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 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. 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.

2. Generación y entrega de Contraseñas 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 o Claves de Acceso de los Operadores.

   Deberán establecerse criterios para las características de la longitud de las Contraseñas o Claves de Acceso de los Operadores.

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.

   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.

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. El comisionista no podrá emitir un duplicado de dicho comprobante o mantener copia de este.

   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 a través del cual se ejecutó la instrucción.

   d) La información que permita la identificación del personal del comisionista que realizó la instrucción.

   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.

   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.

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 breve 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.