

SECRETARIA DE HACIENDA Y CREDITO PUBLICO

RESOLUCION por la que se modifican las disposiciones de carácter general aplicables a las instituciones de crédito.

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

La Comisión Nacional Bancaria y de Valores con fundamento en lo dispuesto por el Artículo 52 de la Ley de Instituciones de Crédito, así como por los Artículos 4, fracciones I, XXXVI y XXXVIII y 19 de la Ley de la Comisión Nacional Bancaria y de Valores, y

CONSIDERANDO

Que en atención al constante desarrollo de nuevas tecnologías y al avance de las existentes, las cuales generan nuevos riesgos y desafíos, resulta conveniente actualizar los requisitos que deberán observar las instituciones de crédito que convengan con el público la celebración de operaciones y la prestación de servicios mediante la utilización de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, a fin de fortalecer la seguridad y confidencialidad de la información transmitida, almacenada o procesada a través de los citados medios, contando con mecanismos que controlen la integridad de dicha información y la continuidad de los servicios;

Que es conveniente actualizar los mecanismos para la identificación de los clientes de las instituciones de crédito, que sean usuarios de medios electrónicos a través de los cuales se realicen operaciones financieras, así como determinar las responsabilidades correspondientes a la utilización de los medios mencionados, a fin de prevenir la realización de operaciones irregulares o ilegales que puedan resultar en una afectación a la situación financiera de las instituciones de crédito o de sus clientes, y

Que de acuerdo con las mejores prácticas internacionales, resulta necesario definir controles específicos que deberán observar las instituciones de crédito de acuerdo con el grado de riesgo en la realización de operaciones a través del uso de medios electrónicos, tales como operaciones en cajeros automáticos, pagos mediante terminales punto de venta, pagos y operaciones mediante teléfonos móviles, operaciones mediante banca por Internet, operaciones a través del servicio host to host, operaciones mediante banca telefónica audio respuesta y voz a voz u otros medios electrónicos, a fin de proteger tanto a los usuarios como a las propias instituciones de crédito, ha resuelto expedir la siguiente:

RESOLUCION POR LA QUE SE MODIFICAN LAS DISPOSICIONES DE CARACTER GENERAL APLICABLES A LAS INSTITUCIONES DE CREDITO

UNICA: Se **ADICIONAN** las fracciones VIII, IX, X, XI, XII, XIII, XV, XXIX, XXX, XXXIII, LXII, LXXII, LXXXVI, C, CI y CII al Artículo 1, recorriéndose la numeración de las fracciones de dicho artículo, cada una en su orden y según corresponda; los Artículos 316 Bis a 316 Bis 22; las Secciones Cuarta y Quinta al Capítulo X del Título Quinto, que comprenderán del Artículo 316 Bis 10 al 316 Bis 12 y del 316 Bis 13 al 316 Bis 22, respectivamente; así como los Anexos 63 y 64; y se **REFORMAN** la actual fracción VII del Artículo 1, la anterior X y actual XVII, la anterior XV y actual XXII, la anterior XX y actual XXVII, la anterior XXVI y actual XXXVI, la anterior XXXIV y actual XLIV, la anterior LI y actual LXI, la anterior LVI y actual LXVII, la anterior LVIII y actual LXIX, la anterior LXXVII y actual XC, todas del Artículo 1; así como el Capítulo X del Título Quinto 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, modificadas mediante resoluciones publicadas en el citado Diario el 3 y 28 de marzo, 15 de septiembre, 6 y 8 de diciembre de 2006, 12 de enero, 23 de marzo, 26 de abril y 5 de noviembre de 2007, 10 de marzo, 22 de agosto, 19 de septiembre, 14 de octubre y 4 de diciembre de 2008, 27 de abril, 28 de mayo, 11 de junio, 12 de agosto, 16 de octubre, 9 de noviembre y 1 de diciembre de 2009, así como por la resolución expedida por esta Comisión el día 17 de diciembre de 2009, para quedar como sigue:

“INDICE**TITULOS PRIMERO a CUARTO . . .****TITULO QUINTO . . .****Capítulos I a IX . . .****Capítulo X****Del uso del servicio de Banca Electrónica****Sección Primera****De la contratación para el uso del servicio de Banca Electrónica****Sección Segunda****De la Identificación del Usuario y la Autenticación en el uso del servicio de Banca Electrónica****Sección Tercera****De la operación del servicio de Banca Electrónica****Sección Cuarta****De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos****Sección Quinta****Del monitoreo, control y continuidad de las operaciones y servicios de Banca Electrónica****Capítulos XI a XIII . . .****Transitorios****Listado de Anexos****Anexos 1 a 62 . . .****Anexo 63** Guía para el uso del servicio de Banca Electrónica.**Anexo 64** Reporte de eventos de pérdida de información administrada a través de Medios Electrónicos.”**“Artículo 1.- . . .****I. a VI. . . .**

- VII. Autenticación: al conjunto de técnicas y procedimientos utilizados para verificar la identidad de:
- a) Un Usuario y su facultad para realizar operaciones a través del servicio de Banca Electrónica.
 - b) Una Institución y su facultad para recibir instrucciones a través del servicio de Banca Electrónica.
- VIII. Banca Electrónica: al conjunto de servicios y operaciones bancarias que las Instituciones realizan con sus Usuarios a través de Medios Electrónicos.
- IX. Banca Host to Host: al servicio de Banca Electrónica mediante el cual se establece una conexión directa entre los equipos de cómputo del Usuario previamente autorizados por la Institución y los equipos de cómputo de la propia Institución, a través de los cuales estos últimos procesan la información para la realización de servicios y operaciones bancarias. Este tipo de servicios incluirán a los proporcionados a través de las aplicaciones conocidas como “Cliente-Servidor”.
- X. Banca Móvil: al servicio de Banca Electrónica en el cual el Dispositivo de Acceso consiste en un Teléfono Móvil del Usuario, cuyo número de línea se encuentre asociado al servicio.
- XI. Banca por Internet: al servicio de Banca Electrónica efectuado a través de la red electrónica mundial denominada Internet, en el sitio que corresponda a uno o más dominios de la Institución, incluyendo el acceso mediante el protocolo WAP o alguno equivalente.
- XII. Banca Telefónica Audio Respuesta: al servicio de Banca Electrónica mediante el cual la Institución recibe instrucciones del Usuario a través de un sistema telefónico, e interactúa con el propio Usuario mediante grabaciones de voz y tonos o mecanismos de reconocimiento de voz, incluyendo los sistemas de respuesta interactiva de voz (IVR).

- XIII. Banca Telefónica Voz a Voz: al servicio de Banca Electrónica mediante el cual un Usuario instruye vía telefónica a través de un representante de la Institución debidamente autorizado por esta, con funciones específicas, el cual podrá operar en un centro de atención telefónica, a realizar operaciones a nombre del propio Usuario.
- XIV. . . .
- XV. Bloqueo de Factores de Autenticación: al proceso mediante el cual la Institución inhabilita el uso de un Factor de Autenticación de forma temporal.
- XVI. . . .
- XVII. Cajero Automático: al Dispositivo de Acceso de autoservicio que permite realizar consultas y operaciones diversas, tales como la disposición de dinero en efectivo y al cual el Usuario accede mediante una tarjeta o cuenta bancaria para utilizar el servicio de Banca Electrónica.
- XVIII. a XXI. . . .
- XXII. Cifrado: al mecanismo que deberán utilizar las Instituciones para proteger la confidencialidad de información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.
- XXIII. a XXVI. . . .
- XXVII. Contraseña: a la cadena de caracteres que autentica a un Usuario en un medio electrónico o en un servicio de Banca Electrónica.
- XXVIII. . . .
- XXIX. Cuentas Destino: a las cuentas receptoras de recursos dinerarios en Operaciones Monetarias.
- XXX. Desbloqueo de Factores de Autenticación: al proceso mediante el cual la Institución habilita el uso de un Factor de Autenticación que se encontraba bloqueado.
- XXXI. y XXXII. . . .
- XXXIII. Dispositivo de Acceso: al equipo que permite a un Usuario acceder al servicio de Banca Electrónica.
- XXXIV. y XXXV. . . .
- XXXVI. Factor de Autenticación: al mecanismo de Autenticación, tangible o intangible, basado en las características físicas del Usuario, en dispositivos o información que solo el Usuario posea o conozca. Estos mecanismos podrán incluir:
- a) Información que el Usuario conozca y que la Institución valide a través de cuestionarios practicados por operadores de centros de atención telefónica.
 - b) Información que solamente el Usuario conozca, tales como Contraseñas y Números de Identificación Personal (NIP).
 - c) Información contenida o generada en medios o dispositivos respecto de los cuales el Usuario tenga posesión, tales como dispositivos o mecanismos generadores de Contraseñas dinámicas de un solo uso y Tarjetas Bancarias con Circuito Integrado, que tengan propiedades que impidan la duplicación de dichos medios, dispositivos o de la información que estos contengan o generen.
 - d) Información del Usuario derivada de sus características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, siempre que dicha información no pueda ser duplicada y utilizada posteriormente.
- XXXVII. a XLIII. . . .
- XLIV. Identificador de Usuario: a la cadena de caracteres, información de un dispositivo o cualquier otra información que conozca tanto la Institución como el Usuario, que permita reconocer la identidad del propio Usuario para el uso del servicio de Banca Electrónica.

XLV. a LX. . . .

LXI. Medios Electrónicos: a los equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados, a que se refiere el Artículo 52 de la Ley.

LXII. Mensajes de texto SMS: al mensaje de texto disponible para su envío en servicios de telefonía móvil.

LXIII. a LXVI. . . .

LXVII. Número de Identificación Personal (NIP): a la Contraseña que autentica a un Usuario en el servicio de Banca Electrónica mediante una cadena de caracteres numéricos.

LXVIII. . . .

LXIX. Operación Monetaria: a la transacción que implique transferencia o retiro de recursos dinerarios. Las operaciones monetarias podrán ser:

- a) Micro Pagos: operaciones de hasta el equivalente en moneda nacional a 70 UDIs.
- b) De Baja Cuantía: operaciones de hasta el equivalente en moneda nacional a 250 UDIs diarias.
- c) De Mediana Cuantía: operaciones de hasta el equivalente en moneda nacional a 1,500 UDIs diarias.
- d) Por montos superiores al equivalente en moneda nacional a 1,500 UDIs diarias.

LXX. y LXXI. . . .

LXXII. Pago Móvil: al servicio de Banca Electrónica en el cual el Dispositivo de Acceso consiste en un Teléfono Móvil del Usuario, cuyo número de línea se encuentre asociado al servicio. Únicamente se podrán realizar consultas de saldo respecto de las cuentas asociadas al servicio, Operaciones Monetarias limitadas a pagos o transferencias de recursos dinerarios de hasta el equivalente en moneda nacional a las Operaciones Monetarias de Mediana Cuantía, con cargo a las tarjetas o cuentas bancarias que tenga asociadas, así como actos para la administración de este servicio, que no requieran un Segundo Factor de Autenticación.

LXXIII. a LXXXV. . . .

LXXXVI. Restablecimiento de Contraseñas y Números de Identificación Personal (NIP): al procedimiento mediante el cual el Usuario puede definir una nueva Contraseña o Número de Identificación Personal.

LXXXVII. a LXXXIX. . . .

XC. Sesión: al periodo en el cual los Usuarios podrán llevar a cabo consultas, Operaciones Monetarias o cualquier otro tipo de transacción bancaria, una vez que hayan ingresado al servicio de Banca Electrónica con su Identificador de Usuario.

XCI. a XCIX. . . .

C. Tarjeta Bancaria con Circuito Integrado: a las tarjetas de débito, crédito o prepagadas bancarias que cuenten con un circuito integrado o chip, que pueda almacenar información y procesarla con el fin de verificar, mediante procedimientos criptográficos, que la tarjeta y la terminal donde se utiliza son válidas.

CI. Teléfono Móvil: a los Dispositivos de Acceso a servicios de telefonía, que tienen asignado un número único de identificación y utilizan comunicación celular o de radiofrecuencia pública.

CII. Terminal Punto de Venta: a los Dispositivos de Acceso al servicio de Banca Electrónica, tales como terminales de cómputo, teléfonos móviles y programas de cómputo, operados por comercios o Usuarios para instruir el pago de bienes o servicios con cargo a una tarjeta o cuenta bancaria.

CIII. a CVII. . . . ”

**“Capítulo X
Del uso del servicio de Banca Electrónica**

**Sección Primera
De la contratación para el uso del servicio de Banca Electrónica**

Artículo 306.- Las Instituciones podrán pactar la celebración de sus operaciones y la prestación de servicios con el público, a través de servicios de Banca Electrónica, debiendo sujetarse a lo establecido por las presentes disposiciones y siempre que:

- I. En la contratación respectiva se establezca de manera clara y precisa, lo siguiente:
 - a) Las operaciones y servicios que podrán proporcionarse a través de Medios Electrónicos.
 - b) Los mecanismos y procedimientos de Identificación del Usuario y Autenticación, así como las responsabilidades del Usuario y de la Institución respecto del uso del servicio de Banca Electrónica.
 - c) Los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados por las Instituciones, a través del servicio de Banca Electrónica.
 - d) Los límites de los montos individuales y agregados diarios, adicionales a los establecidos por las presentes disposiciones, específicos para el servicio de Banca Electrónica de que se trate, definidos por la Institución, en su caso.
 - e) Los mecanismos y procedimientos de cancelación de la contratación del servicio de Banca Electrónica, los cuales deberán ser similares a los de la propia contratación, considerando el tiempo de respuesta de la solicitud, canales de atención al Usuario y procedimientos de Identificación del Usuario y su Autenticación.
 - f) Las restricciones operativas aplicables de acuerdo al Medio Electrónico de que se trate, de conformidad con lo previsto en este Capítulo.
- II. Informen a sus clientes en forma previa a la contratación, los términos y condiciones para el uso del servicio de Banca Electrónica, debiendo mantener dicha información disponible para su consulta en cualquier momento.
- III. Comuniquen a sus Usuarios los riesgos inherentes a la utilización del servicio de Banca Electrónica, así como que hagan de su conocimiento sugerencias para prevenir la realización de operaciones irregulares o ilegales que vayan en detrimento del patrimonio de los clientes y de la Instituciones, pudiendo efectuarse, entre otros, mediante campañas periódicas de difusión de recomendaciones de seguridad para la realización de operaciones a través de dicha Banca Electrónica.

