CAPÍTULO 4.10.

DEL USO DE MEDIOS ELECTRÓNICOS PARA LA CONTRATACIÓN DE OPERACIONES DE SEGUROS Y DE FIANZAS

DEL USO DE MEDIOS ELECTRÓNICOS PARA LA CONTRATACIÓN DE OPERACIONES DE SEGUROS Y DE FIANZAS

Para los efectos de los artículos 214 y 348 de la LISF:

4.10.1. Las Instituciones y Sociedades Mutualistas podrán pactar la celebración de sus operaciones y la prestación de servicios a través de Operaciones Electrónicas, debiendo sujetarse a lo que establece el presente Capítulo y siempre que:

I. En las condiciones de uso de Medios Electrónicos 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 o Sociedad Mutualista respecto de la realización de Operaciones Electrónicas;

c) Los mecanismos y procedimientos para la notificación de las operaciones realizadas y servicios prestados por las Instituciones, a través de Operaciones Electrónicas;

d) Los mecanismos y procedimientos de cancelación de la contratación de Operaciones Electrónicas, 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, y

e) 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 del uso de Medios Electrónicos, los términos y condiciones para su uso, debiendo mantener dicha información disponible para su consulta en la red electrónica mundial denominada Internet, en todo momento actualizada.

Los términos y condiciones de uso de Medios Electrónicos a que se refiere la presente fracción deberán estar disponibles en la página electrónica de la Institución o Sociedad Mutualista y preverse en la documentación contractual la liga al sitio en que puede consultarse dicha información.

III. Incluyan en la documentación contractual de los productos de seguros o de fianzas, una cláusula que especifique, de forma general, la opción del cliente de hacer uso de Medios Electrónicos, en aquellos productos que tengan tal opción, y;

IV. Comuniquen a los Usuarios los riesgos inherentes a la realización de Operaciones Electrónicas, 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 Usuarios y de la Institución o Sociedad Mutualista, pudiendo efectuarse, entre otros, mediante campañas periódicas de difusión de recomendaciones de seguridad para la realización de Operaciones Electrónicas.

** Modificada DOF 08-09-2017*

4.10.2. Las Instituciones y Sociedades Mutualistas, para la realización de Operaciones Electrónicas con sus clientes, adicionalmente a lo previsto en la Disposición 4.10.1 anterior, se sujetarán a lo siguiente:

I. Deberán obtener el consentimiento expreso mediante firma autógrafa de sus clientes, previa identificación de estos, o bien, mediante firma electrónica avanzada o fiable de sus clientes, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio para estos efectos. En todo caso, podría utilizarse alguna otra forma de manifestación del consentimiento, tratándose de las Operaciones Electrónicas Móviles, las Operaciones Electrónicas por Internet, las Operaciones Electrónicas de Audio Respuesta y las Operaciones Telefónicas Voz a Voz;

II. Para la contratación de servicios y operaciones adicionales a los originalmente convenidos o modificar las condiciones del servicio o la operación originalmente contratados, las Instituciones y Sociedades Mutualistas deberán requerir un segundo Factor de Autenticación a que se refiere la Disposición 4.10.5, adicional al utilizado, en su caso, para iniciar la Sesión en los términos de la disposición 4.10.8. En estos casos, las Instituciones y Sociedades Mutualistas deberán enviar una notificación en términos de lo previsto por la Disposición 4.10.10. proporcionando algún medio para realizar cualquier aclaración.

Las Instituciones y Sociedades Mutualistas no podrán permitir a sus Usuarios la contratación de servicios de Operaciones Electrónicas a través de Terminales Punto de Venta;

III. Tratándose de las operaciones mencionadas en la fracción I anterior, la contratación podrá llevarse a cabo de conformidad con las fracciones I y II anteriores, o bien, a través de los centros de atención telefónica de las propias Instituciones y Sociedades Mutualistas, sujetándose a lo señalado en la fracción I de la Disposición 4.10.5, y

IV. 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 y Sociedades Mutualistas les hagan llegar las notificaciones a que se refiere la Disposición 4.10.10.

** Modificado DOF 29-07-2015*

** Modificada DOF 08-09-2017*

4.10.3. Las Instituciones y Sociedades Mutualistas, 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 al menos la Categoría 2 a que se refiere la Disposición 4.10.5.

El Identificador de Usuario deberá ser único para cada Usuario y permitirá a la Institución o Sociedad Mutualista identificar todas las operaciones realizadas por el propio Usuario a través de las Operaciones Electrónicas de que se trate.

