Tegucigalpa, MDC
29 de mayo de 2023

INSTITUCIONES SUPERVISADAS

CIRCULAR CNBS No.008/2023

La infrascrita Secretaria General de la Comisión Nacional de Bancos y Seguros CERTIFICA la parte conducente del Acta de la Sesión No.1728 celebrada en Tegucigalpa, Municipio del Distrito Central el veintiséis de mayo de dos mil veintitrés, con la asistencia de los Comisionados MARCIO GIOVANNY SIERRA DISCUA, Presidente; ALBA LUZ VALLADARES OCONNOR, Comisionada Propietaria; ESDRAS JOSIEL SÁNCHEZ BARAHONA, Comisionado Propietario; ANA GABRIELA AGUILAR PINEDA, Secretaria General; que dice:

"… **5. Asuntos de la Gerencia de Regulación, Investigación y Desarrollo:** … literal **a)** … **RESOLUCIÓN GRD No.365/26-05-2023.-** La Comisión Nacional de Bancos y Seguros,

CONSIDERANDO (1): Que el Artículo 1 de la Ley de la Comisión Nacional de Bancos y Seguros establece que corresponde a este Ente Supervisor vigilar que las Instituciones del Sistema Financiero y demás entidades supervisadas, desarrollen sus actividades en concordancia con las leyes de la República y el interés público, velando porque los marcos regulatorios promuevan la libre competencia, la equidad de participación, la eficiencia de las Instituciones Supervisadas y la protección de los derechos de los usuarios financieros, promoviendo el acceso al financiamiento y velando en todo momento por la estabilidad del sistema financiero supervisado.

CONSIDERANDO (2): Que el Artículo 13, numerales 1), 2) y 11) de la Ley de la Comisión Nacional de Bancos y Seguros establece que corresponde a este Ente Supervisor, dictar las normas que se requieran para la revisión, verificación, control, vigilancia y fiscalización de las Instituciones Supervisadas, lo mismo que las normas prudenciales que deberán cumplir, para lo cual se basará en la legislación vigente y en los acuerdos y prácticas internacionales. Asimismo, es atribución de la Comisión, dictar las normas generales para que las Instituciones Supervisadas proporcionen al público información suficiente, veraz y oportuna sobre su situación jurídica, económica y financiera.

CONSIDERANDO (3): Que los estándares y mejores prácticas internacionales relacionados con las tecnologías de información (TI), están en constante actualización brindando mecanismos de control robustos para la gestión de las TI y el riesgo operativo.

CONSIDERANDO (4): Que durante los últimos años, con el aumento de la oferta de productos y servicios por medio de canales digitales, se ha visto incrementado el riesgo de fraudes cibernéticos; en los cuales ciberdelincuentes obtienen información de acceso de los usuarios

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

financieros y sustraen fondos de sus cuentas bancarias por medio de transferencias a cuentas de terceros. Aún y cuando las Instituciones Supervisadas han implementado controles para fortalecer las plataformas de sus canales digitales, se requiere de mecanismos más efectivos que permitan una acción oportuna y coordinada del sector, coadyuvando a fortalecer la confianza de los clientes y usuarios en los productos y servicios digitales que las Instituciones ofrecen.

CONSIDERANDO (5): Que la Comisión Nacional de Bancos y Seguros, mediante Resolución GRD No.247/23-03-2023, aprobó los "LINEAMIENTOS MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO", los que tienen por objetivo establecer controles mínimos que las Instituciones Supervisadas por la Comisión deben estar aplicando, para prevenir y mitigar la ocurrencia de fraudes cibernéticos en contra de los usuarios financieros; así como crear una mayor conciencia y educación financiera en los usuarios para la prevención de estos eventos.