Artículo 307.- Las Instituciones, para la contratación de los servicios de Banca Electrónica con sus clientes, adicionalmente a lo previsto en el Artículo 306 anterior, se sujetarán a lo siguiente:

- I. Deberán obtener el consentimiento expreso mediante firma autógrafa de sus clientes, previa identificación de estos, salvo tratándose de los siguientes servicios:
 - a) Pago Móvil.
 - a) Que un número de línea de Teléfono Móvil pueda ser asociado a cuentas de diferentes Usuarios.

Las Instituciones podrán permitir asociar hasta dos tarjetas o cuentas bancarias del mismo Usuario a un número de línea de Teléfono Móvil, siempre y cuando una de ellas solamente funcione bajo la modalidad de Operaciones Monetarias de Micro Pagos.

- II. Deberán solicitar a sus Usuarios al momento de la contratación, datos de algún medio de comunicación, tales como su dirección de correo electrónico o número de teléfono móvil para la recepción de Mensajes de Texto SMS, a fin de que las Instituciones les hagan llegar las notificaciones a que se refiere el Artículo 316 Bis 1 de estas disposiciones.
- III. Podrán permitir la contratación del servicio de Banca por Internet, mediante firmas electrónicas avanzadas o fiables de sus clientes, a fin de que estos realicen operaciones entre la cuenta registrada a su nombre en la Institución y otra cuenta en otra Institución cuyo titular sea el propio cliente. Será responsabilidad de la Institución que permita la contratación del servicio de Banca por Internet en términos de lo previsto en esta fracción, verificar que la cuenta en otra Institución para realizar las operaciones previstas en la presente fracción se encuentre registrada a nombre del propio cliente.

En todo caso, la Institución deberá obtener previamente la autorización de la Comisión para ofrecer el servicio de Banca por Internet a que se refiere esta fracción, en cuya solicitud deberá exponer los controles que permitirán a los Usuarios realizar las operaciones de forma segura, sujetándose a lo siguiente:

- a) Al momento de la contratación del servicio de Banca por Internet, las Instituciones deberán requerir a sus Usuarios el registro de una única Cuenta Destino cuyo titular sea el propio Usuario, sin que se requiera un segundo Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de estas disposiciones, en términos de lo previsto en el Artículo 314 de las presentes disposiciones.
- b) Para realizar transferencias de recursos dinerarios o instrucciones de cargo entre la cuenta registrada en la Institución y la Cuenta Destino a que se refiere el párrafo anterior, las Instituciones deberán requerir a sus Usuarios un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, sin que le sea aplicable el primer párrafo del Artículo 313 de las presentes disposiciones, debiendo contemplar, en todo caso, controles que aseguren que es el Usuario quien está instruyendo a la Institución, y
- c) En caso de que un Usuario solicite cambiar la Cuenta Destino a que se refiere el inciso a) de esta fracción, deberá realizarlo mediante el procedimiento mencionado en la fracción I del presente artículo.

Sección Segunda

De la identificación del Usuario y

la Autenticación en el uso del servicio de Banca Electrónica

Artículo 308.- Las Instituciones, para permitir el inicio de una Sesión, deberán solicitar y validar al menos:

- I. El Identificador de Usuario, y
- II. Un Factor de Autenticación de las Categorías 2 ó 4 a que se refiere el Artículo 310 de las presentes disposiciones.

El Identificador de Usuario deberá ser único para cada Usuario y permitirá a la Institución identificar todas las operaciones realizadas por el propio Usuario a través del servicio de Banca Electrónica de que se trate.

La longitud del Identificador de Usuario deberá ser de al menos seis caracteres.

Tratándose de Pago Móvil y de Banca Móvil, el Identificador de Usuario deberá ser el número de la línea del Teléfono Móvil asociado al uso de dichos servicios de Banca Electrónica, debiendo la Institución, en todo caso, obtenerlo de manera automática e inequívoca del Teléfono Móvil correspondiente. Asimismo, tratándose de operaciones realizadas a través de Terminales Punto de Venta y Cajeros Automáticos, el Identificador de Usuario podrá ser el número de la tarjeta bancaria con la cual se accede al servicio de Banca Electrónica.

Artículo 309.- Las Instituciones, en el uso del Identificador de Usuario y los Factores de Autenticación, deberán ajustarse a lo siguiente:

- I. Proveer lo necesario para impedir la lectura en la pantalla del Dispositivo de Acceso, de la información de identificación y Autenticación proporcionada por el Usuario, salvo que se trate de Banca Telefónica de Audio Respuesta.

En caso de que la tecnología utilizada en Pago Móvil no permita implementar lo señalado en el párrafo anterior, las Instituciones podrán ofrecer tal servicio obteniendo la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.

Asimismo, las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán prever al momento de la contratación con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de Pago Móvil, que no cumplan con lo previsto en el primer párrafo de la presente fracción y que no sean reconocidas por los Usuarios. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

Asegurar que en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Usuario quien los reciba, active, conozca, desbloquee y restablezca. El Usuario podrá autorizar a un tercero para recibir dichos Factores de Autenticación, siempre que las Instituciones mantengan procedimientos para que dichas autorizaciones sean de carácter eventual y puedan ser revocados por el cliente cuando así lo solicite.

- II. Contar con procedimientos para invalidar los Factores de Autenticación para impedir su uso en un servicio de Banca Electrónica, cuando un Usuario o la misma Institución cancele el uso de dicho servicio o cuando dicho Usuario deje de ser cliente de la Institución.

Artículo 310.- Las Instituciones deberán utilizar Factores de Autenticación para verificar la identidad de sus Usuarios y la facultad de estos para realizar operaciones a través del servicio de Banca Electrónica. Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en las presentes disposiciones, deberán ser de cualquiera de las categorías siguientes:

- I. Factor de Autenticación Categoría 1: Se compone de información obtenida mediante la aplicación de cuestionarios al Usuario, por parte de operadores telefónicos, en los cuales se requieran datos que el Usuario conozca. En ningún caso los Factores de Autenticación de esta categoría podrán componerse únicamente de datos que hayan sido incluidos en comunicaciones impresas o electrónicas enviadas por las Instituciones a sus clientes.

Las Instituciones, en la utilización de los Factores de Autenticación de esta categoría, para verificar la identidad de sus Usuarios, deberán observar lo siguiente:

- a) Definir previamente los cuestionarios que serán practicados por los operadores telefónicos, impidiendo que sean utilizados de forma discrecional, y
 - b) Validar al menos una de las respuestas proporcionadas por sus Usuarios, a través de herramientas informáticas, sin que el operador pueda consultar o conocer anticipadamente los datos de Autenticación de los Usuarios.
- II. Factor de Autenticación Categoría 2: Se compone de información que solo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como Contraseñas y Números de Identificación Personal (NIP), y deberán cumplir con las características siguientes:

- a) En ningún caso se podrá utilizar como tales, la información siguiente:

- i El Identificador de Usuario.
- ii El nombre de la Institución.
- iii Más de dos caracteres idénticos en forma consecutiva.
- iv Más de dos caracteres consecutivos numéricos o alfabéticos.

No resultará aplicable lo previsto en el presente inciso para el caso de Pago Móvil, Banca Móvil y las operaciones realizadas a través de Cajeros Automáticos y Terminales punto de Venta, siempre que las Instituciones informen al Usuario al momento de la contratación, de la importancia de la composición de las Contraseñas para estos servicios.

- b) Su longitud deberá ser de al menos seis caracteres, salvo por lo siguiente:
 - i Cuatro caracteres para los servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta.
 - ii Cinco caracteres para Pago Móvil, y
 - iii Ocho caracteres para Banca por Internet.
- c) La composición de estos Factores de Autenticación deberá incluir caracteres alfabéticos y numéricos, cuando el Dispositivo de Acceso lo permita.

Las Instituciones deberán permitir al Usuario cambiar sus Contraseñas, Números de Identificación Personal (NIP) y otra información de Autenticación estática, cuando este último así lo requiera, utilizando los servicios de Banca Electrónica.

Tratándose de Contraseñas o Números de Identificación Personal (NIP) definidos o generados por las Instituciones durante la contratación de un servicio de Banca Electrónica o durante el restablecimiento de dichas contraseñas, las propias Instituciones deberán prever mecanismos y procedimientos por medio de los cuales el Usuario deba modificarlos inmediatamente después de iniciar la Sesión correspondiente. Las Instituciones deberán contar con controles que les permitan validar que las nuevas Contraseñas o Números de Identificación Personal (NIP) utilizadas por sus Usuarios, sean diferentes a los definidos o generados por las propias Instituciones.

Las Instituciones deberán recomendar a sus Usuarios en el proceso de contratación del servicio de Banca Electrónica, que mantengan Contraseñas seguras.

- III. Factor de Autenticación Categoría 3: Se compone de información contenida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por las Instituciones a sus Usuarios y la información contenida o generada por ellos, deberá cumplir con las características siguientes:

- a) Contar con propiedades que impidan su duplicación o alteración.
- b) Ser información dinámica que no podrá ser utilizada en más de una ocasión.
- c) Tener una vigencia que no podrá exceder de dos minutos.
- d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o por terceros.

Las Instituciones podrán proporcionar a sus Usuarios medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen información de la Cuenta Destino y en el caso de operaciones no monetarias, cualquier otra información relacionada con el tipo de operación o servicio de que se trate, de manera que dicha Contraseña únicamente pueda ser utilizada para la operación solicitada. En estos casos, no será aplicable lo dispuesto en el inciso c) de la presente fracción, así como lo establecido en el cuarto párrafo del Artículo 314 de estas disposiciones en relación al tiempo en que deberán quedar habilitadas las Cuentas Destino.

Asimismo, las Instituciones podrán considerar dentro de esta categoría a la información contenida en el circuito o chip de las Tarjetas Bancarias con Circuito Integrado, siempre y cuando dichas tarjetas se utilicen únicamente para operaciones que se realicen a través de Cajeros Automáticos y Terminales Punto de Venta y tales Dispositivos de Acceso obtengan la información de la tarjeta a través del dicho circuito o chip.

Las Instituciones que aprueben la celebración de operaciones mediante el uso de tarjetas bancarias sin circuito integrado, en Cajeros Automáticos y Terminales Punto de Venta, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

Tratándose de Banca Host to Host, las Instituciones podrán utilizar como Factor de Autenticación de esta Categoría, cualquier mecanismo que les permita verificar que los equipos de cómputo o dispositivos utilizados por los Usuarios para establecer la comunicación, son los que la propia Institución autorizó.

Las Instituciones podrán utilizar tablas aleatorias de Contraseñas como Factor de Autenticación de esta Categoría, siempre y cuando dichas tablas cumplan con las características listadas en los incisos a), b) y d) de la presente fracción. Para el caso del inciso a), las Instituciones deberán asegurarse que las propiedades que impidan la duplicación o alteración se cumplan hasta el momento de la entrega al Usuario. En todo caso, las Instituciones deberán obtener la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.

Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por aquellos realizadas a través del servicio de Banca Electrónica de que se trate. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

- IV. Factor de Autenticación Categoría 4: Se compone de información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano o patrones en iris o retina, entre otras.

Las Instituciones que utilicen los Factores de Autenticación de esta categoría, deberán aplicar a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario.

Las Instituciones podrán considerar dentro de esta categoría la firma autógrafa de sus Usuarios en los comprobantes generados por las Terminales Punto de Venta, únicamente cuando los propios Usuarios realicen Operaciones Monetarias referidas al pago de bienes o servicios a través de dichas Terminales Punto de Venta.

Artículo 311.- Las Instituciones deberán establecer mecanismos y procedimientos para que sus Usuarios del servicio de Banca por Internet, puedan autenticar a las propias Instituciones al inicio de una Sesión, debiendo sujetarse a lo siguiente:

- I. Proporcionar a sus Usuarios información personalizada y suficiente para que estos puedan verificar, antes de ingresar todos los elementos de identificación y Autenticación, que se trata efectivamente de la Institución con la cual se iniciará la Sesión. Para ello, las Instituciones podrán utilizar la información siguiente:
 - a) Aquella que el Usuario conozca o haya proporcionado a la Institución, o bien, que haya señalado para este fin, tales como nombre sin apellidos, alias, imágenes, entre otros.
 - b) Aquella que el Usuario pueda verificar mediante un dispositivo o medio proporcionado por la Institución para este fin.
- II. Una vez que el Usuario verifique que se trata de la Institución e inicie la Sesión, las Instituciones deberán proporcionar de forma notoria y visible al Usuario a través del Medio Electrónico de que se trate, al menos la siguiente información:
 - a) Fecha y hora del ingreso a su última Sesión, y
 - b) Nombre y apellido del Usuario.

Artículo 312.- Las Instituciones podrán solicitar a sus clientes o Usuarios solo un Factor de Autenticación Categoría 1, de acuerdo con lo establecido en el Artículo 310 de las presentes disposiciones, en los casos siguientes:

- I. Para la Autenticación de sus Usuarios que pretendan utilizar Banca Telefónica Voz a Voz para realizar transacciones;
- II. Para la contratación de Pago Móvil, y
- III. Para el Desbloqueo de Factores de Autenticación, así como la reactivación o desactivación temporal del uso del servicio de Banca Electrónica, mediante centros de atención telefónica.

Sin perjuicio de lo anterior, las Instituciones podrán prever que el procedimiento de Autenticación a través de centros de atención telefónica, se realice mediante enlaces a dispositivos de audio respuesta automática.