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

Tratándose de Operaciones Electrónicas Móviles, el Identificador de Usuario deberá ser el número de la línea del Teléfono Móvil asociado al uso de dichas Operaciones Electrónicas, debiendo la Institución o Sociedad Mutualista, en todo caso, obtenerlo de manera automática e inequívoca del Teléfono Móvil correspondiente.

** Modificada DOF 08-09-2017*

4.10.4. Las Instituciones y Sociedades Mutualistas, 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 Operaciones Electrónicas de Audio Respuesta.

II. Garantizar 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 y Sociedades Mutualistas mantengan procedimientos para que dichas autorizaciones sean de carácter eventual y puedan ser revocados por el cliente cuando así lo solicite, y

III. Contar con procedimientos para invalidar los Factores de Autenticación para impedir la realización de Operaciones Electrónicas, cuando un Usuario o la misma Institución o Sociedad Mutualista cancele el uso de dicho servicio o cuando dicho Usuario deje de ser cliente de la Institución o Sociedad Mutualista.

4.10.5. Las Instituciones y Sociedades Mutualistas deberán utilizar Factores de Autenticación para verificar la identidad de sus Usuarios y la facultad de estos para realizar Operaciones Electrónicas. Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en el presente Capítulo, 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 y Sociedades Mutualistas a sus clientes.

Las Instituciones y Sociedades Mutualistas, 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 sólo 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:

1) El Identificador de Usuario;

2) El nombre de la Institución o Sociedad Mutualista;

3) Más de dos caracteres idénticos en forma consecutiva, o

4) Más de dos caracteres consecutivos numéricos o alfabéticos.

No resultará aplicable lo previsto en el presente inciso para el caso de las Operaciones Electrónicas Móviles, siempre que las Instituciones y Sociedades Mutualistas 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 en el caso de Operaciones Electrónicas por Internet en el que deberá ser de ocho caracteres, y

c) La composición de estos Factores de Autenticación deberá incluir caracteres alfabéticos y numéricos, cuando el Dispositivo de Acceso lo permita.

Las Instituciones y Sociedades Mutualistas 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 las Operaciones Electrónicas.

Tratándose de Contraseñas o Números de Identificación Personal (NIP) definidos o generados por las Instituciones y Sociedades Mutualistas durante la contratación de un servicio de Operaciones Electrónicas o

durante el restablecimiento de dichas contraseñas, las propias Instituciones y Sociedades Mutualistas deberán prever mecanismos y procedimientos por medio de los cuales el Usuario deba modificarlos inmediatamente después de iniciar la Sesión correspondiente. Las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas.

Las Instituciones y Sociedades Mutualistas deberán recomendar a sus Usuarios en el proceso de contratación de Operaciones Electrónicas, 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 y Sociedades Mutualistas 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, y

d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o Sociedad Mutualista, o por terceros.

Las Instituciones y Sociedades Mutualistas podrán proporcionar a sus Usuarios medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen la 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.

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

Las Instituciones y Sociedades Mutualistas que aprueben la celebración de operaciones mediante el uso de tarjetas sin circuito integrado en Terminales Punto de Venta, deberán pactar con sus Usuarios que dichas Instituciones y Sociedades Mutualistas 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.

Tratándose de Operaciones “Host to Host”, las Instituciones y Sociedades Mutualistas 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 o Sociedad Mutualista autorizó.

Las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas deberán asegurarse que las propiedades que impidan la duplicación o alteración se cumplan hasta el momento de la entrega al Usuario, y

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 y Sociedades Mutualistas 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.

4.10.6. Las Instituciones y Sociedades Mutualistas deberán establecer mecanismos y procedimientos para que sus Usuarios en Operaciones Electrónicas por Internet, puedan autenticar a las propias Instituciones y Sociedades Mutualistas 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 o Sociedad Mutualista con la cual se iniciará la Sesión. Para ello, las Instituciones y Sociedades Mutualistas podrán utilizar la información siguiente:

a) Aquella que el Usuario conozca o haya proporcionado a la Institución o Sociedad Mutualista, o bien, que haya señalado para este fin, tales como nombre sin apellidos, alias, imágenes, entre otros, y

b) Aquella que el Usuario pueda verificar mediante un dispositivo o medio proporcionado por la Institución o Sociedad Mutualista para este fin, y

II. Una vez que el Usuario verifique que se trata de la Institución o Sociedad Mutualista e inicie la Sesión, las Instituciones y Sociedades Mutualistas 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.