CONSIDERANDO (6): Que la Asociación Hondureña de Instituciones Bancarias (AHIBA), mediante correo del 27 de abril de 2023, remitió observaciones sobre los Lineamientos, por lo que la Gerencia de Regulación, Investigación y Desarrollo, mediante Dictamen Técnico GRDRA-DT-43/2023, concluye que con base al análisis técnico realizado en conjunto con la Superintendencia de Bancos y Otras Instituciones Financieras y la Gerencia de Riesgos, son del parecer que es procedente recomendar a la Comisión Nacional de Bancos y Seguros, se reformen los "LINEAMIENTOS MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO", en aspectos relacionados, entre otros, con el alcance, las notificaciones, el doble factor de autenticación para ejecución de transacciones, el factor de demora en habilitación de cambios, el plazo para la presentación de reportes de eventos y la notificación y reclamación de transacciones electrónicas no autorizadas. Lo anterior, con la finalidad de una mejor aplicabilidad de las disposiciones contenidas en la Resolución GRD No.247/23-03-2023.

POR TANTO: Con fundamento en lo establecido en los Artículos 1, 6, 8, 13, numerales 1), 2) y 11), y 39 de la Ley de la Comisión Nacional de Bancos y Seguros; Resolución GRD No.247/23-03-2023 contentiva de los "LINEAMIENTOS MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO", emitidos por la Comisión Nacional de Bancos y Seguros;

RESUELVE:

1. Reformar los "LINEAMIENTOS MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO", cuyo contenido íntegramente se leerá así:

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

LINEAMIENTOS MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS PARA PREVENIR Y MITIGAR LA OCURRENCIA DE FRAUDES Y ESTAFAS CIBERNÉTICAS EN CONTRA DEL USUARIO FINANCIERO

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- OBJETO
Los presentes Lineamientos tienen por objeto establecer controles mínimos que las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros (en adelante la Comisión) deben estar aplicando, para prevenir y mitigar la ocurrencia de fraudes cibernéticos en contra de los usuarios financieros; así como crear una mayor conciencia y educación financiera en los usuarios para la prevención de estos eventos.

ARTÍCULO 2.- ALCANCE
Estos Lineamientos son aplicables a las Instituciones Supervisadas por la Comisión, para las transacciones y gestiones realizadas a través de los canales digitales puestos a disposición de los usuarios financieros.

ARTÍCULO 3.- DEFINICIONES
Para los efectos de los presentes Lineamientos, se entenderá por:

1) **ACH (Cámara de Compensación Automatizada, por sus siglas en inglés):** Es un sistema electrónico de procesamiento de pagos, que se utiliza para transferir fondos electrónicamente entre cuentas bancarias.

2) **Canales Digitales:** Canales dispuestos por las Instituciones Supervisadas a los usuarios financieros para la realización de gestiones y transacciones utilizando medios tecnológicos. Pueden ser páginas web, aplicaciones móviles, integraciones con redes sociales, entre otras.

3) **Ciberdelincuente:** Un ciberdelincuente es una persona que utiliza tecnología, como computadoras, dispositivos móviles y redes de Internet entre otros, para cometer delitos y actividades ilícitas.

4) **Ciberseguridad:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas de información a través del ciberespacio.

5) **Código OTP (One Time Password):** Es una contraseña de un único uso (sus siglas en inglés: One-Time Password), también conocida como password o contraseña dinámica. Se utiliza como segundo factor de autenticación, además del nombre de

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

usuario y la contraseña comúnmente utilizados. Solo es válida una vez, de forma que, aunque un atacante consiguiera hacerse con ella no podría reutilizarla.

6) **Comisión o CNBS:** Comisión Nacional de Bancos y Seguros.

7) **Contraseña:** Una contraseña es una combinación de caracteres alfanuméricos (letras, números y símbolos) utilizados para autenticar o verificar la identidad de un usuario en un sistema o servicio en línea.

8) **Contraseñas Robustas:** Son seguras y complejas, y se utilizan para proteger cuentas de usuario en línea contra accesos no autorizados. Una contraseña robusta generalmente es una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, y es lo suficientemente larga para ser difícil de adivinar mediante técnicas de fuerza bruta o diccionario.

9) **Dirección IP (Protocolo de Internet por sus siglas en inglés):** Es un identificador numérico único que se asigna a cada dispositivo conectado a una red que utiliza el protocolo de Internet. Es una serie de números que permite que los dispositivos se comuniquen entre sí a través de la red.