Artículo 313.- Las Instituciones deberán solicitar a sus Usuarios, para la celebración de operaciones o prestación de servicios a través de Medios Electrónicos, un segundo Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de estas disposiciones, adicional al utilizado, en su caso, para iniciar la Sesión y en cada ocasión en que se pretenda realizar cada una de las operaciones y servicios siguientes:

- I. Transferencias de recursos dinerarios a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y de bienes o servicios, así como las autorizaciones e instrucciones de domiciliación de pago de bienes o servicios;

En estos casos, cuando las Cuentas Destino hayan sido registradas en Oficinas Bancarias utilizando la firma autógrafa del Usuario, previa identificación de este, las Instituciones podrán permitir a los Usuarios realizar dichas operaciones utilizando un solo Factor de Autenticación de las Categorías 2, 3 ó 4 a que se refiere el artículo 310 de estas disposiciones. Asimismo, las Instituciones deberán proveer lo necesario para que los Usuarios puedan desactivar o dar de baja las Cuentas Destino registradas en el servicio de Banca Electrónica de que se trate.
- II. Pago de impuestos;
- III. Establecimiento e incremento de límites de monto para Operaciones Monetarias a que se refiere el Artículo 315 de las presentes disposiciones, para el servicio de que se trate u otros servicios de Banca Electrónica;
- IV. Registro de Cuentas Destino de terceros u otras Instituciones para el servicio de que se trate u otros servicios de Banca Electrónica;
- V. Alta y modificación del medio de notificación a que se refiere el Artículo 316 Bis 1 de estas disposiciones, salvo lo previsto en el último párrafo de dicho artículo;

- VI. Consultas de estados de cuenta u otras consultas que permitan conocer información relacionada con el Usuario y sus cuentas, tales como el domicilio, límites de crédito, beneficiarios o cotitulares, u otra que pueda ser utilizada como información de Autenticación;

Las Instituciones podrán permitir a los Usuarios la impresión de estados de cuenta utilizando una tarjeta bancaria y un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, en equipos electrónicos o de telecomunicaciones ubicados únicamente dentro de las Oficinas Bancarias que la Comisión determine, mediante disposiciones de carácter general, que cuentan con las medidas máximas de seguridad conforme a lo establecido por el artículo 96 de la Ley.

Igualmente, las Instituciones podrán permitir a sus Usuarios consultar los estados de cuenta, requiriendo únicamente un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, siempre y cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación a que se hace referencia en el Artículo 316 Bis 1 de las presentes disposiciones. En estos casos, las Instituciones deberán solicitar un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, para dar cumplimiento a lo previsto por la fracción V del presente artículo.

- VII. Contratación de otro servicio de Banca Electrónica o de operaciones y servicios adicionales a los originalmente convenidos, conforme a lo dispuesto en el Artículo 307 de estas disposiciones;

- VIII. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP) respecto de otros servicios de Banca Electrónica que el Usuario tenga contratados, y

- IX. Retiro de efectivo en Cajeros Automáticos.

Las Instituciones no se encontrarán obligadas a solicitar a sus Usuarios un Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de las presentes disposiciones, cuando se trate de las Operaciones Monetarias que se realicen a través de Pago Móvil. Dichas operaciones podrán realizarse utilizando al menos un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, debiendo las Instituciones asegurar que las Operaciones Monetarias se realizan a través del número de línea que se encuentra asociado al servicio.

Tratándose de Operaciones Monetarias consideradas como Micro Pagos, cuyo Dispositivo de Acceso sea un Teléfono Móvil o una Terminal Punto de Venta, podrán ser realizadas sin que las Instituciones soliciten Factores de Autenticación. Las Instituciones deberán prever, al momento de la contratación con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en dichos casos. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

Asimismo, las Instituciones podrán enviar a solicitud de sus Usuarios, estados de cuenta a través de correo electrónico, siempre y cuando la información se transmita de forma Cifrada o con mecanismos que eviten su lectura por parte de terceros no autorizados, y requieran un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, para que el Usuario tenga acceso, el cual deberá ser distinto al utilizado para acceder al servicio de Banca por Internet. Las Instituciones deberán establecer medidas que protejan la confidencialidad de los datos transmitidos y del Factor de Autenticación utilizado.

Tratándose de los servicios de Banca por Internet proporcionados a Usuarios que sean personas morales, las Instituciones podrán implementar mecanismos mediante los cuales una persona autorizada por el Usuario, realice la solicitud para efectuar las operaciones, y otra persona distinta que sea designada por el propio Usuario, autorice su ejecución. En estos casos, se podrá exceptuar a las Instituciones de la obligación de que el servicio de Banca por Internet cumpla con el tiempo de habilitación de la cuenta así como respecto del uso de un segundo Factor de Autenticación por cada operación, siempre y cuando las Instituciones implementen controles que permitan diferenciar las funciones aplicables a la persona que solicita una operación, respecto de aquellas que aplican a la persona que autoriza su ejecución. En el supuesto establecido en el presente párrafo, las Instituciones deberán obtener la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.

Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por los Usuarios en dichos casos. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

Sección Tercera

De la operación del servicio de Banca Electrónica

Artículo 314.- Para la celebración de las Operaciones Monetarias previstas en las fracciones I y II del Artículo 313 de las presentes disposiciones, a través de los servicios de Banca Electrónica, las Instituciones deberán asegurarse de que sus Usuarios registren en el servicio de Banca Electrónica de que se trate, las Cuentas Destino previamente a su uso, ya sea para ser utilizadas dentro del mismo servicio o, si así lo convienen con sus Usuarios, en otros servicios de Banca Electrónica.

Para el caso de pago de servicios e impuestos se considerará como registro de Cuentas Destino, al registro de los convenios, referencias para depósitos, contratos o nombres de beneficiarios, mediante los cuales las Instituciones hacen referencia a un número de cuenta.

En ningún caso se podrán registrar Cuentas Destino a través de Banca Telefónica Voz a Voz.

En el caso de los servicios ofrecidos a Usuarios que sean personas morales o personas físicas con actividad empresarial en términos de la legislación fiscal, las Instituciones podrán permitirles el registro de cuentas por conjuntos de cuentas, considerando el registro de cada conjunto de cuentas como una sola operación.

Las Cuentas Destino deberán quedar habilitadas después de un periodo determinado por la propia Institución, sin que este sea menor a treinta minutos contados a partir de que se efectúe el registro. Las Instituciones deberán informar al Usuario el plazo en que quedarán habilitadas dichas cuentas. Se exceptúa de este periodo a las Cuentas Destino que hayan sido registradas a través de Banca Móvil, sin perjuicio de lo dispuesto en el último párrafo de este artículo, las registradas en Oficinas Bancarias utilizando la firma autógrafa del Usuario, así como aquellas para efectuar pago de impuestos, excluyendo en este último concepto, el pago de tenencias vehiculares a que se refiere la Ley del Impuesto sobre Tenencia o Uso de Vehículos.

Asimismo, las Instituciones podrán habilitar Cuentas Destino registradas por sus Usuarios sin que les sea aplicable el periodo mínimo de tiempo referido en el párrafo anterior, siempre y cuando sea para la realización de Operaciones Monetarias a través de Banca por Internet cuyo monto agregado diario no exceda al equivalente en moneda nacional a las de Baja Cuantía, o bien, el equivalente en moneda nacional a 1,000 UDIs mensuales y obtengan la previa autorización de la Comisión. Las Instituciones deberán exponer en la solicitud respectiva los controles que les permitirán a los Usuarios realizar operaciones de forma segura. En todo caso, las Instituciones deberán determinar el tiempo para que queden habilitadas las Cuentas Destino, una vez que el Usuario haya realizado el registro previo de las mismas.

Las Instituciones, con base en la información disponible deberán validar al momento del registro, la estructura del número de la Cuenta Destino, del contrato o de la clave bancaria estandarizada, ya sea que se trate de cuentas para depósito, pago de servicios, tarjetas bancarias u otros medios de pago.

Para las Operaciones Monetarias que se realicen a través de Banca Host to Host, Terminales Punto de Venta o Cajeros Automáticos, no se requerirá que los Usuarios registren las Cuentas Destino; tampoco para las que se realicen mediante Pago Móvil y Banca Móvil, siempre que, tratándose de estos dos últimos, el monto de dichas operaciones sea hasta el equivalente a las de Baja Cuantía por cada operación.

Artículo 315.- Las Instituciones podrán permitir a sus Usuarios establecer límites de monto para las Operaciones Monetarias que se realicen a través de los servicios de Banca Electrónica, obteniendo su consentimiento mediante firma autógrafa en Oficinas Bancarias, previa identificación de estos.

Asimismo, las Instituciones deberán proveer lo necesario para que sus Usuarios establezcan límites de monto para las Operaciones Monetarias previstas en las fracciones I y II del Artículo 313 de las presentes disposiciones, para los servicios de Banca por Internet, Banca Telefónica Voz a Voz, Banca Telefónica Audio Respuesta y Banca Móvil.

Las Instituciones deberán permitir a sus Usuarios reducir los límites establecidos previamente en dichos servicios de Banca Electrónica, utilizando un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones. Para el caso del servicio de Banca Telefónica Voz a Voz, las Instituciones podrán emplear un Factor de Autenticación Categoría 1 a que se refiere el Artículo 310 de las presentes disposiciones.

Tratándose de Cajeros Automáticos, el monto acumulado diario de las Operaciones Monetarias que representen un cargo a la cuenta del cliente, no podrá exceder del equivalente en moneda nacional a las Operaciones Monetarias de Mediana Cuantía por cuenta.

En ningún caso el monto acumulado de las Operaciones Monetarias realizadas por un Usuario a través de Pago Móvil, aún cuando tenga asociadas hasta dos tarjetas o cuentas bancarias, en su caso, podrá exceder del equivalente en moneda nacional a las Operaciones Monetarias de Mediana Cuantía en un día y no deberán superar el equivalente en moneda nacional a 4,000 UDIs mensuales. Tratándose de Operaciones Monetarias de Micro Pagos, el saldo disponible de la cuenta asociada al Teléfono Móvil no podrá ser mayor al equivalente en moneda nacional a 70 UDIs.

Sin perjuicio de lo dispuesto en el presente artículo, las Instituciones podrán definir límites inferiores específicos para cada servicio de Banca Electrónica, siempre y cuando no contravengan lo previsto por las presentes disposiciones.

Artículo 316.- Las Instituciones deberán solicitar a sus Usuarios que confirmen la celebración de una Operación Monetaria, previo a que se ejecute, haciendo explícita la información suficiente para darle certeza al Usuario de la operación que se realiza.

Se exceptúa de lo anterior a los servicios de Banca Electrónica ofrecidos a través de Terminales Punto de Venta.

Artículo 316 Bis.- Las Instituciones deberán establecer mecanismos y procedimientos para que los servicios de Banca Electrónica generen los comprobantes correspondientes respecto de las operaciones y servicios realizados por sus Usuarios a través de dichos servicios de Banca Electrónica.

Artículo 316 Bis 1.- Las Instituciones estarán obligadas a notificar a sus Usuarios a la brevedad posible y a través del medio de comunicación cuyos datos haya proporcionado el Usuario para tal fin, cualquiera de los siguientes eventos realizados a través de los servicios de Banca Electrónica:

- I. Transferencias de recursos dinerarios a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y de bienes o servicios, así como las autorizaciones e instrucciones de domiciliación de pago de bienes o servicios;
- II. Pago de impuestos;
- III. Modificación de límites de montos de operaciones;
- IV. Registro de Cuentas Destino de terceros u otras Instituciones;
- V. Alta y modificación del medio de notificación al Usuario, debiendo enviarse tanto al medio de notificación anterior como al nuevo;
- VI. Contratación de otro servicio de Banca Electrónica o modificación de las condiciones para el uso del servicio de Banca Electrónica previamente contratado;
- VII. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP), así como para la reactivación del uso de los servicios de Banca Electrónica;
- VIII. Modificación de Contraseñas o Números de Identificación Personal (NIP) por parte del Usuario, y
- IX. Retiro de efectivo en Cajeros Automáticos.

Las Instituciones deberán asegurarse de que la información transmitida para notificar al Usuario sobre los eventos a que se refiere el presente Artículo, no contenga números de cuenta completos, domicilios, ni saldos.

Las notificaciones sobre la realización de las operaciones señaladas en las fracciones I, II y IX del Artículo 313 de estas disposiciones, efectuadas a través de Pago Móvil, Cajeros Automáticos y Terminales Punto de Venta, deberán ser enviadas cuando el acumulado diario de dichas operaciones por servicio de Banca Electrónica de que se trate, sea mayor al equivalente en moneda nacional a 600 UDIs, o bien, cuando las Operaciones Monetarias en lo individual sean mayores al equivalente en moneda nacional a 250 UDIs. En este último caso, siempre y cuando las Instituciones cuenten con esquemas específicos de prevención de fraudes con el fin de revisar continuamente aquellas operaciones que puedan constituir un uso no autorizado de los servicios de Banca Electrónica.

En ningún caso las Instituciones permitirán la modificación del medio de notificación a través de Cajeros Automáticos y Terminales Punto de Venta. Las Instituciones deberán permitir a sus Usuarios modificar el medio de notificación de los servicios de Banca Electrónica ofrecidos en Cajeros Automáticos o Terminales Punto de Venta mediante un centro de atención telefónica, utilizando un Factor de Autenticación Categoría 1 a que se refiere el Artículo 310 de las presentes disposiciones.

Se exceptúa de lo señalado en el presente artículo a las operaciones realizadas mediante el servicio de Banca Host to Host.

Artículo 316 Bis 2.- Las Instituciones deberán proveer lo necesario para que una vez autenticado el Usuario en el servicio de Banca Electrónica de que se trate, la Sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las Instituciones deberán establecer, al menos, los mecanismos siguientes:

- I. Dar por terminada la Sesión en forma automática, e informar al Usuario del motivo en cualquiera de los casos siguientes:
 - a) Cuando exista inactividad por más de veinte minutos.

Tratándose de operaciones realizadas mediante Pago Móvil, Cajeros Automáticos y Terminales Punto de Venta, el periodo de inactividad no podrá exceder de un minuto.