4.10.7. Las Instituciones y Sociedades Mutualistas podrán solicitar a sus clientes o Usuarios solo un Factor de Autenticación Categoría 1, de acuerdo con lo establecido en la Disposición 4.10.5, en los casos siguientes:
I. Para la Autenticación de sus Usuarios que pretendan realizar Operaciones Telefónicas Voz a Voz, y
II. Para el Desbloqueo de Factores de Autenticación, así como la reactivación o desactivación temporal de la realización de Operaciones Electrónicas, mediante centros de atención telefónica. Sin perjuicio de lo anterior, las Instituciones y Sociedades Mutualistas podrán prever que el procedimiento de Autenticación a través de centros de atención telefónica, se realice mediante enlaces a dispositivos de audio respuesta automática.
4.10.8. Las Instituciones y Sociedades Mutualistas deberán solicitar a sus Usuarios, para la celebración o modificación de operaciones o prestación de servicios a través de Medios Electrónicos posteriores a la contratación del uso de Medios Electrónicos, un Factor de Autenticación adicional al utilizado para iniciar la Sesión en que se pretenda realizar cada una de las operaciones y servicios que enseguida se señalan, considerando que, cuando se pretenda realizar alguna de las operaciones y servicios que requieran un Factor de Autenticación de nivel 3 o 4, deberá llevarse a cabo el proceso de autenticación en cada ocasión:
I. Contratación de un seguro de vida o muerte accidental, al menos nivel 3;
II. Contratación de un seguro de daños, de accidentes y enfermedades con excepción de la cobertura por muerte accidental o una fianza, al menos nivel 2;
III. Cancelación de un seguro o una fianza, al menos nivel 2, salvo en seguros de vida o muerte accidental que requerirán un nivel 3;
IV. Solicitud, aceptación o emisión de endosos a los contratos, al menos nivel 2;
V. Transferencias de recursos dinerarios a cuentas de terceros u otras Instituciones o Sociedades Mutualistas, incluyendo el pago de primas, así como las autorizaciones e instrucciones de domiciliación de pago de primas al menos nivel 3.
Cuando las cuentas destino, entendidas como cuentas receptoras de recursos dinerarios en operaciones monetarias, hayan sido registradas en oficinas bancarias o bien el Usuario haya solicitado que dichas cuentas se consideren como cuentas destino recurrentes, las Instituciones o Sociedades Mutualistas podrán permitir a los Usuarios realizar dichas operaciones utilizando un solo Factor de Autenticación de al menos de nivel 2,;
VI. Modificación de designación de beneficiarios, al menos nivel 3;
VII. Alta y modificación del medio de notificación al Usuario, debiendo enviarse tanto al medio de notificación anterior como al nuevo, al menos nivel 2;
VIII. Consultas de estados de cuenta u otras consultas que permitan conocer información relacionada con el Usuario o los contratos que tenga celebrados con la Institución o Sociedad Mutualista, que pueda ser utilizada como información de Autenticación, al menos nivel 3;
IX. Contratación de otro servicio de Operaciones Electrónicas o modificación de las condiciones para el uso del servicio previamente contratado, al menos nivel 2;
X. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP), así como para la reactivación del uso de los servicios respecto de otras Operaciones Electrónicas que tenga contratados, al menos nivel 1;
XI. Modificación de Contraseñas o Números de Identificación Personal (NIP) por parte del Usuario, al menos nivel 2, y
XII. Solicitud de pago de rescate o aplicación de valores garantizados, al menos nivel 3.
* *Modificado DOF 29-07-2015*
* *Modificada DOF 08-09-2017*
Las Instituciones y Sociedades Mutualistas 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 la Disposición 4.10.5, para que el Usuario tenga acceso, el cual deberá ser distinto al utilizado para acceder a la realización de Operaciones Electrónicas por Internet. Las Instituciones y Sociedades Mutualistas deberán establecer medidas que protejan la confidencialidad de los datos transmitidos y del Factor de Autenticación utilizado.
4.10.9. Las Instituciones y Sociedades Mutualistas deberán establecer mecanismos y procedimientos para que la realización de Operaciones Electrónicas genere los comprobantes correspondientes respecto de las operaciones y servicios realizados por sus Usuarios.
4.10.10. Las Instituciones y Sociedades Mutualistas 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 Operaciones Electrónicas:
I. Contratación o cancelación de un seguro o una fianza;
II. Solicitud, aceptación o emisión de endosos a los contratos;
III. Instrucciones para transferencias de recursos dinerarios a cuentas de la Institución o Sociedad Mutualista por concepto de pago de primas;
IV. Modificación de designación de beneficiarios;
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 Operaciones Electrónicas o modificación de las condiciones para el uso del servicio previamente contratado;
VII. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP), así como para la reactivación del uso de los servicios de Operaciones Electrónicas;
VIII. Modificación de Contraseñas o Números de Identificación Personal (NIP) por parte del Usuario, y
IX. Solicitud de pago de rescate o aplicación de valores garantizados
Las Instituciones y Sociedades Mutualistas deberán asegurarse que la información transmitida para notificar al Usuario sobre los eventos a que se refiere la presente Disposición, no contenga domicilios e información completa respecto de los contratos celebrados con la Institución o Sociedad Mutualista.
En ningún caso las Instituciones y Sociedades Mutualistas permitirán la modificación del medio de notificación a través de Terminales Punto de Venta. Las Instituciones y Sociedades Mutualistas deberán permitir a sus Usuarios modificar el medio de notificación de los servicios de Operaciones Electrónicas ofrecidos en Terminales Punto de Venta mediante un centro de atención telefónica, utilizando un Factor de Autenticación Categoría 1 a que se refiere la Disposición 4.10.5.
Se exceptúa de lo señalado en la presente Disposición a las Operaciones “Host to Host”.
4.10.11. Las Instituciones y Sociedades Mutualistas deberán proveer lo necesario para que una vez autenticado el Usuario en la realización de la Operación Electrónica de que se trate, la Sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las Instituciones y Sociedades Mutualistas 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 Terminales Punto de Venta, el período de inactividad no podrá exceder de un minuto.
Para Operaciones “Host to Host”, las Instituciones y Sociedades Mutualistas podrán definir el período de inactividad, con base en los riesgos asociados al servicio que las propias Instituciones y Sociedades Mutualistas determinen, y
b) Cuando en el curso de una Sesión de Operaciones Electrónicas por Internet, la Institución o Sociedad Mutualista 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 la Operación Electrónica de que se trate e informar al Usuario, cuando el Identificador de Usuario esté siendo utilizado en otra Sesión, y
III. En el evento de que las Instituciones y Sociedades Mutualistas ofrezcan servicios de terceros mediante enlaces en la realización de Operaciones Electrónicas, deberán comunicar a sus Usuarios que al momento de ingresar a dichos servicios, se cerrará automáticamente la Sesión abierta con la Institución o Sociedad Mutualista de que se trate y se ingresará a otra cuya seguridad no depende ni es responsabilidad de dicha Institución o Sociedad Mutualista.
4.10.12. Las Instituciones y Sociedades Mutualistas deberán establecer procesos y mecanismos automáticos para bloquear el uso de Contraseñas y otros Factores de Autenticación para la realización de Operaciones Electrónicas, cuando menos para los casos siguientes:
I. Cuando se intente ingresar al servicio de Operaciones Electrónicas 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 un bloqueo automático, y
II. Cuando el Usuario se abstenga de realizar operaciones a través del servicio de Operaciones Electrónicas de que se trate, por un período que determine cada Institución o Sociedad Mutualista 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 período podrá ser mayor a un año. Lo anterior, no será aplicable a la realización de Operaciones Electrónicas a través de Terminales Punto de Venta.
Las Instituciones y Sociedades Mutualistas 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 la Disposición 4.10.5, en términos de lo previsto por la fracción II de la Disposición 4.10.7, 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 o Sociedad Mutualista durante el proceso de contratación del servicio de Operaciones Electrónicas, 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 y Sociedades Mutualistas deberán permitir al Usuario el restablecimiento de Contraseñas y Números de Identificación Personal (NIP) utilizando el procedimiento de contratación al servicio descrito en la Disposición 4.10.2.