10) **Doble Factor de Autenticación (2FA, por sus siglas en inglés):** Es un método de seguridad que se utiliza para proteger las cuentas de usuario en línea. Consiste en solicitar dos formas distintas de autenticación para verificar la identidad de un usuario antes de concederle acceso a una cuenta o sistema.

11) **Instituciones Supervisadas:** Son aquellas instituciones que se encuentran bajo la supervisión, vigilancia y control de la Comisión.

12) **Fraude Cibernético:** Actividad encaminada a obtener de forma engañosa, datos sensibles como información bancaria, credenciales de acceso, información personal para cometer delitos, provocando pérdidas financieras a las víctimas.

13) **Funciones de Vigilancia:** Son las encargadas de brindar vigilancia integral e independiente a nivel institucional, así como el control y monitoreo, de la gestión operativa, como ser: Auditoría Interna, Gestión de Riesgo, Análisis Actuarial, Análisis Financiero, Cumplimiento Regulatorio, Alta Gerencia, Consejo de Administración, Junta Directiva o su equivalente, entre otras según la naturaleza, tamaño, alcance, complejidad y perfil de riesgo de la Institución Supervisada.

14) **Geolocalización:** Es la tecnología que permite identificar la ubicación geográfica de un dispositivo electrónico, como un teléfono móvil, una tablet o un ordenador, utilizando la información proporcionada por diferentes fuentes, como GPS, redes móviles, Wi-Fi y direcciones IP.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

15) **GPS (Sistema de Posicionamiento Global, por sus siglas en inglés):** Es un sistema de navegación por satélite que permite a los usuarios determinar su ubicación y velocidad relativa en cualquier parte del mundo.

16) **LBTR (Sistema de Liquidación Bruta en Tiempo Real por sus siglas en inglés):** Es un sistema de liquidación continua de transferencias de fondos y liquidación de valores, de forma individual (una a una), en tiempo real y sin neteo.

17) **Mecanismos de Autogestión:** Los mecanismos de autogestión en canales digitales son herramientas y funcionalidades que permiten a los usuarios realizar acciones y gestionar su información sin necesidad de la intervención de un agente o representante de la Institución Supervisada.

18) **Órgano de Administración:** Se refiere a la Junta Directiva, Consejo de Administración Asamblea de Participantes o Aportantes, o su órgano equivalente.

19) **Perfil de Riesgo:** Evaluación de las exposiciones de riesgo de la Institución Supervisada, después de tomar en cuenta los mitigantes.

20) **Programa de Educación Financiera (PEF):** Son las acciones que mediante procesos educativos integrados por diferentes módulos de capacitación, información, asesoría o consulta, tienen como finalidad formar habilidades y competencias, y facilitar el proceso de aprendizaje de los usuarios financieros, a fin de generar cambios positivos de conducta de las poblaciones objetivo a los cuáles se dirige, en torno al uso de productos y servicios financieros, así como a las decisiones que tome en relación al uso de sus recursos financieros.

21) **Protección de Marca:** En el contexto de la ciberseguridad, la protección de marca se refiere a las medidas y estrategias que se utilizan para proteger y defender la identidad digital de una Institución Supervisada, incluyendo su nombre, logotipo, sitio web y presencia en las redes sociales entre otros.

22) **Sim Swap (también conocido como cambio de SIM):** Es una técnica de fraude en la que un ciberdelincuente se apodera del número de teléfono de la víctima mediante la activación de una nueva tarjeta SIM en un dispositivo móvil bajo su control.

23) **Sistema Operativo:** Es un conjunto de programas y utilidades que se encargan de administrar los recursos de hardware y software de una computadora, permitiendo que otros programas se ejecuten de manera eficiente y proporcionando una interfaz para que los usuarios puedan interactuar con la computadora.

