciso b) e inciso d), párrafo tercero, inciso b) y Anexo 59, numeral 2 y 6.

Atentamente

Ciudad de México, 3 de julio de 2024.- Presidente de la Comisión Nacional Bancaria y de Valores, Dr. **Jesús de la Fuente Rodríguez**.- Rúbrica.

ANEXO 57

CRITERIOS PARA EVALUAR LA EXPERIENCIA Y CAPACIDAD TÉCNICA DE LOS COMISIONISTAS QUE OPEREN AL AMPARO DE LA SECCIÓN SEGUNDA DEL CAPÍTULO XI DEL TÍTULO QUINTO DE LAS DISPOSICIONES

Se presumirá que los comisionistas cuentan con capacidad técnica suficiente cuando manifiesten bajo protesta de decir verdad que cumplen lo siguiente:

1. Su personal se encuentre capacitado para operar adecuadamente los Medios Electrónicos que la Institución ponga a su disposición para autenticar a los clientes bancarios.

2. Contar con la infraestructura necesaria para llevar a cabo el procesamiento de las operaciones objeto del servicio bancario.

3. Sean personas morales o personas físicas con actividad empresarial y cuenten con (i) establecimiento permanente, entendido éste como cualquier lugar de negocios en el que se desarrollen, parcial o totalmente, actividades empresariales o se presten servicios personales independientes, tales como oficinas, sucursales, agencias, u otras instalaciones en territorio nacional, o (ii) pongan a disposición del Público Usuario una página de Internet o aplicación informática e Infraestructura Tecnológica que permita llevar a cabo los procesos señalados en el Capítulo XI de estas Disposiciones.

4. Tener un giro de negocio propio.

5. Contar con honorabilidad e historial crediticio y de negocios satisfactorio; al efecto, se considerará que cumplen con este requisito los comisionistas que:

   a) Gocen de buen historial crediticio de acuerdo con los Reportes de Información Crediticia y se encuentren al corriente en el cumplimiento de sus obligaciones crediticias.

   b) Por sí o a través de interpósitas personas, no hayan causado quebranto, menoscabo o detrimento patrimonial alguno, en perjuicio de instituciones de crédito o de sociedades emisoras en el mercado de valores.

   c) No hayan sido declarados en concurso civil o mercantil.

   d) En su caso, no hayan sido condenados por sentencia irrevocable por delito doloso que le imponga pena por más de un año de prisión.

   e) En su caso, no hayan sido condenados por sentencia irrevocable por delitos patrimoniales cometidos dolosamente cualquiera que haya sido la pena.

   f) En su caso, no hayan estado sujetos a procedimientos de averiguación o investigación de carácter administrativo ante la Comisión por infracciones graves a las leyes financieras nacionales o extranjeras, o ante otras instituciones supervisoras y reguladoras mexicanas del sistema financiero o de otros países, las cuales hayan tenido como conclusión cualquier tipo de resolución firme y definitiva o convenio en el que no se hubiere determinado expresamente la exoneración del interesado.

Tratándose de Entidades de la Administración Pública Federal, Estatal o Municipal, bastará con que cumplan con lo dispuesto en los numerales 1 y 2 de este Anexo y se encuentren facultadas expresamente por su ley o reglamento, para prestar los servicios o comisiones de que se trate.

Las Instituciones podrán eximir del cumplimiento de los requisitos señalados en los numerales 3, y 5, inciso a) del presente anexo, tratándose de comisionistas administrados por un Administrador de Comisionistas, bastando para ello que el citado Administrador de Comisionistas dé cumplimiento a todos los requisitos previstos por el presente anexo.

ANEXO 58

REQUERIMIENTOS TÉCNICOS PARA LA OPERACIÓN DE MEDIOS ELECTRÓNICOS PARA LAS OPERACIONES CONTEMPLADAS EN LA SECCIÓN SEGUNDA DEL CAPÍTULO XI DEL TÍTULO QUINTO DE LAS DISPOSICIONES

Los Medios Electrónicos que utilicen las Instituciones para garantizar la correcta ejecución de las operaciones bancarias que se realicen a través de comisionistas y de seguridad de la información de los clientes bancarios y del público en general, deberán cumplir con los requerimientos a que se refiere el presente anexo.

La Institución deberá contar con la evidencia de la verificación de cumplimiento realizada previo al inicio de operaciones y al menos una vez al año, de los siguientes aspectos y tenerla a disposición de la Comisión cuando esta así la requiera.

Tratándose de Administradores de Comisionistas, estos deberán verificar que los comisionistas que conformen su red cumplan con lo establecido en el presente Anexo.