4.10.13. Para el manejo de Contraseñas y otros Factores de Autenticación, las Instituciones y Sociedades Mutualistas 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, y
III. Tendrán prohibido solicitar a sus Usuarios, a través de sus funcionarios, empleados, representantes, Agentes o apoderados, la información parcial o completa, de los Factores de Autenticación de la Categoría 2 o de la Categoría 3 a que se refiere la Disposición 4.10.5.
Se exceptúa de lo previsto en esta fracción, a las Operaciones Telefónicas Voz a Voz, siempre y cuando el Usuario haya iniciado la llamada, se requiera información parcial del Factor de Autenticación de la Categoría 2 o de la Categoría 3 a que se refiere la Disposición 4.10.5, y éste sea utilizado exclusivamente para la realización de Operaciones Electrónicas.
4.10.14. Las Instituciones y Sociedades Mutualistas que pongan al alcance de sus Usuarios equipos electrónicos o de telecomunicaciones, en sus instalaciones o en áreas de acceso al público, para la realización de Operaciones Electrónicas, 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 y Sociedades Mutualistas, y
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 o Sociedad Mutualista, 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, seguimiento y análisis de comportamientos fuera de los parámetros establecidos por la Institución o Sociedad Mutualista.
Para tal fin, la Institución o Sociedad Mutualista deberá presentar al comité de auditoría, cada vez que sesione, así como al Área de Administración de Riesgos, un informe de los resultados de la ejecución de dichos procedimientos.
4.10.15. Las Instituciones y Sociedades Mutualistas 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 éstas, 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, y
III. Impedir que los operadores telefónicos cuenten con mecanismos que les permitan registrar la información proporcionada por los Usuarios en medios diferentes a los dispuestos por la propia Institución o Sociedad Mutualista para efectos de Autenticación. Para ello, las Instituciones y Sociedades Mutualistas 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.
4.10.16. Las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas 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 y Sociedades Mutualistas, a fin de proteger la información 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 de la Disposición 4.10.12.
Para efectos de lo anterior, las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas 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 Operaciones Telefónicas Voz a Voz y Operaciones Electrónicas de Audio Respuesta, podrán implementar controles compensatorios al Cifrado en la transmisión de información a fin de protegerla;
II. Las Instituciones y Sociedades Mutualistas deberán Cifrar o truncar la información de 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 y Sociedades Mutualistas 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.
La información de los Factores de Autenticación Categoría 2 a que se refiere la Disposición 4.10.5, 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 ésta sea enviada utilizando mecanismos de seguridad, previa solicitud del Usuario y se hayan llevado a cabo los procesos de Autenticación correspondientes, y
IV. Las Instituciones y Sociedades Mutualistas 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.
4.10.17. Las Instituciones y Sociedades Mutualistas 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, aun cuando dichas bases de datos y archivos residan en medios de almacenamiento de
I. El acceso a las bases de datos y archivos estará permitido exclusivamente a las personas expresamente autorizadas por la Institución o Sociedad Mutualista en función de las actividades que realizan. Al otorgarse dichos accesos, deberá dejarse constancia de tal circunstancia y señalar los propósitos y el período 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, y