Para operaciones realizadas mediante Banca Host to Host, las Instituciones podrán definir el periodo de inactividad, con base en los riesgos asociados al servicio que las propias Instituciones determinen.
 - b) Cuando en el curso de una Sesión del servicio de Banca por Internet, la Institución identifique cambios relevantes en los parámetros de comunicación del Medio Electrónico, tales como identificación del Dispositivo de Acceso, rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros.
- II. Impedir el acceso en forma simultánea, mediante la utilización de un mismo Identificador de Usuario a más de una Sesión en el servicio de Banca Electrónica de que se trate e informar al Usuario, cuando el Identificador de Usuario esté siendo utilizado en otra Sesión.
- III. En el evento de que las Instituciones ofrezcan servicios de terceros mediante enlaces en el servicio de Banca Electrónica, deberán comunicar a sus Usuarios que al momento de ingresar a dichos servicios, se cerrará automáticamente la Sesión abierta con la Institución de que se trate y se ingresará a otra cuya seguridad no depende ni es responsabilidad de dicha Institución.

Artículo 316 Bis 3.- Las Instituciones deberán establecer procesos y mecanismos automáticos para Bloquear el uso de Contraseñas y otros Factores de Autenticación para el servicio de Banca Electrónica, cuando menos para los casos siguientes:

- I. Cuando se intente ingresar al servicio de Banca Electrónica utilizando información de Autenticación incorrecta. En ningún caso los intentos de acceso fallidos podrán exceder de cinco ocasiones consecutivas, situación en la cual se deberá generar el Bloqueo automático.
- II. Cuando el Usuario se abstenga de realizar operaciones o acceder a su cuenta, a través del servicio de Banca Electrónica de que se trate, por un periodo que determine cada Institución en sus políticas de operación y de acuerdo con el Medio Electrónico correspondiente, así como en función de los riesgos inherentes al mismo. En ningún caso, dicho periodo podrá ser mayor a un año. Lo anterior, no será aplicable a los servicios de Banca Electrónica ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta.

Las Instituciones podrán Desbloquear el uso de Factores de Autenticación que previamente hayan sido Bloqueados en los casos contemplados en las fracciones I y II anteriores, para lo cual podrán utilizar un Factor de Autenticación Categoría 1 a que se refiere el artículo 310 de las presentes disposiciones, en términos de lo previsto por la fracción III del Artículo 312 de estas disposiciones, o bien, realizar a sus Usuarios preguntas secretas, cuyas respuestas deben conservarse almacenadas en forma Cifrada. Para efectos de lo previsto en el presente párrafo, se entenderá por pregunta secreta al cuestionamiento que define el Usuario o la Institución durante el proceso de contratación del servicio de Banca Electrónica, respecto del cual se genera información como respuesta. Cada pregunta secreta que se defina únicamente podrá ser utilizada en una ocasión.

Con independencia de lo anterior, las Instituciones deberán permitir al Usuario el Restablecimiento de Contraseñas y Números de Identificación Personal (NIP) utilizando el procedimiento de contratación al servicio descrito en el Artículo 307 de las presentes disposiciones.

Artículo 316 Bis 4.- Para el manejo de Contraseñas y otros Factores de Autenticación, las Instituciones se sujetarán a lo siguiente:

- I. Deberán mantener procedimientos que proporcionen seguridad en la información contenida en los dispositivos de Autenticación en su custodia, la distribución, así como en la asignación y reposición a sus Usuarios de dichas Contraseñas y Factores de Autenticación.
- II. Tendrán prohibido contar con mecanismos, algoritmos o procedimientos que les permitan conocer, recuperar o descifrar los valores de cualquier información relativa a la Autenticación de sus Usuarios.
- III. Tendrán prohibido solicitar a sus Usuarios, a través de sus funcionarios, empleados, representantes o comisionistas, la información parcial o completa, de los Factores de Autenticación de las Categorías 2 ó 3 a que se refiere el Artículo 310 de las presentes disposiciones.

Se exceptúa de lo previsto en esta fracción, a las operaciones realizadas por Banca Telefónica Voz a Voz, siempre y cuando el Usuario haya iniciado la llamada, se requiera información parcial del Factor de Autenticación de las Categorías 2 ó 3 a que se refiere el Artículo 310 de las presentes disposiciones, y este sea utilizado exclusivamente para este servicio de Banca Electrónica.

Artículo 316 Bis 5.- Las Instituciones deberán establecer procedimientos para que sus Usuarios de Pago Móvil y Banca Móvil puedan, en todo momento, desactivar su uso de forma temporal en caso de requerirlo, así como establecer procedimientos para reactivar el uso cuando el Usuario lo disponga.

La desactivación del uso de manera temporal de los servicios de Banca Electrónica mencionados en el párrafo anterior, deberá realizarse en todo momento dentro de una Sesión en el mismo servicio, o bien, a través de algún otro servicio de Banca Electrónica que el Usuario tenga contratado, debiendo requerir en ambos casos, un Factor de Autenticación de cualquiera de las categorías previstas en el Artículo 310 de las presentes disposiciones.

Para la reactivación del uso de los servicios de Banca Electrónica mencionados en el primer párrafo de este artículo, los Usuarios podrán utilizar los mismos mecanismos señalados en el Artículo 307 de estas disposiciones, o bien, un Factor de Autenticación Categoría 1 a que se refiere el Artículo 310 de las presentes disposiciones. Las Instituciones deberán observar lo señalado en el Artículo 308 de estas disposiciones para poder iniciar una Sesión una vez que se haya reactivado el servicio.

Artículo 316 Bis 6.- Las Instituciones que pongan al alcance de sus Usuarios equipos electrónicos o de telecomunicaciones, en sus instalaciones o en áreas de acceso al público, para el uso del servicio de Banca Electrónica, deberán:

- I. Adoptar medidas que procuren detectar e impedir la instalación en tales equipos, de dispositivos o programas que puedan interferir con el manejo de la información de los Usuarios, o que puedan permitir que dicha información sea leída, copiada, modificada o extraída por terceros. Adicionalmente, deberán informar a sus Usuarios, mediante campañas de difusión, sobre la apariencia y el funcionamiento de los equipos electrónicos o de telecomunicaciones que pongan al alcance de estos, a fin de prevenir actos que deriven o pudieran derivar en operaciones irregulares o ilegales que afecten a los Usuarios o a las propias Instituciones.
- II. Contar con procedimientos tanto preventivos como correctivos, que permitan correlacionar la información proveniente de las reclamaciones de los clientes con lo siguiente:
 - a) El modo de operación del personal interno o externo de la Institución, que opera o administra los equipos electrónicos o de telecomunicaciones;
 - b) Si los equipos han sido sujetos a alteraciones para robo de información de tarjetas, Números de Identificación Personal (NIP) o Contraseñas, y
 - c) El resultado de las labores de identificación, monitoreo y análisis de comportamientos fuera de los parámetros establecidos por la Institución.

Para tal fin, la Institución deberá presentar a los Comités de Auditoría y de Riesgos, cada vez que sesionen, un informe de los resultados de la ejecución de dichos procedimientos.

Artículo 316 Bis 7.- Las Instituciones que ofrezcan al público operaciones y servicios a través de centros de atención telefónica, deberán:

- I. Mantener controles de seguridad física y lógica en la infraestructura tecnológica de los centros de atención telefónica, incluyendo los dispositivos de grabación de llamadas y los medios de almacenamiento y respaldo de estas, que protejan en todo momento la confidencialidad e integridad de la información proporcionada por sus Usuarios.
- II. Delimitar las funciones de los operadores telefónicos a fin de que sean Independientes respecto de otras funciones operativas.
- III. Impedir que los operadores telefónicos cuenten con mecanismos que les permitan registrar la información proporcionada por sus Usuarios en medios diferentes a los dispuestos por la propia Institución para efectos de Autenticación. Para ello, las Instituciones deberán cerciorarse que las personas que tengan acceso a los centros de atención telefónica, no utilicen equipos electrónicos u otros dispositivos, servicios de correo electrónico externo, programas de mensajería instantánea, programas de cómputo, o que a través de estos tengan acceso a páginas de Internet no autorizadas, o cualquier otro mecanismo que les permita copiar, enviar o extraer por cualquier medio o tecnología información relacionada con los Usuarios, o con las operaciones y servicios que se realicen a través de los centros de atención telefónica.

Artículo 316 Bis 8.- Las Instituciones que ofrezcan servicios de Banca Electrónica a través de Cajeros Automáticos y Terminales Punto de Venta, deberán asegurarse que estos cuenten con lectores que permitan obtener la información de las Tarjetas Bancarias con Circuito Integrado, en el entendido de que la información deberá ser leída directamente del propio circuito o chip.

Artículo 316 Bis 9.- Las Instituciones podrán consultar la Guía para el uso del servicio de Banca Electrónica, contenida en el Anexo 63 de las presentes disposiciones, sin que dicho documento tenga carácter vinculante para las mismas.

Sección Cuarta

De la seguridad, confidencialidad e integridad de la información transmitida, almacenada o procesada a través de Medios Electrónicos

Artículo 316 Bis 10.- Las Instituciones que utilicen Medios Electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información a través de dichos Medios Electrónicos, a fin de evitar que sea conocida por terceros. Para tales efectos, las Instituciones deberán cumplir con lo siguiente:

- I. Cifrar los mensajes o utilizar medios de comunicación Cifrada, en la transmisión de la Información Sensible del Usuario procesada a través de Medios Electrónicos, desde el Dispositivo de Acceso hasta la recepción para su ejecución por parte de las Instituciones, a fin de proteger la información a que se refiere el Artículo 117 de la Ley, incluyendo la relativa a la identificación y Autenticación de Usuarios tales como Contraseñas, Números de Identificación Personal (NIP), cualquier otro Factor de Autenticación, así como la información de las respuestas a las preguntas secretas a que se refiere el penúltimo párrafo del Artículo 316 Bis 3 de estas disposiciones.

Para efectos de lo anterior, las Instituciones deberán utilizar tecnologías que manejen Cifrado y que requieran el uso de llaves criptográficas para asegurar que terceros no puedan conocer los datos transmitidos.

Las Instituciones serán responsables de la administración de las llaves criptográficas, así como de cualquier otro componente utilizado para el Cifrado, considerando procedimientos que aseguren su integridad y confidencialidad, protegiendo la información de Autenticación de sus Usuarios.

Tratándose de Pago Móvil, Banca Telefónica Voz a Voz y Banca Telefónica Audio Respuesta, podrán implementar controles compensatorios al Cifrado en la transmisión de información a fin de protegerla.

- II. Las Instituciones deberán Cifrar o truncar la información de las cuentas u operaciones de sus Usuarios y Cifrar las Contraseñas, Números de Identificación Personal (NIP), respuestas secretas, o cualquier otro Factor de Autenticación, en caso de que se almacene en cualquier componente de los Medios Electrónicos.

- III. En ningún caso, las Instituciones podrán transmitir las Contraseñas y Números de Identificación Personal (NIP), a través de correo electrónico, servicios de mensajería instantánea, Mensajes de Texto SMS o cualquier otra tecnología, que no cuente con mecanismos de Cifrado.

Se exceptúa de lo previsto en esta fracción a las Contraseñas y Números de Identificación Personal (NIP) utilizados para acceder al servicio de Pago Móvil, siempre y cuando las Instituciones mantengan controles para que no se pongan en riesgo los recursos y la información de sus Usuarios. Las Instituciones que pretendan utilizar los controles a que se refiere el presente párrafo deberán obtener la previa autorización de la Comisión, para tales efectos.

Asimismo, la información de los Factores de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, utilizados para acceder a la información de los estados de cuenta, podrá ser comunicada al Usuario mediante dispositivos de audio respuesta automática, así como por correo, siempre y cuando esta sea enviada utilizando mecanismos de seguridad, previa solicitud del Usuario y se hayan llevado a cabo los procesos de Autenticación correspondientes.

- IV. Las Instituciones deberán asegurarse de que las llaves criptográficas y el proceso de Cifrado y descifrado se encuentren instalados en dispositivos de alta seguridad, tales como los denominados HSM (Hardware Security Module), los cuales deberán contar con prácticas de administración que eviten el acceso no autorizado y la divulgación de la información que contienen.

Artículo 316 Bis 11.- Las Instituciones deberán contar con controles para el acceso a las bases de datos y archivos correspondientes a las operaciones y servicios efectuados a través de Medios Electrónicos, aún cuando dichas bases de datos y archivos residan en medios de almacenamiento de respaldo. Para efectos de lo anterior, las Instituciones deberán ajustarse a lo siguiente:

- I. El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por la Institución en función de las actividades que realizan. Al otorgarse dichos accesos, deberá dejarse constancia de tal circunstancia y señalar los propósitos y el periodo al que se limitan los accesos.
- II. Tratándose de accesos que se realicen en forma remota, deberán utilizarse mecanismos de Cifrado en las comunicaciones.
- III. Deberán contar con procedimientos seguros de destrucción de los medios de almacenamiento de las bases de datos y archivos que contengan Información Sensible de sus Usuarios, que prevengan su restauración a través de cualquier mecanismo o dispositivo.
- IV. Deberán desarrollar políticas relacionadas con el uso y almacenamiento de información que se transmita y reciba por los Medios Electrónicos, estando obligadas a verificar el cumplimiento de sus políticas por parte de sus proveedores y afiliados.

La obtención de información almacenada en las bases de datos y archivos a que se refiere el presente artículo, sin contar con la autorización correspondiente, o el uso indebido de dicha información, será sancionada en términos de lo previsto en la Ley, inclusive tratándose de terceros contratados al amparo de lo establecido en el Artículo 46 Bis 1 de dicho ordenamiento legal.

Artículo 316 Bis 12.- En caso de que la Información Sensible del Usuario sea extraída, extraviada o las Instituciones supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán:

- I. Enviar por escrito a la Dirección General de la Comisión encargada de su supervisión, dentro de los cinco días naturales siguientes al evento de que se trate, la información que se contiene en el Anexo 64 de las presentes disposiciones.
- II. Llevar a cabo una investigación inmediata para determinar si la información ha sido o puede ser mal utilizada, y en este caso deberán notificar esta situación, en los siguientes 3 días hábiles, a sus Usuarios afectados a fin de prevenirlos de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada o comprometida, debiendo informarle las medidas que deberán tomar. Asimismo, deberán enviar a la Dirección General de la Comisión encargada de su supervisión, el resultado de dicha investigación en un plazo no mayor a cinco días naturales posteriores a su conclusión.