Para efectos del presente Anexo se entenderá como “Operador” al empleado del comisionista que tenga acceso a los Medios Electrónicos.

I. Requerimientos de los Medios Electrónicos

1. Mecanismos necesarios para realizar las transacciones en línea.

   Los Medios Electrónicos deberán contar con los mecanismos necesarios para realizar las transacciones en línea, es decir, al instante mismo en que se lleve a cabo la operación, actualizando los saldos del cliente en línea salvo tratándose de las operaciones referidas en las fracciones I, IV y XII el Artículo 319 de las presentes disposiciones, donde podrán realizar la actualización de saldos en apego a lo establecido por las reglas de operación de las propias Instituciones.

   Para tales efectos, las operaciones de pago de servicios en efectivo o con tarjeta de débito, o con cargo a Cuentas Bancarias, depósito de efectivo, pago de créditos en efectivo y situación de fondos; deberán registrarse como un cargo a la cuenta de depósito que el comisionista tenga con la Institución. Por su parte, las operaciones de retiro de efectivo y pago de cheques deberán registrarse como un abono a la misma cuenta.

   En los casos en que la información del saldo del cliente se almacene en dispositivos tales como tarjetas con circuito integrado o equipos ubicados en las instalaciones de los comisionistas, no se considerará como afectación en línea la realizada en tales dispositivos, siempre y cuando existan mecanismos para su consolidación periódica en los sistemas centrales de las Instituciones.

   Tratándose de las operaciones referidas en las fracciones I y IV del Artículo 319, así como en la fracción I, inciso c) del Artículo 319 Bis, de las presentes disposiciones y en caso de que el procesamiento se realice a través del esquema batch, deberán mantener controles implementados para el envío seguro de los archivos, así como para la conciliación y liquidación de las operaciones que se realicen a través de este medio.

2. Validación de Medios Electrónicos del comisionista.

   Únicamente los Medios Electrónicos de los comisionistas autorizados por la Institución tendrán acceso a la infraestructura dispuesta por aquélla (uso de líneas dedicadas, identificación de direcciones físicas o lógicas, VPNs, firmas digitales, entre otros).

   Los sistemas informáticos de la Institución deberán autenticar a los Medios Electrónicos que los comisionistas utilicen para realizar operaciones bancarias.

3. Certificación de Medios Electrónicos del comisionista.

La Institución será responsable de certificar la instalación y el uso de los Medios Electrónicos que el comisionista mantenga para la realización de las operaciones bancarias, así como de establecer evaluaciones anuales de dichos Medios Electrónicos. Dicha certificación podrá realizarla la Institución, en su caso, a través de sus áreas técnicas especializadas en seguridad de la información o auditoría interna de sistemas, o bien, a través de terceros independientes, contratados por la propia Institución, quienes deberán acreditar ante la misma, que cuentan con credenciales técnicas adecuadas en materia de auditoría informática o de sistemas.

La certificación antes mencionada, deberá considerar al menos que la Institución deberá cerciorarse en todo momento que los medios electrónicos utilizados por los comisionistas mantienen mecanismos de control que eviten la lectura y extracción de la información de los clientes por terceros no autorizados.

4. Políticas y procedimientos para la administración de accesos y configuración de Medios Electrónicos.

   Es responsabilidad de la Institución verificar que el comisionista cuente con políticas y procedimientos para:

   a) La configuración de la Infraestructura Tecnológica que se conecte a los sistemas informáticos de la Institución.

   b) La administración de llaves criptográficas utilizadas entre los comisionistas y los sistemas de la Institución.

5. Generación de registros electrónicos de operaciones.

   Todas las operaciones realizadas a través de los comisionistas deberán generar registros electrónicos que no puedan ser modificados o borrados y en los que se deberá incluir al menos la fecha, hora y minuto, el tipo y monto de la instrucción, el número de cuenta del cliente bancario, ubicación física de la ventanilla o medio a través del cual se ejecutó la instrucción, así como la información suficiente que permita la identificación del personal que realizó la instrucción, así como información de auditoría que consideren al menos, cliente, direcciones IP de origen y destino, fecha, hora, nombre de la interfaz de programación de aplicaciones (API por sus siglas en inglés), tipo de petición, versión y código de respuesta a efecto de contar con trazabilidad de los eventos en los sistemas de la Institución y del comisionista. La custodia de dichos registros deberá estar a cargo de la Institución.