24) **Transacciones Electrónicas No Autorizadas:** Es una transacción electrónica realizada desde la cuenta de un usuario financiero iniciada por un tercero sin su consentimiento y de la cual el usuario financiero no recibe ningún beneficio.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

25) **Token:** Es un código único que se utiliza para autenticar o verificar la identidad de un usuario en un sistema o servicio en línea. El token se genera a través de un algoritmo criptográfico y se puede utilizar en lugar de una contraseña para permitir el acceso a un sistema o servicio. Los tokens pueden ser físicos o virtuales. Los tokens físicos son dispositivos que se pueden llevar consigo, como tarjetas inteligentes o llaves de seguridad USB, que generan un código único para su uso en la autenticación. Los tokens virtuales, por otro lado, son generados por una aplicación de software que se ejecuta en un dispositivo móvil u otro tipo de dispositivos.

26) **URL (Localizador de Recursos Uniforme por sus siglas en inglés):** Es una cadena de caracteres que se utiliza para identificar la ubicación de un recurso en internet, como una página web, una imagen, un archivo de audio o cualquier otro tipo de archivo disponible en la red.

27) **Usuario Financiero:** Persona natural o jurídica que recibe Educación Financiera, y que utiliza un servicio o producto brindado por una Institución Supervisada.

28) **VPN (Red Privada Virtual, por sus siglas en inglés):** Es una red que permite a los usuarios conectarse a Internet de forma segura y privada. La VPN utiliza técnicas de encriptación para asegurar que la conexión a Internet sea privada y segura.

CAPÍTULO II
ESTRATEGIA DE MITIGACIÓN Y EDUCACIÓN FINANCIERA

ARTÍCULO 4.- ESTRATEGIA DE MITIGACIÓN DE FRAUDES CIBERNÉTICOS
Como parte del Marco de Gobierno de Riesgos de las Instituciones Supervisadas, deben contar con una estrategia para minimizar los riesgos de fraude cibernético por medio de los canales digitales que ponen a disposición de sus usuarios financieros, misma que debe estar enmarcada en una evaluación de riesgos, realizada de manera conjunta con las unidades de negocio y las funciones de vigilancia correspondientes, alineados con las políticas de seguridad de la Institución; con el objetivo de determinar si los controles implementados son lo suficientemente robustos para mitigar las tipologías de fraude que afectan a los usuarios financieros. Dicha estrategia debe estar aprobada por el Órgano de Administración y ser objeto de revisiones y actualizaciones de forma periódica, en función de la identificación de nuevos riesgos y nuevas tipologías de fraude que puedan afectar a las Instituciones y a los usuarios financieros. La evaluación de riesgos debe actualizarse periódicamente o cuando las Instituciones Supervisadas dispongan de nuevos canales digitales para los usuarios financieros.

ARTÍCULO 5.- EDUCACIÓN AL USUARIO FINANCIERO
El Programa de Educación Financiera debe incluir aspectos relacionados con la concientización de los usuarios financieros para prevenir que sean objeto de fraudes y estafas cibernéticas; para lo cual, realizará campañas masivas y permanentes de

concientización mediante canales de comunicación efectivos, conteniendo al menos los siguientes elementos:

1) Riesgos asociados con el uso de sus productos y servicios por medio de canales digitales, tipologías existentes de fraudes, así como los derechos y obligaciones de los usuarios sobre este particular.

2) Prácticas de ingeniería social que utilizan los estafadores para obtener información confidencial: Llamadas telefónicas suplantando al personal del banco, mensajes a aplicaciones de comunicación, correos electrónicos invitando a hacer clic en URLs falsos, SMS, entre otros.

3) Buenas prácticas de protección de sus credenciales de usuario.

4) Concientizar a sus clientes que la Institución nunca solicitará su usuario, clave u OTP en ninguna circunstancia, por lo que el cliente está en autorización de nunca entregarlas.

5) Protección del correo electrónico personal registrado para hacer uso de los canales digitales, con doble factor de autenticación y el uso de contraseñas robustas, ya que este es el principal canal para recuperar sus credenciales, y por tanto, el objetivo principal de los ciberdelincuentes.

6) Detección de un ataque de secuestro de número telefónico (SIM Swap), de manera que logren identificar la suplantación de su tarjeta SIM y comunicarse con servicio al cliente de la Institución para el congelamiento de sus cuentas.