Sección Quinta
Del monitoreo, control y continuidad de las operaciones y
servicios de Banca Electrónica

Artículo 316 Bis 13.- Las Instituciones deberán mantener mecanismos de control para la detección y prevención de eventos que se aparten de los parámetros de uso habitual de sus Usuarios a través de Medios Electrónicos. Para tales efectos, las Instituciones podrán:

- I. Solicitar a sus Usuarios la información que estimen necesaria para definir el uso habitual que estos hagan de los servicios de Banca Electrónica.
- II. Aplicar, bajo su responsabilidad, medidas de prevención, tales como la suspensión de la utilización del servicio de Banca Electrónica o, en su caso, de la operación que se pretenda realizar, en el evento de que cuenten con elementos que hagan presumir que el Identificador de Usuario o los Factores de Autenticación no están siendo utilizados por el propio Usuario, debiendo informar a este tal situación de forma inmediata. Lo anterior, en los términos y condiciones que las Instituciones hayan pactado con sus Usuarios en el contrato respectivo.

Artículo 316 Bis 14.- Las Instituciones deberán mantener en bases de datos las incidencias, fallas o vulnerabilidades detectadas en los servicios de Banca Electrónica, así como todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios y que al menos incluya la información siguiente:

- I. La relacionada con la detección de eventos de fallas, errores operativos, intentos o eventos efectuados de ataques informáticos, robo o pérdida de información y uso indebido de información de los Usuarios, que incluya al menos lo siguiente: fecha del suceso, duración, servicio de Banca Electrónica afectado y clientes afectados.
- II. Aquella relacionada con operaciones no reconocidas por los Usuarios y el trámite que, en su caso, haya promovido el Usuario, tales como folio de reclamación, fecha de reclamación, fecha de la operación, cuenta origen, tipo de producto, servicio de Banca Electrónica en el que se realizó la operación, causa o motivo, importe, estado de la reclamación, resolución, fecha de resolución, monto abonado, monto recuperado y monto quebrantado.

La información anterior deberá mantenerse en la Institución durante un periodo no menor a cinco años contado a partir de su registro, sin perjuicio de otras disposiciones que resulten aplicables.

Artículo 316 Bis 15.- Las Instituciones deberán generar registros, bitácoras, huellas de auditoría de las operaciones y servicios bancarios realizados a través de Medios Electrónicos y, en el caso de Banca Telefónica Voz a Voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de Banca Electrónica, debiendo observar lo siguiente:

- I. Las bitácoras deberán registrar cuando menos la información siguiente:
 - a) Los accesos a los Medios Electrónicos y las operaciones o servicios realizados por sus Usuarios, así como el acceso a dicha información por las personas expresamente autorizadas por la Institución, incluyendo las consultas efectuadas.
 - b) La fecha y hora, número de cuenta origen y Cuenta Destino y demás información que permita identificar el mayor número de elementos involucrados en el acceso y operación en los Medios Electrónicos.
 - c) Los datos de identificación del Dispositivo de Acceso utilizado por el Usuario para realizar la operación de que se trate.
 - d) En el caso de Banca por Internet, deberán registrarse las direcciones de los protocolos de Internet o similares, y para los servicios de Banca Electrónica en los que se utilicen Teléfonos Móviles o fijos, deberá registrarse el número de la línea del teléfono en el caso de que esté disponible.

Las bitácoras, incluyendo las grabaciones de llamadas de Banca Telefónica Voz a Voz, deberán ser almacenadas de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Las bitácoras a que se refiere la presente fracción, deberán ser revisadas por las Instituciones en forma periódica y en caso de detectarse algún evento inusual, deberá reportarse a los Comités de Auditoría y de Riesgos, conforme se establece en el último párrafo del Artículo 316 Bis 19 de las presentes disposiciones.

- II. Deberán contar con mecanismos para que la información de los registros de las bitácoras en los diferentes equipos críticos de cómputo y telecomunicaciones utilizados en las operaciones de Banca Electrónica sea consistente.

La información a que se refiere el presente Artículo deberá ser proporcionada a los Usuarios que así lo requieran expresamente a la Institución mediante sus canales de atención al cliente, en un plazo que no exceda de diez días hábiles, siempre que se trate de operaciones realizadas en las propias cuentas de los Usuarios durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate. En caso de grabaciones de voz no se entregará copia de la grabación, solo se permitirá su audición, debiendo proporcionar una transcripción de la misma si es requerida por el Usuario.

Artículo 316 Bis 16.- Las Instituciones deberán proveer procedimientos y mecanismos para que sus Usuarios les reporten el robo o extravío de los Dispositivos de Acceso o, en su caso, de su información de identificación y Autenticación, que permitan a las propias Instituciones impedir el uso indebido de los mismos. Asimismo, deberán establecer políticas que definan las responsabilidades tanto del Usuario como de la Institución, respecto de las operaciones que hayan sido efectuadas previas al reporte.

Las Instituciones deberán contar con procedimientos y mecanismos para que el reporte de robo o extravío pueda ser enviado por el Usuario tanto a través de Medios Electrónicos como por cualquier medio que defina la propia Institución. Cada reporte de robo o extravío deberá generar un folio que se haga del conocimiento del Usuario y que le permita dar seguimiento a dicho reporte.

Adicionalmente, las Instituciones deberán establecer procedimientos y mecanismos para la atención y seguimiento de las operaciones realizadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios.

Artículo 316 Bis 17.- Las Instituciones estarán obligadas a realizar revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la infraestructura de cómputo y telecomunicaciones utilizada para la realización de operaciones y prestación de servicios a través de Medios Electrónicos.

Las revisiones a que se refiere el párrafo anterior deberán realizarse al menos en forma anual, o bien, cuando se presenten cambios significativos en dicha infraestructura, debiendo comprender al menos lo siguiente:

- I. Mecanismos de Autenticación de los Usuarios;
- II. Configuración y controles de acceso a la infraestructura de cómputo y telecomunicaciones;
- III. Actualizaciones requeridas para los sistemas operativos y software en general;
- IV. Análisis de vulnerabilidades sobre la infraestructura y sistemas;
- V. Identificación de posibles modificaciones no autorizadas al software original;
- VI. Infraestructura tecnológica, sistemas y procesos asociados a los Medios Electrónicos, a fin de verificar que no se cuente con herramientas o procedimientos que permitan conocer los valores de Autenticación de los Usuarios, así como cualquier información que de manera directa o indirecta pudiera dar acceso a una Sesión en nombre del Usuario, y
- VII. El análisis metódico de los aplicativos críticos relacionados con los servicios de Banca Electrónica, con la finalidad de detectar errores, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información de los Usuarios y de la propia Institución.

Las Instituciones deberán revisar adicionalmente, en los términos de este artículo, los equipos que, en su caso, hayan dispuesto para que sus Usuarios realicen operaciones a través de Medios Electrónicos.

Asimismo, las Instituciones deberán mantener en su infraestructura de cómputo y telecomunicaciones para la operación del servicio de Banca Electrónica, dispositivos y medios automatizados para detectar y prevenir eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de sus Usuarios, así como aquellos que eviten conexiones y flujos de datos entrantes o salientes, no autorizados. Asimismo, las Instituciones deberán mantener controles que eviten la divulgación no autorizada de la información de configuración de dicha infraestructura.

Artículo 316 Bis 18.- Las Instituciones estarán obligadas a contar con áreas de soporte técnico y operacional, integradas por personal capacitado, las cuales se encargarán de atender y dar seguimiento a las incidencias que tengan sus Usuarios del servicio de Banca Electrónica, así como a eventos de seguridad relacionados con el uso de Medios Electrónicos.

Artículo 316 Bis 19.- Las Instituciones deberán procurar la operación continua de la infraestructura de cómputo y de telecomunicaciones, así como dar pronta solución, para restaurar el servicio de Banca Electrónica, en caso de presentarse algún incidente.

Las incidencias deberán informarse a los Comités de Auditoría y de Riesgos de la Institución en la sesión inmediata siguiente a la verificación del evento de que se trate, a efecto de que se adopten las medidas conducentes para prevenir o evitar que se presenten nuevamente.

Artículo 316 Bis 20.- La Dirección General deberá asegurar que la Institución cuente con medidas preventivas, de detección, disuasivas y procedimientos de respuesta a incidentes de seguridad, controles y medidas de seguridad informática para mitigar amenazas y vulnerabilidades relacionadas con los servicios proporcionados a través de Banca Electrónica, que puedan afectar a sus Usuarios o a la operación de la Institución. Las referidas medidas y procedimientos, deberán ser evaluadas por el área de auditoría interna de las Instituciones para determinar su efectividad y, en su caso, realizar las actualizaciones correspondientes. En caso de que se detecten la existencia de vulnerabilidades y riesgos asociados a los servicios mencionados, deberán tomarse medidas de forma oportuna previniendo que los Usuarios o la Institución puedan verse afectados.

Artículo 316 Bis 21.- Las Instituciones deberán implementar las acciones correctivas que la Comisión les requiera, como resultado de la identificación de riesgos asociados con el uso de los servicios de Banca Electrónica.

Artículo 316 Bis 22.- En caso de catástrofes naturales u otras situaciones que afecten la adecuada oferta a nivel nacional de operaciones y servicios bancarios, que por su naturaleza justifiquen temporalmente el uso masivo de Medios Electrónicos, la Comisión podrá autorizar a las Instituciones prestar servicios de Banca Electrónica en términos distintos a los señalados en las presentes disposiciones, de acuerdo con las necesidades del Público Usuario y con los riesgos asociados, por un determinado periodo de tiempo hasta que se restablezcan las condiciones normales."

TRANSITORIOS

PRIMERO.- Las disposiciones aplicables a los servicios de Pago Móvil y Banca Móvil entrarán en vigor el día siguiente al de la publicación de la presente Resolución en el Diario Oficial de la Federación. Las demás disposiciones entrarán en vigor a los seis meses contados a partir del día siguiente al de la citada publicación, salvo lo dispuesto en los Artículos transitorios siguientes.

SEGUNDO.- Las Instituciones contarán con un plazo de un año contado a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para dar cumplimiento a lo establecido en el Artículo 316 Bis 6, fracción II.

Las Instituciones deberán remitir a la Comisión Nacional Bancaria y de Valores a más tardar en un plazo no mayor a ciento ochenta días naturales contados a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, un programa de trabajo para dar cumplimiento a lo establecido en el Artículo 316 Bis 6, fracción II, que comprenda como mínimo las fases del proyecto, las fechas de inicio y conclusión, el responsable del proyecto, los recursos presupuestados y la fecha de implementación.

TERCERO.- Las Instituciones contarán con un plazo de un año y medio contado a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para dar cumplimiento a lo establecido en el Artículo 310, fracción I, inciso b).

CUARTO.- Las Instituciones contarán con un plazo de un año y medio contado a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para dar cumplimiento a lo establecido en el Artículo 316 Bis 8, respecto de Terminales Punto de Venta.

QUINTO.- Las Instituciones que previo a la fecha de publicación de la presente Resolución se encuentren utilizando tablas aleatorias de Contraseñas como Factor de Autenticación Categoría 3 a que se refiere el Artículo 310, en los servicios de Banca Electrónica, contarán con un plazo de dos años contados a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para obtener la autorización a que se refiere el penúltimo párrafo de la fracción III del Artículo 310, en el entendido de que transcurrido dicho plazo sin haber obtenido la autorización referida, las Instituciones no podrán utilizar tablas aleatorias de Contraseñas como Factor de Autenticación Categoría 3 a que se refiere el Artículo 310, en los servicios de Banca Electrónica.

SEXTO.- Las Instituciones tendrán un plazo de dos años contados a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para dar cumplimiento a lo establecido en el Artículo 310, fracción II, inciso b), numeral iii, debiendo utilizar antes de dicho plazo, Factores de Autenticación Categoría 2 a que se refiere el Artículo 310, cuya longitud sea de por lo menos seis caracteres.

SEPTIMO.- Las Instituciones contarán con un plazo de tres años contados a partir del día siguiente al de la publicación en el Diario Oficial de la Federación de la presente Resolución, para dar cumplimiento a lo establecido en el Artículo 316 Bis 10, fracción I en el caso de las Terminales Punto de Venta, incluyendo aquellas de los comercios que agrupan las transacciones de sus diversas Terminales Punto de Venta mediante infraestructura tecnológica y de comunicaciones centralizada.

OCTAVO.- Las Instituciones que previo a la entrada en vigor de la presente Resolución proporcionen servicios de Banca Host to Host, contarán con un plazo de tres años contados a partir del día siguiente al de la publicación de la presente Resolución en el Diario Oficial de la Federación, para adecuarse a lo establecido en dicha Resolución.

NOVENO.- Lo previsto en el Artículo 316 Bis 8 respecto de Cajeros Automáticos entrará en vigor de conformidad con lo siguiente:

- I. El 1 de septiembre de 2011, para los Cajeros Automáticos que sean clasificados por las Instituciones como de alto riesgo.
- II. El 1 de septiembre de 2013, para los Cajeros Automáticos que sean clasificados por las Instituciones como de mediano riesgo.
- III. El 1 de septiembre de 2014, para los Cajeros Automáticos que sean clasificados por las Instituciones como de bajo riesgo.

Para tales efectos, las Instituciones deberán someter a la autorización de la Comisión Nacional Bancaria y de Valores dentro de los seis meses contados a partir del día siguiente al de la publicación de la presente Resolución en el Diario Oficial de la Federación, un programa para el cumplimiento de la obligación contenida en el Artículo 316 Bis 8, que incluya los criterios utilizados para clasificar sus Cajeros Automáticos de acuerdo a su nivel de riesgo.

DECIMO.- Las Instituciones que en términos de lo previsto por el cuarto párrafo de la fracción III del Artículo 310 permitan la realización de operaciones en Cajeros Automáticos y Terminales Punto de Venta mediante el uso de tarjetas bancarias sin circuito integrado, asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas en términos de lo dispuesto por la citada disposición, una vez transcurrido el plazo de tres años contados a partir del día siguiente al de la publicación de la presente Resolución en el Diario Oficial de la Federación.