II. Requerimientos de Identificación de Operadores y Autenticación clientes bancarios.

1. Mecanismos necesarios para la plena identificación de los Operadores que se conectarán a través de los comisionistas.

   Tratándose de la identificación de los Operadores de los comisionistas de base tecnológica a que se refiere el numeral 6, del inciso a), de la fracción III, del Artículo 318 de estas Disposiciones, se deberá observar lo mencionado en el Apartado II Bis “Identificación de Operadores de los comisionistas de base tecnológica” del presente Anexo.

2. Generación y entrega de Contraseñas, Contraseñas dinámicas de un solo uso o Claves de Acceso de los Operadores.

   Las Instituciones deberán establecer mecanismos para el proceso de generación y entrega de los Factores de Autenticación que aseguren que sólo el comisionista, y en su caso, los Operadores podrán conocer.

3. Composición de Contraseñas, Contraseñas dinámicas de un solo uso o Claves de Acceso de los Operadores.

   Deberán establecerse criterios para las características de la longitud de las Contraseñas, Contraseñas dinámicas de un solo uso o Claves de Acceso de los Operadores.

3 Bis. Vigencia de Contraseñas, Contraseñas dinámicas de un solo uso o Claves de Acceso de los Operadores.

   Las Instituciones deberán establecer criterios para la vigencia de las Contraseñas, Contraseñas dinámicas de un solo uso o Claves de Acceso, a fin de fortalecer los procesos de identificación de los Operadores del comisionista de base tecnológica. En el caso de las Contraseñas dinámicas de un solo uso, su vigencia no podrá superar 1 minuto y para las Contraseñas o Claves de acceso que no correspondan a Factores de Autenticación de Categoría 4 esta vigencia no podrá superar los 90 días hábiles.

4. Protección de Contraseñas o Claves de Acceso y Números de Identificación Personal (NIP).

   Las Instituciones deberán proveer lo necesario para evitar la lectura de los caracteres que componen las Contraseñas o Claves de Acceso, así como los Números de Identificación Personal (NIP) digitados por los clientes bancarios, respectivamente, en los Medios Electrónicos de acceso, tanto en su captura como en su despliegue a través de la pantalla.

   Las Contraseñas o Claves de Acceso y los Números de Identificación Personal (NIP) deberán validarse y almacenarse a través de mecanismos de cifrado, cuyas llaves criptográficas deberán estar bajo administración y control de la Institución de que se trate. En ningún momento, los comisionistas podrán tener acceso a los datos o algoritmos relacionados con dichas Contraseñas o Claves de Acceso y Números de Identificación Personal (NIP).

   Los comisionistas deberán de contar con certificaciones de normas de seguridad de la industria de tarjetas de los requisitos de seguridad y transacciones con NIP (PTS) o sus equivalentes o aquellos que, a criterio de la Comisión, permitan la debida protección de la información almacenada, transmitida o procesada relacionada con el ingreso de los Números de Identificación Personal (NIP) de los clientes bancarios y los datos de las tarjetas bancarias.

5. Autenticación para clientes bancarios.

   Para la realización a través de los comisionistas de consultas y operaciones que representen un cargo a la cuenta de los clientes bancarios, éstos últimos deberán autenticarse a través de los Medios Electrónicos con los que se realicen las mencionadas operaciones utilizando dos Factores de Autenticación diferentes. Lo anterior, no será aplicable para los comisionistas a que se refiere el Artículo 319 Bis de estas Disposiciones.

   Para efectos de lo anterior, las Instituciones podrán optar por la combinación de al menos dos de los siguientes Factores de Autenticación y ajustarse a lo dispuesto en el Capítulo X del Título Quinto de las presentes Disposiciones:

   a) Tarjetas de débito o crédito con mecanismos de seguridad tales como tarjetas con banda magnética y/o circuito integrado o “chip”.

   b) Número de Identificación Personal (NIP).

      En el caso de que se utilicen tarjetas de débito o crédito, se deberá hacer uso de lectoras de tarjetas, tales como PIN PADS, para la Autenticación de clientes bancarios, que cuenten con una pantalla y un teclado exclusivamente diseñado para que el cliente bancario pueda ingresar la información de su respectiva tarjeta y su Número de Identificación Personal (NIP), así como con mecanismos que eviten su lectura por parte de terceros.

      Los comisionistas deberán de contar con certificaciones de normas de seguridad de la industria de tarjetas de los requisitos de seguridad y transacciones con NIP (PTS) o sus equivalentes o aquellos que, a criterio de la Comisión, permitan la debida protección de la información almacenada, transmitida o procesada relacionada con el ingreso de los Números de Identificación Personal (NIP) de los clientes bancarios y los datos de las tarjetas bancarias.