7) Promover el uso de la aplicación oficial. Los clientes deberán estar enterados que la aplicación oficial se deberá descargar solamente desde las tiendas oficiales de aplicaciones móviles y no desde fuentes no autorizadas.

8) Orientar a los clientes para que sean capaces de reconocer una URL oficial contra una fraudulenta.

Sin perjuicio de las campañas de concientización que a nivel gremial o general puedan desarrollar las diferentes asociaciones de las que forman parte las Instituciones Supervisadas, cada Institución debe estar desarrollando sus propias campañas de concientización, considerando los aspectos particulares de sus diferentes canales digitales, ya sean estos propios o tercerizados.

ARTÍCULO 6.- IDENTIFICACIÓN DE NUEVAS TIPOLOGÍAS DE FRAUDES

Las Instituciones Supervisadas deben contar con mecanismos para identificar nuevas tipologías de fraudes y estafas cibernéticas que estén ocurriendo en el país y en la región, con el objetivo de actualizar el análisis de riesgos en canales digitales e incluir en las campañas de concientización, alertas que puedan prevenir al usuario financiero de ser

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

objeto de engaños. Asimismo, deberán implementar los controles correspondientes para mitigar la ocurrencia de las nuevas tipologías que se identifiquen.

CAPÍTULO III
CONTROLES MÍNIMOS CON LOS QUE DEBEN CONTAR LAS INSTITUCIONES SUPERVISADAS

ARTÍCULO 7.- SOBRE LOS CONTROLES
Las Instituciones Supervisadas tienen la responsabilidad de contar con controles preventivos, detectivos y correctivos para proteger las cuentas de los usuarios financieros ante la ocurrencia de fraudes y estafas cibernéticas. Dichos controles deben permitir identificar y responder ante transacciones sospechosas o atípicas conforme al perfil de riesgo y comportamiento histórico transaccional del usuario financiero, incluyendo sin limitarse a: montos transaccionales, dispositivos utilizados, navegadores, localización y dirección IP. Las Instituciones deben requerir una confirmación al usuario financiero, cuando se identifique la ocurrencia de estas transacciones; la cual no debe ser efectiva hasta que la Institución confirme la autenticidad de esta.

ARTÍCULO 8.- MECANISMOS DE AUTOGESTIÓN
Las Instituciones Supervisadas deben contar con análisis de riesgo a sus mecanismos de autogestión en canales digitales, para creación de nuevos usuarios, cambio de token, cambio de claves, bloqueo de cuentas, recuperación de credenciales, entre otros; que incluya como mínimo:

1) Servicio analizado para el canal digital.

2) Riesgos inherentes asociados por servicio.

3) Controles implementados por riesgo.

4) Análisis de riesgo residual.

5) Monitoreo de efectividad de los controles definidos.

6) Plan de acción a implementar para la mitigación de riesgos.

7) Acuerdos formales de aceptaciones de riesgo.

ARTÍCULO 9.- NOTIFICACIÓN DE TRANSACCIONES
Las Instituciones Supervisadas deben notificar en tiempo real a los usuarios cuando se realice cualquier tipo de transacción por medio de los canales digitales. De igual manera, debe notificarse al usuario cuando se realicen eventos como inicios de sesión, cambios de contraseña, cambios de token, actualización de número de teléfono o correo electrónico, entre otros. Estas notificaciones deben realizarse mediante correo electrónico y mensaje

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

de texto, adicional a cualquier otro medio que la Institución considere pertinente y que haya sido autorizado por el cliente.

Las notificaciones podrán ser realizadas por un solo medio (correo electrónico o mensaje de texto), en los casos siguientes:

a) Transferencias realizadas a cuentas registradas como favoritos, pre registros o calendarización de pagos; y,

b) Transacciones menores a Cinco Mil Lempiras Exactos (L5,000.00), que no excedan un acumulado diario de Diez Mil Lempiras Exactos (L10,000.00).

En el caso de las notificaciones de inicio de sesión, estas se realizarán únicamente cuando se identifique que la misma sea atípica, para ello las Instituciones Supervisadas deben contar con mecanismos que permitan la identificación de este tipo de operación.