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 la presente Disposición, sin contar con la autorización correspondiente, o el uso indebido de dicha información, será sancionada en términos de lo previsto en la LISF, inclusive tratándose de terceros contratados al amparo de lo establecido en los artículos 268 y 269 de dicho ordenamiento legal.
4.10.18. En caso de que Información Sensible del Usuario sea modificada, extraída, extraviada, eliminada o las Instituciones y Sociedades Mutualistas supongan o sospechen de algún incidente que involucre accesos no autorizados a dicha información, deberán 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, dentro de 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, modificada, eliminada o comprometida, debiendo informarles las medidas que deberán tomar.
** Modificada DOF 10-09-2018*
4.10.19. Las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas podrán:
I. Solicitar a sus Usuarios la información que estimen necesaria para definir el uso habitual que estos hagan de los servicios relacionados con las Operaciones Electrónicas, y
II. Aplicar, bajo su responsabilidad, medidas de prevención, tales como la suspensión de la utilización del servicio de Operaciones Electrónicas 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 y Sociedades Mutualistas hayan pactado con sus Usuarios en el contrato respectivo.

4.10.20. Las Instituciones y Sociedades Mutualistas deberán mantener en bases de datos las incidencias, fallas o vulnerabilidades detectadas en las Operaciones Electrónicas, así como todas las operaciones efectuadas a través de dicho servicio 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, Operación Electrónica afectada y clientes afectados, y

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, Operación Electrónica de que se trate, causa o motivo, importe, estado de la reclamación, resolución y fecha de resolución.