Atentamente

México, D.F., a 15 de enero de 2010.- El Presidente de la Comisión Nacional Bancaria y de Valores,
Guillermo Enrique Babatz Torres.- Rúbrica.

ANEXO 63

GUÍA PARA EL USO DEL SERVICIO DE BANCA ELECTRONICA

I. POR SERVICIO

a) Servicios Pago Móvil, Banca Móvil y Banca por Internet

A=Artículo, P=Párrafo, B=Bis, F= Fracción, T= Transitorio

Concepto	Pago Móvil	Banca Móvil	Banca por Internet
Resumen	Servicio en el cual el dispositivo de acceso consiste en un Teléfono Móvil del Usuario cuyo número de línea se encuentra asociado al servicio y en el que únicamente se podrán realizar consultas de saldos de las cuentas asociadas al servicio, pagos o transferencias con cargo a una tarjeta o cuenta bancaria y actos para la administración del servicio A1.F67. Se pueden realizar las siguientes operaciones: a) Micro Pagos (70 UDIs) sin registro de cuentas A314.P8 y sin Factor de Autenticación (FA) A313.P3, siempre y cuando la Institución pague las reclamaciones en 48 horas A313.P3 b) Baja Cuantía (250 UDIs) sin registro de cuentas A314.P8 c) Mediana Cuantía (1,500 UDIs) requieren registro de Cuentas Destino A314.P1 b) y c) requieren de un solo FA A313.P2 (NIP de 5 dígitos A310.F2.b).ii) El monto de operaciones está limitado a 1,500 UDIs diarias y 4,000 UDIs mensuales A315.P5	Servicios y operaciones bancarias a través de un Teléfono Móvil del Usuario cuyo número de línea está asociado al servicio A1.F10. Este dato debe ser obtenido de forma automática por la Institución para ser utilizado como identificador de Usuario A308.P4 Los servicios que utilicen navegadores u otras aplicaciones, y cuyo número de línea del Teléfono Móvil no se encuentre asociado al servicio, son considerados Banca por Internet	Servicios y operaciones bancarias realizadas a través de Internet, en el sitio que corresponda a uno o más dominios de la Institución, incluyendo el acceso mediante el protocolo WAP o equivalente A1.F11 El acceso al servicio puede realizarse mediante cualquier equipo (PC, Teléfono Móvil, PDA) con conexión a Internet
Contratación	A través de uno de los siguientes: a) Centros de atención telefónica A307.F3 b) Con firma autógrafa A307.F1 c) En otro servicio utilizando un Segundo Factor de Autenticación (2FA) A307.F2.P1. Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos A307.F2.P2	A través de uno de los siguientes: a) Con firma autógrafa A307.F1 b) En otro servicio utilizando un 2FA A307.F2.P1. Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos A307.F2.P2 Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados A306.F1.c)	A través de uno de los siguientes: a) Con firma autógrafa A307.F1 b) En otro servicio utilizando un 2FA A307.F2.P1. Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos A307.F2.P2 c) Con firma electrónica avanzada o fiable (únicamente para realizar operaciones entre la cuenta del Usuario y una cuenta del propio Usuario en otra Institución). Se requiere autorización A307.F5

Concepto	Pago Móvil	Banca Móvil	Banca por Internet
	Se pueden asociar hasta dos tarjetas o cuentas bancarias del mismo Usuario a un número de línea de Teléfono Móvil, siempre y cuando solamente una de ellas funcione bajo la modalidad de Operaciones de Micro Pagos ^{A307.F3.P2} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}		Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}
Identificador de Usuario	Número de la línea del teléfono móvil obtenido automáticamente por la Institución ^{A308.P4}	Número de la línea del teléfono móvil obtenido automáticamente por la Institución ^{A308.P4}	Identificador único de Usuario ^{A308.P2} definido por la Institución o por el propio Usuario de mínimo seis caracteres de longitud ^{A308.P3}
Factores de Autenticación	Factor Categoría 2: Contraseña o Número de Identificación Personal (NIP) de 5 caracteres ^{A310.F2.b).ii}	Factor Categoría 2: Contraseña o NIP de 6 caracteres ^{A310.F2.b)} , más cualquiera de los siguientes: Factor Categoría 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} . Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6} , para ello requieren autorización ^{A310.F3.P6} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P7} (Aplica A5T), ó; Factor Categoría 4: Biométricos ^{A310.F4.P1}	Factor Categoría 2: Contraseña o NIP de 8 caracteres (Aplica A6T) ^{A310.F2.b).iii} , más cualquiera de los siguientes: Factor Categoría 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} . Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6} , para ello requieren autorización ^{A310.F3.P6} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P7} (Aplica A5T), ó; Factor Categoría 4: Biométricos ^{A310.F4.P1}
Autenticación de la Institución por el Usuario	No Aplica	No Aplica	Se debe proporcionar información que solo el Usuario conozca antes de ingresar todos los elementos de identificación y Autenticación del Usuario ^{A311.F1} Una vez que el Usuario identifique a la Institución e inicie Sesión, la Institución desplegará fecha y hora del último acceso al servicio de Banca Electrónica y nombre completo ^{A311.F2}
Impedir la lectura en pantalla de la información de Autenticación	Puede no enmascarse el NIP , para ello requieren autorización ^{A309.F1.P2} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A309.F1.P3}	Aplica ^{A309.F1}	Aplica ^{A309.F1}

Concepto	Pago Móvil	Banca Móvil	Banca por Internet
Operaciones y uso de un 2FA Categoría 3 (OTP) ó 4 (Biométrico)	No requiere un 2FA para Operaciones Monetarias ^{A313.P2} Operaciones Monetarias permitidas: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} Se pueden realizar pagos de hasta 70 UDIs sin necesidad de utilizar ningún FA ^{A313.P3}. Se requiere autorización y deberán asumir por escrito el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A313.P3}	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento e incremento de límites de monto ^{A313.F3} d) Registro de Cuentas Destino ^{A313.F4} e) Alta y modificación del medio de notificación ^{A313.F5} f) Consultas de estados de cuenta ^{A313.F6} g) Contratación de otro servicio ^{A313.F7} h) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso f), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3} Se pueden realizar pagos de hasta 70 UDIs sin necesidad de utilizar ningún FA ^{A313.P3}. Se requiere autorización y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A313.P3}	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento e incremento de límites de monto ^{A313.F3} d) Registro de Cuentas Destino ^{A313.F4} e) Alta y modificación del medio de notificación ^{A313.F5} f) Consultas de estados de cuenta ^{A313.F6} g) Contratación de otro servicio ^{A313.F7} h) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso f), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3} En el caso de personas morales, no será obligatorio el uso de un 2FA por cada operación, si se utilizan mecanismos mediante los cuales una persona realiza la solicitud de la operación y otra es quien la autoriza ^{A313.P5}. Se requiere autorización y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A313.P6}
Registro de Cuentas Destino	Para operaciones mayores a 250 UDIs se requiere el registro de Cuentas Destino ^{A314.P8}. Las Cuentas Destino serán habilitadas treinta minutos posteriores a su registro ^{A314.P5} No es posible registrar cuentas por este servicio ^{A1.F67} Se pueden registrar cuentas	Para operaciones mayores a 250 UDIs se requiere el registro de Cuentas Destino ^{A314.P8}, las cuales se habilitarán al momento de registrarlas por este servicio ^{A314.P5} Se pueden registrar en el mismo servicio usando un 2FA Categorías 3 ó 4 ^{A313.F4}, mediante firma autógrafa ^{A313.F1.P2}, o en otro	Se requiere el registro de Cuentas Destino ^{A314.P1}, las cuales se habilitarán treinta minutos posteriores a su registro ^{A314.P5} Se pueden registrar en el mismo servicio usando un 2FA Categorías 3 ó 4 ^{A313.F4}, mediante firma autógrafa ^{A313.F1.P2}, o en otro servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4}

Concepto	Pago Móvil	Banca Móvil	Banca por Internet
	mediante firma autógrafa ^{A313.F1.P2} o en otro servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5}	servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5}	Se pueden habilitar Cuentas Destino antes de los 30 minutos siempre y cuando las operaciones no excedan del equivalente a las Operaciones Monetarias de Baja Cuantía (250 UDIs) y 1,000 UDIs mensuales ^{A314.P6}, para ello requieren autorización ^{A314.P6} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5} Las Cuentas Destino registradas por personas morales utilizando mecanismos mediante los cuales una persona realiza la solicitud de la operación y otra es quien la autoriza podrán quedar habilitadas antes de los 30 minutos ^{A313.P5}. Se requiere autorización y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A313.P6} En el caso de personas morales y personas físicas con actividad empresarial, se podrá permitir el registro de un conjunto de Cuentas Destino considerándolo como una sola operación ^{A314.P4}
Notificaciones	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Modificación de Contraseñas y NIPs ^{A316.B1.F8} No se requieren notificaciones para las operaciones referidas en los incisos a) y b) en los siguientes casos: a) El monto acumulado diario sea menor o igual a 600 UDIs ^{A316.B1.P3}	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Modificación de límites de montos ^{A316.B1.F3} d) Registro de Cuentas Destino ^{A316.B1.F4} e) Alta y modificación del medio de notificación (al nuevo y al anterior, en caso de cambio) ^{A316.B1.F5} f) Contratación de otro servicio o modificación de condiciones en el uso ^{A316.B1.F6}	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Modificación de límites de montos ^{A316.B1.F3} d) Registro de Cuentas Destino ^{A316.B1.F4} e) Alta y modificación del medio de notificación (al nuevo y al anterior, en caso de cambio) ^{A316.B1.F5} f) Contratación de otro servicio o modificación de condiciones en el uso ^{A316.B1.F6} g) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7}

Concepto	Pago Móvil	Banca Móvil	Banca por Internet
	b) La operación sea menor o igual a 250 UDIs y cuenten con esquemas de prevención de fraudes A316.B1.P3	g) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio A316.B1.F7 h) Modificación de Contraseñas y NIPs A316.B1.F8	h) Modificación de Contraseñas y NIPs A316.B1.F8
Límites de monto operativos	Se pueden realizar Operaciones Monetarias de hasta Mediana Cuantía (1,500 UDIs diarias) y 4,000 UDIs mensuales A315.P5 Operaciones de hasta Mediana Cuantía A1.F67 requieren registro previo de cuentas A314.P1 Se pueden realizar Operaciones de Baja Cuantía (250 UDIs) sin registro de Cuentas Destino A314.P8 Para Operaciones de Micro Pagos, el saldo disponible de la cuenta asociada debe ser menor o igual a 70 UDIs A315.P5	Límite definido por el Usuario A315.P2 sin sobrepasar los límites establecidos por la propia Institución A315.P6 Se pueden realizar Operaciones hasta de Baja Cuantía (250 UDIs) sin registro de Cuentas Destino A314.P8 Para Operaciones de Micro Pagos, el saldo disponible de la cuenta asociada debe ser menor o igual a 70 UDIs A315.P5	Límite definido por el Usuario A315.P2 sin sobrepasar los límites establecidos por la propia Institución A315.P6 Se limitan a Operaciones Monetarias de Baja Cuantía (250 UDIs) y hasta 1,000 UDIs mensuales, a las Cuentas Destino que queden habilitadas antes de pasar 30 minutos desde su registro A314.P6, para ello requieren autorización A314.P6
Controles para establecer límites de monto aplicables al mismo canal o a otro	No es posible establecer o incrementar límites de monto en este servicio A1.F67	Proveer lo necesario para que los Usuarios establezcan límites de monto A315.P2. Para establecer o incrementar, se requiere firma autógrafa A315.P1 o un 2FA Categoría 3 ó 4 en el mismo servicio o en otro A313.F4 Para disminuir, mismo servicio con FA Categoría 2 A315.P3	Proveer lo necesario para que los Usuarios establezcan límites de monto A315.P2. Para establecer o incrementar, se requiere firma autógrafa A315.P1 o un 2FA Categoría 3 ó 4 en el mismo servicio o en otro A313.F4 Para disminuir, mismo servicio con FA Categoría 2 A315.P3
Seguridad en el envío de Contraseñas y Números de Identificación Personal	Podrán implementar controles compensatorios para proteger la transmisión de Información Sensible del Usuario A316.B10.F1.P4	Transmisión cifrada de Información Sensible del Usuario desde el Dispositivo de Acceso hasta su recepción por la Institución A316.B10.F1	Transmisión cifrada de Información Sensible del Usuario desde el Dispositivo de Acceso hasta su recepción por la Institución A316.B10.F1
Activación / Desactivación Servicios	Los Usuarios deberán tener la opción de desactivar en forma temporal el servicio A316.B5.P1 en el mismo servicio o en otro con un FA A316.B5.P1.P2 La reactivación se puede hacer en un centro de atención telefónica o usando los medios de contratación A316.B5.P3	Los Usuarios deberán tener la opción de desactivar en forma temporal el servicio A316.B5.P1 en el mismo servicio o en otro con un FA A316.B5.P1.P2 La reactivación se puede hacer en un centro de atención telefónica o usando los medios de contratación A316.B5.P3	No aplica

b) Servicios de Banca Electrónica ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta

A=Artículo, P=Párrafo, B=Bis, F= Fracción, T= Transitorio

Concepto	Cajeros Automáticos	Terminal Punto de Venta
Resumen	Servicios de Banca Electrónica proporcionados a través de Dispositivos de Acceso de autoservicio que permiten realizar consultas y operaciones bancarias y al cual se accede mediante una tarjeta o cuenta bancaria ^{A1.F17} Deben contar con lectores que permitan obtener información de Tarjetas Bancarias con Circuito Integrado ^{A316.B8} (Aplica A9T)	Servicios de Banca Electrónica proporcionados a través de Dispositivos de Acceso, tales como terminales de cómputo, teléfonos móviles y programas de cómputo, operados por comercios o Usuarios para el pago de bienes o servicios con cargo a una tarjeta o cuenta bancaria ^{A1.F91} Deben contar con lectores que permitan obtener información de Tarjetas Bancarias con Circuito Integrado ^{A316.B8} (Aplica A4T)
Contratación	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un Segundo Factor de Autenticación (2FA) ^{A307.F2.P1}. Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Tratándose de tarjetas prepagadas o las cuentas a que se refiere la Décima Cuarta de las Disposiciones de Carácter General a que se refiere el Artículo 115 de la Ley de Instituciones de Crédito (LIC), no requiere consentimiento mediante firma autógrafa para su uso ^{A307.F1.b)} No se puede contratar otro servicio desde este medio ^{A307.F2.P3} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un 2FA ^{A307.F2.P1}. Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Tratándose de tarjetas prepagadas o las cuentas a que se refiere la Décima Cuarta de las Disposiciones de Carácter General a que se refiere el Artículo 115 de la LIC, no requiere consentimiento mediante firma autógrafa para su uso ^{A307.F1.b)} No se puede contratar otro servicio desde este medio ^{A307.F2.P3} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}
Identificación de Usuario	Puede ser el número de tarjeta bancaria ^{A308.P4}	Puede ser el número de tarjeta bancaria ^{A308.P4}
Factores de Autenticación	Factor 2: Contraseña o NIP de 4 dígitos ^{A310.F2.b).i} más cualquiera de los siguientes: Factor 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} y Tarjetas Bancarias con Circuito Integrado ^{A310.F3.P3} Asimismo se podrán usar Tarjetas Bancarias sin Circuito Integrado siempre y cuando las Instituciones que aprueben las operaciones asuman el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P4} (Aplica A10T) Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la	Factor 2: Contraseña o NIP de 4 dígitos ^{A310.F2.b).i} más cualquiera de los siguientes: Factor 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} y Tarjetas Bancarias con Circuito Integrado ^{A310.F3.P3} Asimismo se podrán usar Tarjetas Bancarias sin Circuito Integrado siempre y cuando las Instituciones que aprueben las operaciones asuman el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P4} (Aplica A10T)

Concepto	Cajeros Automáticos	Terminal Punto de Venta
	Institución o por terceros ^{A310.F3.P6}, para ello requieren autorización ^{A310.F3.P6} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P7} (Aplica A5T), ó; Factor 4: Biométricos ^{A310.F4.P1}	Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6}, para ello requieren autorización ^{A310.F3.P6} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P7} (Aplica A5T), ó; Factor 4: Biométricos ^{A310.F4.P1}
Impedir la lectura en pantalla de la información de Autenticación	Aplica ^{A309.F1}	Aplica ^{A309.F1}
Operaciones y uso de un 2FA Categoría 3 (OTP) ó 4 (Biométrico)	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento de límites de monto ^{A313.F3} d) Registro de Cuentas Destino ^{A313.F4} e) Alta del medio de notificación ^{A313.F5} f) Consultas de estados de cuenta ^{A313.F6} g) Desbloqueo de Contraseñas o NIPs ^{A313.F8} h) Retiro de efectivo ^{A313.F9} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso f), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3} No se puede modificar el medio de notificación en este servicio ^{A316.B1.P4} Los Cajeros Automáticos que las Instituciones pongan a disposición de los Usuarios para realizar operaciones deberán contar con lectores que obtengan la información directamente del circuito de las Tarjetas Bancarias con Circuito Integrado ^{A316.B8} (Aplica A9T)	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento de límites de monto ^{A313.F3} d) Registro de Cuentas Destino ^{A313.F4} e) Alta del medio de notificación ^{A313.F5} f) Consultas de estados de cuenta ^{A313.F6} g) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso f), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3} Se pueden realizar pagos de hasta 70 UDIs sin necesidad de utilizar un FA ^{A313.P3}. Se requiere autorización y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A313.P3}

Concepto	Cajeros Automáticos	Terminal Punto de Venta
		No se puede modificar el medio de notificación en este servicio ^{A316.B1.P4} Las Terminales Punto de Venta que las Instituciones pongan a disposición de los Usuarios para realizar operaciones deberán contar con lectores que obtengan la información directamente del circuito de las Tarjetas Bancarias con Circuito Integrado ^{A316.B8} (Aplica A4T)
Registro de Cuentas Destino	No requiere registro de Cuentas Destino ^{A314.P8}	No requiere registro de Cuentas Destino ^{A314.P8}
Notificaciones	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros y otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Establecimiento de límites de monto ^{A316.B1.F3} d) Registro de Cuentas Destino de terceros u otras Instituciones ^{A316.B1.F4} e) Alta del medio de notificación ^{A316.B1.F5} f) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7} g) Modificación de Contraseñas y NIPs ^{A316.B1.F8} h) Retiro de efectivo ^{A316.B1.F9} No se requieren notificaciones para las operaciones referidas en los incisos a) y b) en los siguientes casos: a) El monto acumulado diario sea menor o igual a 600 UDIs ^{A316.B1.P3} b) La operación sea menor o igual a 250 UDIs y cuenten con esquemas de prevención de fraudes ^{A316.B1.P3}	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros y otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Establecimiento de límites de monto ^{A316.B1.F3} d) Registro de Cuentas Destino de terceros u otras Instituciones ^{A316.B1.F4} e) Alta del medio de notificación ^{A316.B1.F5} f) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7} g) Modificación de Contraseñas y NIPs ^{A316.B1.F8} No se requieren notificaciones para las operaciones referidas en los incisos a) y b) en los siguientes casos: a) El monto acumulado diario sea menor o igual a 600 UDIs ^{A316.B1.P3} b) La operación sea menor o igual a 250 UDIs y cuenten con esquemas de prevención de fraudes ^{A316.B1.P3}
Límites de monto operativos	Límite de 1,500 UDIs diarias por cuenta ^{A315.P4}	No aplica
Controles para establecer límites de monto aplicables al mismo canal o a otro	Es posible establecer o incrementar mediante firma autógrafa ^{A315.P1} o con un 2FA Categoría 3 ó 4 en otro servicio ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 2 ^{A315.P3}	Es posible establecer o incrementar mediante firma autógrafa ^{A315.P1} o con un 2FA Categoría 3 ó 4 en otro servicio ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 2 ^{A315.P3}

Concepto	Cajeros Automáticos	Terminal Punto de Venta
Seguridad en el envío de Contraseñas y Números de Identificación Personal	Transmisión cifrada de Información Sensible del Usuario A316.B10.F1	Transmisión cifrada de Información Sensible del Usuario A316.B10.F1 (Aplica A7T)
Activación / Desactivación Servicios	No aplica	No aplica

c) Servicio de Banca Telefónica Audio Respuesta y Banca Telefónica Voz a Voz

A=Artículo, P=Párrafo, B=Bis, F= Fracción, T= Transitorio

Concepto	Banca Telefónica Audio Respuesta (IVR)	Banca Telefónica Voz - Voz
Resumen	Servicios y operaciones bancarias realizadas por el Usuario a través de un sistema telefónico de audio respuesta (IVR) ^{A1.F12} Uso de un Segundo Factor de Autenticación (2FA) para realizar Operaciones y Servicios bancarios A313.F1	Servicio mediante el cual el Usuario instruye vía telefónica a un representante para realizar operaciones a su nombre ^{A1.F13} La autenticación se realiza mediante cuestionarios que incluyen información que el Usuario conoce y la Institución valida ^{A312.F1}
Contratación	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un 2FA ^{A307.F2.P1} . Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un 2FA ^{A307.F2.P1} . Asimismo, requiere confirmar la contratación utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}
Identificador de Usuario	Identificador único de Usuario ^{A308.P2} definido por la Institución o por el propio Usuario de mínimo seis caracteres de longitud ^{A308.P3}	Identificador único de Usuario ^{A308.P2} definido por la Institución o por el propio Usuario de mínimo seis caracteres de longitud ^{A308.P3}
Factores de Autenticación	Factor 2: Contraseñas o NIP de 6 dígitos ^{A310.F2.b)} , más cualquiera de los siguientes: Factor 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} . Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6} , para ello requieren autorización ^{A310.F3.P6} y deberán asumir el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.F3.P7} (Aplica A5T) , ó; Factor 4: Biométricos ^{A310.F4.P1}	Factor 1: Información proporcionada a través de cuestionarios en centros de atención telefónica ^{A310.F1.P1} (Aplica A3T) Incluye información parcial de los FA categorías 2 o 3 , proporcionada a operadores telefónicos, siempre que el usuario haya iniciado la llamada y la información sea utilizada para realizar operaciones de este servicio ^{A316.B4.F3.P2}

Concepto	Banca Telefónica Audio Respuesta (IVR)	Banca Telefónica Voz - Voz
Impedir la lectura en pantalla de la información de Autenticación	Excepción, no se requiere enmascarar ^{A309.F1}	No aplica
Operaciones y uso de un 2FA Categoría 3 (OTP) ó 4 (Biométrico)	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento e incremento de límites de monto ^{A313.F3} d) Registro de Cuentas Destino ^{A313.F4} e) Alta y modificación del medio de notificación ^{A313.F5} f) Consultas de estados de cuenta ^{A313.F6} g) Contratación de otro servicio ^{A313.F7} h) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un Factor de Autenticación (FA) Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso f), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3}	Operaciones permitidas utilizando un FA Categoría 1 (Información en centros de atención telefónica) ^{A312.F1}. Incluye información parcial de los FA categorías 2 o 3, proporcionada a operadores telefónicos, siempre que el usuario haya iniciado la llamada y la información sea utilizada para realizar operaciones de este servicio ^{A316.B4.F3.P2}. Requiere registro de cuentas mediante firma autógrafa ^{A313.P3} o en otro servicio con 2FA, Categorías 3 ó 4 ^{A314.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Establecimiento e incremento de límites de monto ^{A313.F3} d) Alta y modificación del medio de notificación ^{A313.F5} e) Consultas de estados de cuenta ^{A313.F6} f) Contratación de otro servicio (sólo Pago Móvil) ^{A312.F2} g) Desbloqueo de Contraseñas o NIPs ^{A313.F8}
Registro de Cuentas Destino	Se requiere el registro de Cuentas Destino ^{A314.P1}, las cuales se habilitarán treinta minutos posteriores a su registro ^{A314.P5} Se pueden registrar en el mismo servicio usando un 2FA Categorías 3 ó 4 ^{A313.F4}, mediante firma autógrafa ^{A313.F1.P2}, o en otro servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5}	Se requiere el registro de Cuentas Destino ^{A314.P1}, las cuales se habilitarán treinta minutos posteriores a su registro ^{A314.P5} No se pueden realizar registros de cuentas en este servicio ^{A314.P3} Se pueden registrar Cuentas Destino mediante firma autógrafa ^{A313.F1.P2} o en otro servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5}

Concepto	Banca Telefónica Audio Respuesta (IVR)	Banca Telefónica Voz - Voz
Notificaciones	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros y otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Alta y modificación de límites de montos ^{A316.B1.F3} d) Registro de Cuentas Destino ^{A316.B1.F4} e) Alta y modificación del medio de notificación (al nuevo y al anterior, en caso de cambio) ^{A316.B1.F5} f) Contratación de otro servicio o modificación de condiciones en el uso ^{A316.B1.F6} g) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7} h) Modificación de Contraseñas y NIPs ^{A316.B1.F8}	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1}: a) Transferencias a cuentas de terceros y otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Alta y modificación de límites de montos ^{A316.B1.F3} d) Alta y modificación del medio de notificación (al nuevo y al anterior, en caso de cambio) ^{A316.B1.F5} e) Contratación de otro servicio o modificación de condiciones en el uso ^{A316.B1.F6} f) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7}
Límites de monto operativos	Límite definido por el Usuario sin sobrepasar los límites establecidos por las disposiciones o por la misma Institución ^{A315.P6}	Límite definido por el Usuario sin sobrepasar los límites establecidos por las disposiciones o por la misma Institución ^{A315.P6}
Controles para establecer límites de monto aplicables al mismo canal o a otro	Proveer lo necesario para que los Usuarios establezcan límites de monto ^{A315.P2}. Para establecer o incrementar, se requiere firma autógrafa ^{A315.P1} o un 2FA Categoría 3 ó 4 en el mismo servicio o en otro ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 2 ^{A315.P3}	Proveer lo necesario para que los Usuarios establezcan límites de monto ^{A315.P2}. Para establecer o incrementar, se requiere firma autógrafa ^{A315.P1}, en el mismo servicio con un FA categoría 1 ^{A312.F1}, con información parcial de un FA categoría 2 o 3 ^{A316.B4.F3.P2}, ó con 2FA Categoría 3 ó 4 en otro servicio ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 1 ^{A315.P3}
Seguridad en el envío de Contraseñas y Números de Identificación Personal	Podrán implementar controles compensatorios para proteger la transmisión de Información Sensible del Usuario ^{A316.B10.F1.P4}	Podrán implementar controles compensatorios para proteger la transmisión de Información Sensible del Usuario ^{A316.B10.F1.P4}
Activación / Desactivación Servicios	No aplica	No aplica

d) Banca Host to Host y otro servicio no especificado en las Disposiciones

A=Artículo, P=Párrafo, B=Bis, F= Fracción, T= Transitorio

Concepto	Banca Host to Host	Otro Servicio
Resumen	Conexión directa entre equipos de cómputo del Usuario y de la Institución, incluye aplicaciones conocidas como <i>cliente-servidor</i> ^{A1.F9} (Aplica A8T) Servicios utilizados por personas morales o personas físicas con actividad empresarial Generalmente se utiliza para altos volúmenes de operaciones	Cualquier otro servicio de Banca Electrónica no definido en las presentes Disposiciones
Contratación	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un Segundo Factor de Autenticación (2FA) ^{A307.F2.P1} . Asimismo, requiere confirmar utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}	A través de uno de los siguientes: a) Con firma autógrafa ^{A307.F1} b) En otro servicio utilizando un 2FA ^{A307.F2.P1} . Asimismo, requiere confirmar utilizando un 2FA adicional en un periodo no menor a 30 minutos ^{A307.F2.P2} Se deben establecer los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados ^{A306.F1.c)}
Identificador de Usuario	Identificador único de Usuario ^{A308.P2} definido por la Institución o por el propio Usuario de mínimo seis caracteres de longitud ^{A308.P3}	Identificador único de Usuario ^{A308.P2} definido por la Institución o por el Usuario de mínimo seis caracteres de longitud ^{A308.P3}
Factores de Autenticación	Factor 2: Contraseña o NIP de 6 dígitos ^{A310.F2.b)} , más cualquiera de los siguientes: Factor 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} o mecanismos para validar los equipos de cómputo autorizados por la Institución ^{A310.F3.P5} . Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6} , para ello requieren autorización ^{A310.P6} y deberán asumir por escrito el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.P7} (Aplica A5T) , ó; Factor 4: Biométricos ^{A310.F4.P1}	Factor 2: Contraseñas o NIP de 6 dígitos ^{A310.F2.b)} , más cualquiera de los siguientes: Factor 3: Contraseñas de un solo uso (OTP) ^{A310.F3.P1} . Se podrán usar tablas aleatorias de Contraseñas con características que impidan su duplicación, información que no se pueda usar más de una vez y que la información no sea conocida por personal de la Institución o por terceros ^{A310.F3.P6} , para ello requieren autorización ^{A310.F3.P6} y deberán asumir por escrito el riesgo y los costos de operaciones no reconocidas, abonando al Usuario antes de 48 horas ^{A310.P7} (Aplica A5T) , ó; Factor 4: Biométricos ^{A310.F4.P1}
Impedir la lectura en pantalla de la información de Autenticación	Aplica ^{A309.F1}	Aplica ^{A309.F1}

Concepto	Banca Host to Host	Otro Servicio
Operaciones y uso de un 2FA Categoría 3 (OTP) ó 4 (Biométrico)	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Registro de Cuentas Destino ^{A313.F4} d) Alta y modificación del medio de notificación ^{A313.F5} e) Consultas de estados de cuenta ^{A313.F6} f) Contratación de otro servicio ^{A313.F7} g) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso e), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3}	Operaciones permitidas utilizando un 2FA ^{A313.P1}: a) Transferencias a cuentas de terceros u otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A313.F1} b) Pago de impuestos ^{A313.F2} c) Registro de Cuentas Destino ^{A313.F4} d) Alta y modificación del medio de notificación ^{A313.F5} e) Consultas de estados de cuenta ^{A313.F6} f) Contratación de otro servicio ^{A313.F7} g) Desbloqueo de Contraseñas o NIPs ^{A313.F8} En el caso del inciso a), se podrá requerir un FA Categoría 2, 3 ó 4 para Cuentas Destino registradas en Oficinas Bancarias utilizando firma autógrafa ^{A313.F1.P2} En el caso del inciso e), se podrán consultar estados de cuenta utilizando un FA Categoría 2 cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación correspondiente ^{A313.F6.P3}
Registro de Cuentas Destino	No requiere registro de Cuentas Destino ^{A314.P8}	Se requiere el registro de Cuentas Destino ^{A314.P1}, las cuales se habilitarán treinta minutos posteriores a su registro ^{A314.P5} Se pueden registrar en el mismo servicio usando un 2FA Categorías 3 ó 4 ^{A313.F4}, mediante firma autógrafa ^{A313.F1.P2}, o en otro servicio ^{A314.P1} con 2FA, Categorías 3 ó 4 ^{A313.F4} Las Cuentas Destino registradas mediante firma autógrafa podrán quedar habilitadas antes de los 30 minutos ^{A314.P5} En el caso de personas morales y personas físicas con actividad empresarial, se podrá permitir el registro de un conjunto de Cuentas Destino considerándolo como una sola operación ^{A314.P4}

Concepto	Banca Host to Host	Otro Servicio
Notificaciones	No aplica ^{A316.B1.P5}	Se deberá notificar por el medio de comunicación proporcionado por el Usuario, en su caso, los siguientes eventos ^{A316.B1.P1} : a) Transferencias a cuentas de terceros y otras Instituciones, incluyendo el pago de créditos y bienes o servicios, así como autorizaciones e instrucciones de domiciliación de pagos de bienes o servicios ^{A316.B1.F1} b) Pago de impuestos ^{A316.B1.F2} c) Modificación de límites de montos ^{A316.B1.F3} d) Registro de Cuentas Destino ^{A316.B1.F4} e) Alta y modificación del medio de notificación (al nuevo y al anterior, en caso de cambio) ^{A316.B1.F5} f) Contratación de otro servicio o modificación de condiciones en el uso ^{A316.B1.F6} g) Desbloqueo de Contraseñas y NIPs, así como reactivaciones del servicio ^{A316.B1.F7} h) Modificación de Contraseñas y NIPs ^{A316.B1.F8}
Límites de monto operativos	No aplica	No aplica
Controles para establecer límites de monto aplicables al mismo canal o a otro	Para establecer o incrementar, se requiere firma autógrafa ^{A315.P1} o un 2FA Categoría 3 ó 4 en el mismo servicio o en otro ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 2 ^{A315.P3}	Para establecer o incrementar, se requiere firma autógrafa ^{A315.P1} o un 2FA Categoría 3 ó 4 en el mismo servicio o en otro ^{A313.F4} Para disminuir, mismo servicio con FA Categoría 2 ^{A315.P3}
Seguridad en el envío de Contraseñas y Números de Identificación Personal	Transmisión cifrada de Información Sensible del Usuario ^{A316.B10.F1}	Transmisión cifrada de Información Sensible del Usuario ^{A316.B10.F1}
Activación / Desactivación Servicios	No aplica	No aplica

II. GENERALES

Disposición	Detalle
Definición Factores de Autenticación	Mecanismo de autenticación, basado en características del Usuario, dispositivos o información que sólo el Usuario posea o conozca ^{A1.F35} Factor 1: Información proporcionada mediante la aplicación de cuestionarios en centros de atención telefónica ^{A1.F35.a)} Factor 2: Información que sólo el Usuario conoce, tales como: Contraseñas y Números de Identificación Personal ^{A1.F35.b)} Factor 3: Información que sólo el usuario tiene, tales como generadores de contraseñas de un solo uso (OTP) "Tokens" o Tarjetas Bancarias con Circuito Integrado ^{A1.F35.c)} Factor 4: Información biométrica. Huellas digitales, geometría de la mano ^{A1.F35.d)}
Operaciones Monetarias	Transacción que implique transferencias de recursos dinerarios, las cuales podrán ser ^{A1.F64.} Micropagos: 70 UDIs ^{A1.F64.a)} Baja Cuantía: 250 UDIs diarias ^{A1.F64.b)} Mediana Cuantía: 1,500 UDIs diarias ^{A1.F64.c)} Montos superiores a 1,500 UDIs diarias ^{A1.F64.d)}
Comprobantes	Se deberá emitir un comprobante de cada una de las operaciones realizadas ^{A316.B}
Sesiones Seguras	La Sesión debe terminarse en forma automática cuando se detecte ^{A316.B2.F1.} -- Inactividad del Usuario por más de veinte minutos ^{A316.B2.F1.a)} -- Cuando existan cambios relevantes en la conexión del servicio de Banca por Internet ^{A316.B2.F1.b)} Deben evitarse sesiones simultáneas ^{A316.B2.F2} y se debe advertir al Usuario en caso de enlaces a servicios de terceros ^{A316.B2.F3}
Equipos Electrónicos o de Telecomunicaciones Dispuestos por la Institución	Adoptar medidas que impidan la instalación de dispositivos o programas que permitan que la información del Usuario sea copiada o modificada por terceros ^{A316.B6.F1} Contar con procedimientos que permitan correlacionar la información de las operaciones no reconocidas por los clientes con la operativa de los equipos y del personal que los administra ^{A316.B6.F2} (Aplica A2T)
Base de Datos Operaciones no Reconocidas	Deberán mantener bases de datos con información de incidencias, fallas y vulnerabilidades, así como operaciones no reconocidas por los Usuarios ^{A316.B14}
Centros de Atención Telefónica	Los centros de atención telefónica deberán mantener controles de seguridad física y lógica para evitar que la información de los clientes pueda ser extraída o copiada ^{A316.B7.F1} , delimitar funciones de operadores ^{A316.B7.F2} y evitar el uso de medios diferentes a los autorizados ^{A316.B7.F3}
Cifrado	En la transmisión y almacenamiento de Información Sensible del Usuario, deberán utilizarse mecanismos de Cifrado con llaves criptográficas ^{A316.B10.F1} . Adicionalmente, las llaves criptográficas y el proceso de Cifrado y descifrado deberán estar instalados en dispositivos de alta seguridad (HSM) ^{A316.B10.F4}
Reporte de eventos de pérdida de información	En caso de que la Información Sensible del Usuario sea extraída, extraviada o se sospeche de algún incidente de acceso no autorizado, deberán ^{A316.B12.} -- Dar aviso por escrito a esta Comisión en cinco días naturales ^{A316.B12.F1} -- Realizar una investigación, enviando los resultados a esta Comisión a los cinco días naturales de concluida y notificar a los Usuarios afectados, en su caso ^{A316.B12.F2}
Prevención de Fraudes	Deberán mantener mecanismos de control para detección de eventos que se aparten de los parámetros de uso habitual de los Usuarios ^{A316.B13}
Bitácoras	Deberán mantener registros, bitácoras, huellas de auditoría y grabaciones de voz relativos a ^{A316.B15.F1.} -- Accesos a los Medios Electrónicos ^{A316.B15.F1.a)} -- Datos de las operaciones realizadas (fechas, horas, dispositivos de acceso) ^{A316.B15.F1.b) y c)} Deberán mantener controles para que la información registrada en los equipos críticos de cómputo y telecomunicaciones utilizados en las operaciones de Banca Electrónica sea consistente. ^{A316.B15.F2}

Disposición	Detalle
Revisiones de Seguridad	Anualmente, deberán realizar revisiones de seguridad que comprendan ^{A316.B17.}: -- Mecanismos de Autenticación ^{A316.B17.F1} -- Configuración y control de acceso de la Infraestructura de Cómputo y Telecomunicaciones ^{A316.B17.F2} -- Actualizaciones de software (parches) ^{A316.B17.F3} -- Análisis de vulnerabilidades ^{A316.B17.F4} -- Identificación de modificaciones al software original ^{A316.B17.F5} -- Infraestructura tecnológica, sistemas y procesos asociados a los Medios Electrónicos ^{A316.B17.F6} -- Análisis metódico de aplicativos críticos relacionados con servicios de Banca Electrónica ^{A316.B17.F7} Adicionalmente, deberán mantener esquemas de monitoreo permanente ^{A316.B17.P4}
Acciones correctivas	Deberán implementar las acciones correctivas que la Comisión les requiera, como resultado de la identificación de riesgos asociados con el uso de los servicios de Banca Electrónica ^{A316.B21}
Medidas preventivas y detección	La Dirección General deberá asegurar que la Institución cuenta con medidas preventivas, de detección, disuasivas y procedimientos de respuesta a incidentes de seguridad, controles y medidas de seguridad informática para mitigar amenazas, vulnerabilidades derivadas del uso de la Banca Electrónica y que puedan afectar las operaciones de la Institución ^{A316.B20}
Acciones contingentes	La Comisión podrá autorizar que las Instituciones realicen operaciones en términos distintos a los establecidos en las Disposiciones en caso de catástrofes naturales o situaciones que afecten la adecuada oferta a nivel nacional de operaciones o servicios bancarios que justifiquen el uso masivo de los Medios Electrónicos en forma temporal ^{A316.B22}

ANEXO 64

**REPORTE DE EVENTOS DE PERDIDA DE INFORMACION ADMINISTRADA
A TRAVES DE MEDIOS ELECTRONICOS**

I. Información de la Institución Financiera

1. Nombre de la Institución Financiera
2. Dirección de la(s) oficina(s) donde ocurrió el incidente de seguridad informática
 - 2.1. Ciudad
 - 2.2. Estado
 - 2.3. Código Postal
3. ¿La información involucrada era administrada por terceros? [Sí] [No]
 En caso afirmativo:
 - 3.1. Nombre del proveedor
 - 3.2. Dirección del proveedor
 - 3.3. Contacto

II. Información del incidente de seguridad informática

1. Breve descripción del incidente de seguridad informática
2. Información comprometida

Información personal del Usuario		En conjunto con:	
Nombres	☐		Número de tarjetas de débito, crédito u otras ☐
Domicilios	☐		Números de cuenta ☐
Teléfonos	☐		Contraseñas o Números de Identificación Personal ☐
Direcciones de correo electrónico	☐		Identificadores de Usuarios ☐
Otro: _____	☐		Límites de crédito ☐
			Salvos ☐
			Otro: _____ ☐

3. Número de cuenta(s) afectadas. Especificar el número de cuentas que están bloqueadas o suspendidas:

Número de cuentas afectadas	Número de cuentas afectadas bloqueadas o suspendidas	Comentarios

Anexar al reporte el desgregado de los números de cuentas afectadas de manera digital conforme se indica en el siguiente cuadro:

No.	Número de cuenta afectada	Estado de la cuenta afectada (bloqueada, suspendida, activa)	Comentarios
1			
2			
3			

4. Fecha o periodo en que ocurrió el incidente de seguridad informática
5. Monto total en pesos conocido o estimado involucrado en el incidente de seguridad informática, en su caso
6. Clasificación del incidente de seguridad informática:
- a. Intrusión en equipos de cómputo ☐
 - b. Préstamos al consumo ☐
 - c. Tarjetas de crédito ☐
 - d. Tarjetas de débito ☐
 - e. Transferencia electrónica de fondos ☐
 - f. Robo de identidad ☐
 - g. Otros ☐
 - h. Corresponsales ☐
 - i. Pago Móvil ☐
 - j. Banca Móvil ☐
 - k. Otros ☐
-

7. Monto de la pérdida en pesos en su caso
8. Monto recuperado en pesos en su caso
9. ¿Se ha dado a conocer el incidente de seguridad informática a alguna autoridad local o federal?
- [Sí] [No]

En caso afirmativo:

¿A qué autoridad?

¿En qué fecha?

III. Contacto en la Institución Financiera

- 1. Nombre de la persona que está facultada para dar información a la CNBV
 - 2. Puesto desempeñado
 - 3. Teléfono
 - 4. Correo electrónico
-