      En el caso de utilizar teléfono celular, el Número de Identificación Personal (NIP) deberá ser ingresado directamente en el teclado de dicho teléfono. En ningún caso la información del NIP podrá ser almacenada en el teléfono celular sin mecanismos de cifrado.

   c) Factor Biométrico.

      En caso de utilizar lectores biométricos para la Autenticación de los clientes bancarios, dichos lectores deberán tener mecanismos que aseguren que es el cliente autorizado el que realiza la operación, así como implementar mecanismos o procedimientos para que el comisionista no almacene la información procesada relacionada con los factores biométricos de los clientes.

      Toda la administración y control de la información biométrica deberá ser responsabilidad única de la Institución a través de los canales de atención al cliente que tienen establecidos.

   d) Teléfono celular.

      En caso de utilizar teléfonos celulares para la Autenticación de los clientes bancarios, las Instituciones deberán verificar que la tecnología de dichos teléfonos celulares les permita funcionar como Factor de Autenticación y que cuenta con mecanismos de seguridad que eviten su duplicación o suplantación.

Las Instituciones no podrán utilizar la combinación de los Factores de Autenticación a que se refieren los incisos a) y d) para autenticar a sus clientes.

6. Autenticación para Operadores.

   Para la recepción y operación de transacciones solicitadas por los clientes bancarios a través de los Medios Electrónicos de los comisionistas, los Operadores deberán iniciar una sesión y autenticarse a través de dichos Medios.

   Los procesos de autenticación deberán ser validados por la Institución, a través de los mecanismos y controles que esta estime convenientes. Será responsabilidad de la Institución asegurarse de que los comisionistas cuenten con dichos mecanismos de autenticación de operadores, para la realización de las operaciones.

7. Bloqueo de los Factores de Autenticación de los Operadores.

   Se deberán establecer esquemas de bloqueo de los Factores de Autenticación de los Operadores cuando se intente ingresar a los Medios Electrónicos de forma incorrecta. En ningún caso los intentos de acceso fallidos podrán exceder de cinco ocasiones consecutivas sin que se genere el bloqueo automático.

8. Acceso a datos del cliente bancario.

   En ningún caso los Medios Electrónicos utilizados por los comisionistas podrán permitir la realización de operaciones o consulta de saldos sin la previa Autenticación en términos del numeral 5 del apartado II “Requerimientos de Identificación de Operadores y Autenticación clientes bancarios” del presente anexo, del cliente correspondiente. Quedarán exceptuadas para este caso las operaciones de depósito y pagos.

   Asimismo, tratándose de operaciones bancarias que requieran que el comisionista acceda a los saldos de las cuentas de los clientes bancarios, dicho comisionista deberá, en todo momento, guardar confidencialidad respecto de dicha operación y realizar previamente al acceso respectivo, la Autenticación referida en el numeral 1 del apartado III “Operaciones de Medios Electrónicos” del presente anexo.

II. Bis Identificación de Operadores de los comisionistas de base tecnológica

Adicional a lo previsto en la fracción II “Requerimientos de Identificación de Operadores y Autenticación clientes bancarios” del presente Anexo, las Instituciones deberán solicitar a los comisionistas de base tecnológica realizar la identificación de sus Operadores a efectos de dar cumplimiento a lo establecido en el numeral 6, inciso a), fracción III del Artículo 318 de estas Disposiciones.

Para lo anterior, los comisionistas de base tecnológica deberán solicitar a sus Operadores, al menos, un Factor de Autenticación de Categoría 2 y un Factor de Autenticación de Categoría 3, observando lo siguiente:

1. A efectos de que el Operador establezca un Factor de Autenticación de Categoría 2 para su identificación, el comisionista de base tecnológica deberá observar lo siguiente:

   a) El comisionista de base tecnológica deberá generar y proporcionar al Operador un Factor de Autenticación de Categoría 3, el cual será enviado al correo institucional que el Operador proporcionó en el documento al que se refiere numeral 6, inciso a), fracción III del Artículo 318 de estas Disposiciones.

   b) El comisionista de base tecnológica le deberá solicitar al Operador el Factor de Autenticación de Categoría 3 que se le proporcionó según lo establecido en el inciso a) del presente numeral.

   c) El Operador deberá ingresar en la Infraestructura Tecnológica del comisionista de base tecnológica el Factor de Autenticación de Categoría 3 al que se refiere el inciso b) del presente numeral, verificando la validez de dicho Factor.

   d) Una vez que el comisionista de base tecnológica verifique la validez del Factor de Autenticación de Categoría 3 al que se refiere el inciso c) anterior, el comisionista de base tecnológica le deberá solicitar al Operador definir un Factor de Autenticación de Categoría 2, el cual únicamente podrá ser utilizado por éste a fin de proteger su información de identificación.

2. Para que el comisionista de base tecnológica identifique al Operador, le deberá solicitar, al menos, (i) el Factor de Autenticación Categoría 2 establecido por Operador conforme a lo mencionado en el numeral 1 de la presente fracción, y (ii) un Factor de Autenticación de Categoría 3, debiendo observar lo siguiente:

   a) Previo a que el comisionista de base tecnológica realice la identificación del Operador, el comisionista de base tecnológica deberá generar y proporcionar al Operador un Factor de Autenticación de Categoría 3. Este Factor de Autenticación de Categoría 3 deberá ser enviado al correo institucional que el Operador proporcionó en el documento al que se refiere numeral 6, inciso a), fracción III del Artículo 318 de estas Disposiciones.

   b) El comisionista de base tecnológica deberá solicitar al Operador el Factor de Autenticación de Categoría 2 establecido por el Operador y el Factor de Autenticación de Categoría 3 proporcionado por el comisionista de base tecnológica, a efectos de realizar la identificación del Operador.

3. El comisionista de base tecnológica le deberá proporcionar al Operador los medios necesarios para modificar el Factor de Autenticación de Categoría 2 debiendo observar lo previsto en el numeral 1 de la presente fracción.

4. En el caso de que un Operador deje de realizar los procesos informados en el documento entregado a la Institución según lo establecido en el segundo párrafo del numeral 6, inciso a), fracción III del Artículo 318 de estas Disposiciones, el comisionista de base tecnológica deberá revocar los permisos de acceso de su Infraestructura Tecnológica, a fin de proteger la integridad de los procesos ejecutados por el comisionista de base tecnológica y la operatividad de la Institución.

III. Operación de Medios Electrónicos

1. Validación de estructura de cuenta destino.

   Los Medios Electrónicos de los comisionistas deberán validar, con base en la información disponible para la Institución, la estructura del número de la cuenta destino o del contrato, sea que se trate de cuentas para depósito, pago de servicios, Clave Bancaria Estandarizada, tarjetas de crédito u otros medios de pago.

2. Generación de comprobantes de operación.

   Los Medios Electrónicos deberán generar automáticamente los comprobantes de operación que emitan las Instituciones para cada operación, sin mediar intervención alguna por parte del personal del comisionista. Dichos comprobantes de operación serán diferentes a aquéllos que utilicen los comisionistas para registrar las operaciones propias de su giro comercial y deberán incluir lo dispuesto por las Disposiciones de carácter general de la CONDUSEF en materia de transparencia y sanas prácticas aplicables a las instituciones de crédito. En adición a las referidas disposiciones, las Instituciones deberán considerar en los comprobantes de operación lo siguiente:

   a) Los datos que permitan al cliente bancario identificar la cuenta respecto de la cual se efectuó la operación. En ningún momento se deberá mostrar en los comprobantes el número completo de la cuenta.

   b) La información de las consultas de saldos, cuando el cliente así lo haya solicitado y autorizado, en cuyo caso deberá ser proporcionada únicamente al cliente a través del comprobante correspondiente, la página de Internet o aplicación informática del comisionista. El comisionista no podrá resguardar o conservar información relacionada o asociada en medios físicos o digitales.

   c) La identificación de la Institución y del comisionista con el que se efectuó la operación, precisando en este último caso, el domicilio del establecimiento o dirección de la página de Internet o aplicación informática a través del cual se ejecutó la instrucción.

   d) La información que permita la identificación del personal del comisionista que realizó la instrucción donde, al menos, aparezca el nombre completo del funcionario o empleado del comisionista.

   Cuando se rebasen los límites a que se refiere el Artículo 323 de las presentes disposiciones, según corresponda, no se podrán llevar a cabo las operaciones solicitadas, por lo que los Medios Electrónicos deberán generar comprobantes que indiquen al cliente bancario, dicha

situación. Para tales efectos, se deberá proporcionar un comprobante que incluya las leyendas siguientes:

a) En el caso del límite a que se refiere el Artículo 323, fracción II, inciso b) de las presentes Disposiciones: “Transacción no realizada por haber excedido su límite permitido. Acuda a una sucursal bancaria.”

b) En el caso de los límites a que se refiere el Artículo 323, fracciones I y II, inciso a) de las presentes Disposiciones, según corresponda: “Transacción no realizada”. Por ningún motivo deberá mostrarse en el comprobante de operación el domicilio del cliente. Asimismo, el domicilio no deberá mostrarse a ningún empleado o funcionario del comisionista durante la generación de dicho comprobante.

Las Instituciones pondrán a disposición de sus clientes en los comprobantes de operación la información relativa al número telefónico y correo electrónico de la unidad especializada de atención a usuarios con que la Institución debe contar en términos de la Ley de Protección y Defensa al Usuario de Servicios Financieros, así como del centro de atención de la Institución.

Todos los comprobantes de operaciones que se celebren a través de comisionistas tendrán valor probatorio para fines de cualquier aclaración y deberán ser reconocidos en esos términos por parte de las Instituciones que los emitan.

3. Monitoreo de operaciones.

La Institución deberá establecer mecanismos continuos mediante herramientas informáticas que le permitan monitorear las actividades realizadas por los Operadores a través de los Medios Electrónicos de los comisionistas con el fin de detectar transacciones que se alejen de los parámetros habituales de operación.

4. Almacenamiento de Información Sensible del Usuario bancario en Medios Electrónicos de los comisionistas.

En los casos que por razones operativas y técnicas se requiera almacenar parcial o totalmente Información Sensible del Usuario de la Institución en los Medios Electrónicos del comisionista, la institución deberá verificar que existan mecanismos de cifrado. Asimismo, los comisionistas no podrán emitir un duplicado de los comprobantes de consultas de saldos o mantener copias de estos.

5. La Institución deberá contratar con el comisionista de base tecnológica que, al acceder los clientes a las Interfaces gráficas de página de Internet o aplicaciones informáticas del comisionista, estas deberán proporcionar información detallada y suficiente que identifique la celebración de operaciones con la Institución para lo cual podrá utilizar imágenes, letras o colores visibles relacionados con la misma.

6. La Institución estará obligada a notificar a sus clientes, a la brevedad posible y a través de los medios de comunicación que pongan a su disposición y que estos hayan elegido para tal fin, las operaciones a que se refieren los incisos a), b) y c) de la fracción I, del Artículo 319 Bis realizadas a través de los comisionistas de base tecnológica.

IV. Seguridad de la Información

1. 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 o matriz, Administradores, comisionistas y otros terceros, considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (DMZ por sus siglas en inglés).

2. Configuración segura de componentes, considerando al menos, puertos y servicios, 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.

3. Medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada en la infraestructura tecnológica, contando al menos con lo siguiente:

a) Mecanismos de identificación y autenticación de todos y cada uno de los usuarios de la infraestructura tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el

acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio. Para lo anterior, se deberán incluir controles pertinentes para aquellos usuarios de la infraestructura tecnológica con mayores privilegios, derivados de sus funciones, tales como, la de administración de bases de datos y de sistemas operativos.

b) Cifrado de la información conforme al grado de sensibilidad o clasificación que la Institución determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes, o almacenada en la infraestructura tecnológica o se acceda de forma remota.

c) Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el usuario de la Infraestructura Tecnológica sea quien las conozca, así como medidas de seguridad, cifrado en su almacenamiento y mecanismos para cambiar las claves de acceso cada 90 días o menos.

d) Controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de usuario de la infraestructura tecnológica.

e) Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la infraestructura tecnológica y permitan la operación conforme a las especificaciones del proveedor, fabricante o desarrollador.

f) Medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la infraestructura tecnológica, considerando, al menos lo siguiente:

i. La veracidad e integridad de la información.

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 transacciones atípicas, previendo que las aplicaciones cuenten con medidas de alerta automática para su atención de las áreas operativas correspondientes.

g) La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones.

4. Mecanismos automatizados para detectar y prevenir eventos e incidentes de seguridad de la información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información, considerando entre otros, medios de almacenamiento removibles.

5. Políticas y procedimientos de administración de llaves de cifrado utilizadas por la Institución y el comisionista, en su caso.

6. Políticas y procedimientos de borrado seguro para la destrucción de los datos cuando dejan de ser necesarios, o en la conclusión de la comisión mercantil.

7. Políticas y procedimientos para la gestión de incidentes de seguridad de la información de los comisionistas que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a niveles jerárquicos competentes, solución, seguimiento y comunicación inmediata a la Institución y contrapartes de dichos incidentes.

8. Registro en bases de datos, de los incidentes, fallas o vulnerabilidades detectadas en la Infraestructura Tecnológica del comisionista, que incluya al menos 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 del comisionista, en donde se contemple la fecha del suceso y una descripción de este, su duración, servicio o canal afectado, montos, así como las medidas correctivas implementadas.

Asimismo, 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.

9. Realización de pruebas de escaneo de vulnerabilidades de los componentes de la infraestructura tecnológica de los comisionistas que almacenen, procesen o transmitan información de las operaciones bancarias. Dichas pruebas deberán realizarse al menos trimestralmente.

10. Realización de pruebas de penetración por un tercero independiente, cuyo personal cuente con capacidad técnica comprobable mediante certificaciones especializadas en la materia, dichas pruebas deberán contemplar la infraestructura tecnológica del comisionista para la comisión mercantil. Las pruebas deberán considerar, al menos lo siguiente:

    a) Su alcance y metodología.

    b) Ser realizadas al menos una vez al año.

    c) Se deberán efectuar pruebas adicionales, cuando existan cambios significativos en los sistemas y aplicativos, o realizarlas sobre sistemas y aplicativos previamente revisados cuando existan vulnerabilidades críticas.

11. Seguimiento continuo a los planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren los numerales 9 y 10 anteriores. Dichos planes deberán ser revisados por la institución y dar seguimiento de las acciones implementadas para su mitigación.

12. Contar con controles de acceso a la información de acuerdo con los niveles de acceso y perfiles determinados por la Institución.

V. Requerimientos para la operación a que se refiere la fracción IX del Artículo 319 de las presentes disposiciones

1. Que los sistemas de la Institución, así como, en su caso, los de las casas de bolsa con las que pretendan celebrar comisiones mercantiles, cuenten con los requerimientos técnicos necesarios que les permitan dar cumplimiento con lo dispuesto en el Artículo 124 de la Ley, así como para recibir y transmitir la información a que se refieren las “Reglas de carácter general a las que deberán sujetarse las instituciones de banca múltiple para clasificar la información relativa a operaciones activas y pasivas a que se refiere el Artículo 124 de la Ley de Instituciones de Crédito”, y a las emitidas por el IPAB, o las que las sustituyan, incluyendo lo señalado en el numeral 3 siguiente.

2. Los procedimientos a través de los cuales la Institución autorizará a las casas de bolsa para realizar tales operaciones.

3. La obligación de la casa de bolsa comisionista para:

    a) Recabar del cliente la información necesaria a fin de dar cumplimiento a lo previsto en el Artículo 115 de la Ley y las "Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones de Crédito" emitidas por la Secretaría, o las que las sustituyan.

    Para ello, las casas de bolsa deberán transmitir en tiempo y forma a la Institución la información relativa a las mencionadas operaciones, a fin de que la propia Institución dé cumplimiento al citado Artículo 115 de la Ley y las "Disposiciones de carácter general a que se refiere el Artículo 115 de la Ley de Instituciones de Crédito" emitidas por la Secretaría, o las que las sustituyan.

    b) Tratándose de operaciones celebradas con instituciones de banca múltiple comitentes:

        i. Recabar y clasificar en sistemas automatizados de procesamiento y conservación de datos, así como en cualesquier otro procedimiento técnico, toda la información que le permita a la institución de banca múltiple dar cumplimiento a la Tercera de las "Reglas de carácter general a las que deberán sujetarse las instituciones de banca múltiple para clasificar la información relativa a operaciones activas y pasivas a que se refiere el Artículo 124 de la Ley de Instituciones de Crédito" emitidas por el IPAB o las que las sustituyan;

        ii. Transmitir a la institución de banca múltiple comitente, simultáneamente al momento de la celebración de cada operación, a través de sus sistemas, la información que de conformidad con las Reglas referidas en el numeral anterior, esta última deba mantener. Lo anterior, sin perjuicio de que los contratos a que se refiere el presente artículo deberán contener la obligación a cargo de las casas de bolsa que actúen como comisionistas, de transmitir a las instituciones de banca múltiple comitentes, toda la información referida en la Tercera de las Reglas mencionadas en el numeral i. anterior, cuando así les sea requerido por la Comisión, directamente o a petición del IPAB, siempre que se actualicen los supuestos correspondientes a la resolución de la institución de banca múltiple comitente en términos del Artículo 122 Bis de la Ley;

iii. Obtener del cliente al momento de celebrar las operaciones, una manifestación por escrito o por cualquier medio que se pacte con el cliente bancario, en los términos del formato contenido como Anexo 60 de las presentes disposiciones, y

iv. Entregar al cliente, en el reverso del documento a que se refiere el numeral iii. anterior, o por cualquier medio que se pacte con el cliente bancario, un texto informativo en los términos establecidos en el Anexo 61 de las presentes disposiciones.

c) Los términos bajo los cuales deberá efectuarse la liquidación de las operaciones.