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

4.10.21. Las Instituciones y Sociedades Mutualistas deberán generar registros, bitácoras, huellas de auditoría de las operaciones y servicios realizados a través de Medios Electrónicos y, en el caso de Operaciones Telefónicas Voz a Voz, adicionalmente grabaciones de los procesos de contratación, activación, desactivación, modificación de condiciones y suspensión del uso del servicio de Operación Electrónica, debiendo observar lo siguiente:

** Modificado DOF 29-07-2015*

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 o Sociedad Mutualista, incluyendo las consultas efectuadas;

b) La fecha y hora, 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, y

d) En el caso de Operaciones Electrónicas por Internet, deberán registrarse las direcciones de los protocolos de Internet o similares, y para las Operaciones Electrónicas 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 relativas a las Operaciones Telefónicas Voz a Voz, deberán ser almacenadas de forma segura por un período 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 y Sociedades Mutualistas en forma periódica y en caso de detectarse algún evento inusual, deberá reportarse al comité de auditoría y al encargado del Área de Administración de Riesgos, conforme se establece en el último párrafo de la Disposición 4.10.25, y

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 Electrónicas sea consistente.

La información a que se refiere la presente Disposición deberá ser proporcionada a los Usuarios que así lo requieran expresamente a la Institución o Sociedad Mutualista mediante sus canales de atención al cliente, en un plazo que no exceda de diez días hábiles, siempre que se trate de operaciones realizadas 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.

4.10.22. Las Instituciones y Sociedades Mutualistas 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 y Sociedades Mutualistas impedir el uso indebido de los mismos. Asimismo, deberán establecer políticas que definan las responsabilidades tanto del Usuario como de la Institución o Sociedad Mutualista, respecto de las operaciones que hayan sido efectuadas previas al reporte.

Las Instituciones y Sociedades Mutualistas 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 o Sociedad Mutualista. 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 y Sociedades Mutualistas deberán establecer procedimientos y mecanismos para la atención y seguimiento de las operaciones realizadas a través de Operaciones Electrónicas que no sean reconocidas por sus Usuarios.

4.10.23. Las Instituciones y Sociedades Mutualistas 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 las Operaciones Electrónicas, 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 o Sociedad Mutualista.

Las Instituciones y Sociedades Mutualistas deberán revisar adicionalmente, en los términos de la presente Disposición, los equipos que, en su caso, hayan dispuesto para que sus Usuarios realicen operaciones a través de Medios Electrónicos.

Asimismo, las Instituciones y Sociedades Mutualistas deberán mantener en su infraestructura de cómputo y telecomunicaciones para la realización de Operaciones Electrónicas, 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 y Sociedades Mutualistas deberán mantener controles que eviten la divulgación no autorizada de la información de configuración de dicha infraestructura.

4.10.24. Las Instituciones y Sociedades Mutualistas 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 en la realización de Operaciones Electrónicas, así como a eventos de seguridad relacionados con el uso de Medios Electrónicos.

4.10.25. Las Instituciones y Sociedades Mutualistas deberán procurar la operación continua de la infraestructura de cómputo y de telecomunicaciones, así como dar pronta solución, para restaurar el servicio relativo a las Operaciones Electrónicas, en caso de presentarse algún incidente.

Las incidencias deberán informarse al comité de auditoría en la sesión inmediata siguiente a la verificación del evento de que se trate, así como al encargado del Área de Administración de Riesgos, a efecto de que se adopten las medidas conducentes para prevenir o evitar que se presenten nuevamente.

4.10.26. El director general deberá garantizar que la Institución o Sociedad Mutualista 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 la realización de Operaciones Electrónicas, que puedan afectar a sus Usuarios o a la operación de la Institución o Sociedad Mutualista. Las referidas medidas y procedimientos, deberán ser evaluados por el Área de Auditoría Interna de las Instituciones y Sociedades Mutualistas 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 o Sociedad Mutualista, puedan verse afectados. 4.10.27. Las Instituciones y Sociedades Mutualistas deberán implementar las acciones correctivas que la Comisión les requiera, como resultado de la identificación de riesgos asociados con la realización de Operaciones Electrónicas.

4.10.28. La evidencia de la realización de Operaciones Electrónicas por parte de las Instituciones y Sociedades Mutualistas, deberá estar documentada y disponible en caso de que la Comisión la solicite para fines de inspección y vigilancia.

4.10.29. En la realización de las operaciones a que se refiere este Capítulo, las Instituciones y Sociedades Mutualistas deberán dar cumplimiento a las presentes Disposiciones, a las Disposiciones de Carácter General a que se refiere el artículo 492 de la LISF, y demás disposiciones legales, reglamentarias y administrativas aplicables.

* *Adicionada DOF 08-09-2017* siguiente: