ANEXO 58

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

Los Medios Electrónicos que utilicen las Instituciones para garantizar la correcta ejecución de las operaciones bancarias 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.

I. Definiciones.

Para efectos del presente anexo, en adición a las definiciones señaladas en el Artículo 1 de las presentes disposiciones, se entenderá por:

1. Identificador Individual: La cadena de caracteres asignada a cada Operador en lo individual.

2. Operador: El empleado del comisionista Usuario que tenga acceso a los Medios Electrónicos.

II. 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 el Artículo 319, fracción IV, de las disposiciones.

   Para tales efectos, las operaciones de pago de servicios en efectivo o con tarjeta de débito, o prepagadas o con cargo a Cuentas Móviles, depósito de efectivo, pago de créditos en efectivo, situación de fondos y colocación de tarjetas prepagadas o de Cuentas Móviles; 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.

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.

   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 mecanismos periódicos de evaluación de dichos Medios Electrónicos.

   Asimismo, 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.

   La Institución deberá contar con políticas y procedimientos para la:

a) Administración de los accesos y perfiles de los empleados de los comisionistas a sus sistemas informáticos.

b) Capacitación a los comisionistas en el uso de los Medios Electrónicos. Dicha capacitación deberá incluir aspectos relacionados con la protección de la información de los clientes bancarios.

c) Configuración de los Medios Electrónicos que se conecten a sus sistemas informáticos.

d) Administración de llaves criptográficas utilizadas entre los comisionistas y sus sistemas.

5. Transmisión de datos Cifrada.

   Las Instituciones deberán cifrar el mensaje o utilizar medios de comunicación Cifrada para la transmisión de la Información Sensible del Usuario, desde el punto de originación de la operación hasta los sistemas centrales de la Institución, para llevar a cabo consultas, Operaciones Monetarias y cualquier otro tipo de transacción bancaria, entre la Institución y sus clientes utilizando los Medios Electrónicos de los comisionistas.

6. 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, minuto y segundo, 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.

III. Requerimientos de Autenticación de Operadores y clientes bancarios.

1. Mecanismos necesarios para la plena identificación de los comisionistas.

   Los sistemas informáticos de la Institución deberán autenticar a los Operadores que se conectarán a través de los comisionistas, mediante el uso de un Identificador Individual, en su caso, más dos Factores de Autenticación diferentes.

   Asimismo, los sistemas informáticos deberán evitar el acceso en forma simultánea, mediante la utilización de un mismo Identificador Individual, en su caso, a los sistemas de información de la Institución.

2. Generación y entrega de Contraseñas o Claves de Acceso de los Operadores y Números de Identificación Personal (NIP) de los clientes bancarios.

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

3. Composición de Contraseñas o Claves de Acceso de los Operadores y Números de Identificación Personal (NIP) de los clientes bancarios.

   La longitud de las Contraseñas o Claves de Acceso de los Operadores deberá ser de al menos ocho caracteres.

   La longitud de los Números de Identificación Personal (NIP) de los clientes bancarios deberá ser de al menos cuatro caracteres.

Adicionalmente, deberán realizarse las acciones necesarias para que los Operadores y los clientes bancarios no utilicen como Contraseñas o Claves de Acceso o Números de Identificación Personal (NIP), respectivamente, más de dos caracteres idénticos en forma consecutiva.

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 Operadores y 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 encripción, 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).

5. Autenticación con dos factores 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:

   a) Tarjetas de débito, crédito o prepagada 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, crédito o prepagadas bancarias, se deberá hacer uso de lectoras de tarjetas (PIN PAD) 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.

      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 encripción.

   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.

      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, y ajustarse a lo dispuesto en el Capítulo X del Título Quinto de las presentes disposiciones.

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 con dos factores 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 utilizando dos Factores de Autenticación diferentes.

Las Instituciones podrán optar por utilizar la combinación de al menos dos de los siguientes Factores de Autenticación, de acuerdo al servicio proporcionado y en función a los riesgos asociados:

a) Contraseña o Clave de Acceso.