En caso de que la liquidación de las operaciones respectivas se lleve a cabo en las oficinas de las casas de bolsa, entregar al cliente el importe respectivo en la forma en que se pacte al momento de la contratación. En todo caso, si el cliente no solicita a la oficina la referida liquidación en un plazo de tres días hábiles contados a partir de la fecha de vencimiento de la operación, la casa de bolsa quedará liberada de la obligación de realizar el pago correspondiente a favor del cliente, por lo que la liquidación deberá efectuarse directamente con la Institución.

4. La obligación por parte de la Institución de proveer los medios necesarios a fin de dar cumplimiento a las disposiciones a que se refieren los numerales 1 y 2 anteriores y, en general, a lo establecido por las disposiciones relativas al sistema de protección al ahorro bancario, así como de asegurarse de que el comisionista efectivamente cumple lo anterior.

Anexo 59

Información que deberá presentarse en la solicitud de autorización del comisionista

La información para presentarse en la solicitud de autorización del comisionista deberá contener al menos lo siguiente:

1. Descripción detallada y diagrama de flujo de los procesos de cada una de las operaciones a realizar a través de los comisionistas considerando 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.
2. Diagrama de arquitectura y telecomunicaciones en el que se muestren los componentes de seguridad, de redes y bases de datos de la infraestructura tecnológica utilizada para la operación con comisionistas, que aseguren que solamente el tráfico autorizado es el permitido. Dicho diagrama deberá incluir a cada uno de los participantes, así como todos los sitios de procesamiento de información incluyendo los esquemas de redundancia, tipos de enlace y rutas de respaldo, servidores y dispositivos de comunicación.
3. Las ubicaciones completas y detalladas de los centros de datos principal y de respaldo, tanto de la Institución, del comisionista o del proveedor de la infraestructura tecnológica del comisionista en donde será almacenada y/o procesada la información de las transacciones realizadas a través del comisionista (calle, número exterior e interior, colonia, alcaldía o municipio, estado y país).
4. Diagrama de interrelación de aplicaciones o sistemas del comisionista, incluyendo los sistemas propios de la Institución. (Deberá Incluir a todos los participantes involucrados en la operación (p.e.: comisionista, *switches*, procesadores de medios de pago, terceros y la propia Institución).
5. Detalle de la Información Sensible que será almacenada por el comisionista en sus equipos o instalaciones, o del proveedor de la infraestructura tecnológica del comisionista, o a la que podrán tener acceso. Tratándose de Información Sensible, el comisionista o deberá implementar mecanismos de almacenamiento cifrado.
6. Estructura del personal del comisionista y del proveedor de la infraestructura del comisionista con acceso a la información de las transacciones realizadas a través del comisionista y la Información Sensible asociada, que incluya como mínimo cargo, nivel jerárquico del mismo y responsabilidades y actividades autorizadas relacionadas a dicha Información para dicho cargo.
7. Incluir las características de los comprobantes de operación, adjuntar el diseño de comprobante de cada una de las operaciones a contratar.
8. Descripción de las medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la infraestructura tecnológica, considerando, al menos lo siguiente:
   a) La veracidad e integridad de la información.
   b) 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.
   c) Los protocolos de mensajería, comunicaciones y cifrado, los cuales deben procurar la integridad y confidencialidad de la información.

d) La identificación de transacciones atípicas, previendo que las aplicaciones cuenten con medidas de alerta automática para su atención de las áreas operativas correspondientes.

9. Un listado que contenga todas las llaves y los certificados públicos de las páginas de Internet o aplicaciones informáticas del comisionista para aquellos comisionistas a que se refiere el Artículo 319 Bis de las presentes Disposiciones.
10. Descripción de mecanismos automatizados para detectar y prevenir eventos e incidentes de seguridad de la información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información, considerando entre otros, medios de almacenamiento removibles.
11. Informe detallado de resultados de pruebas de escaneo de vulnerabilidades de los componentes de la infraestructura tecnológica de los comisionistas que almacenen, procesen o transmitan información de las operaciones bancarias.
12. Informe de resultados detallado de las pruebas de penetración realizadas por un tercero independiente, cuyo personal cuente con capacidad técnica comprobable mediante certificaciones especializadas en la materia, dichas pruebas deberán contemplar la infraestructura tecnológica del comisionista para la comisión mercantil.
13. Planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren los numerales 9 y 10 anteriores, así como la evidencia de las acciones de mitigación implementadas para subsanar las vulnerabilidades de severidad críticas y altas.
14. Documentación de los Formatos de Certificación Interna de Comisionistas (FCIC) relativa a las pruebas preoperativas de las operaciones a los comisionistas.