Para la lectura de estos medios, se deberán utilizar dispositivos que cuenten con una pantalla y un teclado para que el Operador pueda ingresar su respectivo Identificador Individual y su Contraseña o Clave de Acceso, así como con mecanismos que eviten su lectura por parte de terceros.

b) Factor Biométrico.

En caso de utilizar lectores biométricos para la autenticación de los Operadores, deberán tener mecanismos que aseguren que es el Operador autorizado el que realiza la operación.

c) Información dinámica obtenida a través de un generador de Contraseñas o Claves de Acceso de un solo uso (“Token”).

En caso de utilizar este Factor de Autenticación, las Instituciones deberán cumplir con lo dispuesto en el Capítulo X del Título Quinto de las presentes disposiciones.

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

e) Teléfono celular.

En caso de utilizar teléfonos celulares para la Autenticación de los operadores, 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, y ajustarse a lo dispuesto en el Capítulo X del Título Quinto de las presentes disposiciones.

f) Mecanismos de control de acceso fisico a los dispositivos y Medios Electrónicos utilizados para realizar operaciones que aseguren que solamente personal autorizado hará uso de los mismos.

La administración y control de la asignación de los Factores de Autenticación deberá ser responsabilidad única de la Institución, a través de los mecanismos que ésta estime conveniente.

7. Bloqueo automático de los Factores de Autenticación.

Se deberán establecer esquemas de bloqueo automático de los Factores de Autenticación 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.

Únicamente la Institución, previa autenticación del cliente bancario o del Operador, en su caso, podrá desbloquear dichos Factores de Autenticación.

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 III 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 del presente anexo.

IV. 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, ya 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, en adición a lo dispuesto por las disposiciones aplicables en materia de comprobantes de operación de las Instituciones, 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, debiendo únicamente mostrar como máximo los últimos 5 dígitos de la misma.

   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 del mismo.

   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, así como la identificación de los medios de disposición que se hubieren utilizado.

   d) La identificación del empleado del comisionista que realizó la operación.

e) El número telefónico y el 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. Asimismo, deberán indicarse los números correspondientes al "Centro de Atención Telefónica" de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

f) Cuando se alcancen los límites a que se refieren los Artículos 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, dichos comprobantes deberán incluir las leyendas siguientes:

   i) En el caso del límite a que se refieren la fracción I del Artículo 323 de las presentes disposiciones:

      "Transacción no realizada por haber excedido su límite permitido. Acuda a una sucursal bancaria."

   ii) En el caso del límite a que se refieren la fracción II del Artículo 323 de las presentes disposiciones, según corresponda:

      "Transacción no realizada."

Por ningún motivo deberá mostrarse en el comprobante de operación el domicilio del cliente.

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 de clientes bancarios en Medios Electrónicos de los comisionistas.

   Los comisionistas no podrán almacenar, conservar o copiar en sus Medios Electrónicos o en cualquier otro medio, información relacionada con la clientela de la Institución. Asimismo, los comisionistas no podrán emitir un duplicado de los comprobantes de consultas de saldos o mantener copias de los mismos. En los casos que por razones operativas y técnicas se requiera almacenar parcial o totalmente dicha información en sus Medios Electrónicos, ésta deberá mantener mecanismos de encripción. Las llaves criptográficas correspondientes deberán ser administradas por la propia Institución.

   En el caso de que la información relacionada con la clientela de la Institución corresponda a operaciones derivadas del uso de tarjetas prepagadas bancarias o de Cuentas Móviles, podrá ser almacenada sin mecanismos de encripción, siempre y cuando la información no contenga nombres y domicilios.

   Corresponderá a las Instituciones verificar el cumplimiento del presente numeral.

5. Administración y control de aclaraciones y reportes por robo o extravío de los Factores de Autenticación.

Todas las aclaraciones y quejas a las que se refieren el segundo párrafo de la fracción III del Artículo 322 de las presentes disposiciones, según corresponda, así como los reportes por robo o extravío de los Factores de Autenticación mencionados en la fracción VI del mismo artículo, deberán consolidarse en una base de datos administrada y controlada en todo momento por la Institución de que se trate.