En el caso de transacciones realizadas entre cuentas propias del usuario dentro de la misma Institución Supervisada, no requerirá mensaje de notificación.

ARTÍCULO 10.- DOBLE FACTOR DE AUTENTICACIÓN PARA EJECUCIÓN DE TRANSACCIONES

La Institución debe contar con mecanismos de doble factor de autenticación obligatorio, para la ejecución de todas las transacciones monetarias y no monetarias que se realicen por medio de los canales digitales. Lo anterior, no es aplicable para las transacciones a cuentas registradas como favoritas, pre registros, calendarizaciones de transferencias o pagos, o transacciones entre cuentas propias dentro de la misma Institución Supervisada, debiendo aplicar el doble factor de autenticación únicamente al momento de su registro.

ARTÍCULO 11.- ENVÍO DE ENLACES EN COMUNICACIONES

Las Instituciones Supervisadas no deben enviar enlaces o links en las comunicaciones que se realicen por medio de correos electrónicos o mensajes de texto a los usuarios financieros.

ARTÍCULO 12.- BLOQUEO TEMPORAL DE USUARIOS DE CANALES DIGITALES

Las Instituciones Supervisadas deben tener habilitado en sus canales digitales y en sus centros de atención telefónica, mecanismos que le permitan al usuario financiero realizar bloqueos temporales de sus productos financieros de forma expedita, cuando estos identifiquen que sus credenciales de acceso puedan estar comprometidas para accesos no autorizados.

ARTÍCULO 13.- SISTEMAS DE PREVENCIÓN DE FRAUDES CIBERNÉTICOS

Las Instituciones Supervisadas en función de la exposición que presenten sus operaciones por medio de canales digitales, deben contar con sistemas de prevención de fraude en tiempo real, estableciendo parámetros para aprobar o denegar transacciones, y solicitar

información adicional en caso de ser necesario, para garantizar la autenticidad de las transacciones. Para su correcto funcionamiento, este sistema debe basarse en un análisis de riesgos que contemple, como mínimo, los siguientes elementos:

1) **Análisis del perfil transaccional:** El sistema debe analizar el perfil transaccional del usuario, considerando factores como sus patrones de navegación en los canales digitales disponibles, patrones de transacciones, preferencias en cuanto a días o fechas de operación, destinatarios frecuentes, monto y tipo de transacciones realizadas (transferencias, pagos, ACH, retiros, entre otros), así como otros aspectos relevantes para definir su comportamiento y detectar posibles actividades sospechosas.

2) **Análisis de dispositivos:** El sistema debe analizar las preferencias de uso de dispositivos del cliente para acceder a los canales digitales, considerando elementos como el historial de dispositivos utilizados, sistema operativo y horarios habituales de uso. Además, deberá verificar las formas de autenticación preferidas por el usuario, detectar ingresos a la aplicación o al token desde dispositivos diferentes, entre otros.

3) **Análisis de geolocalización:** El sistema debe analizar la geolocalización del cliente con relación a su comportamiento, considerando aspectos como país de ubicación del dispositivo, la frecuencia de cambio de ubicaciones, las direcciones IP utilizadas en las transacciones y su posible inclusión en listas negras, y el uso de herramientas VPN para enmascarar las direcciones IP.

ARTÍCULO 14.- LISTAS DE ATENCIÓN ESPECIAL

Las Instituciones Supervisadas deben mantener registros especiales, en los cuales se incluyan los clientes cuyas cuentas, se haya identificado que fueron utilizados en fraudes y estafas cibernéticas, para adoptar las medidas correspondientes de monitoreo y debida diligencia, conforme a su perfil de riesgo. Asimismo, pueden crear listas de usuarios financieros que han sido afectados con transacciones electrónicas no autorizadas, para su seguimiento y monitoreo.

Las Instituciones pueden establecer mecanismos para el intercambio de información entre Instituciones de las listas de atención especial, relacionadas con los defraudadores, a efectos de promover la colaboración y cooperación para la prevención de fraudes y estafas cibernéticas.

ARTÍCULO 15.- POLÍTICA DE CONGELAMIENTO DE FONDOS

Las Instituciones Supervisadas deben contar con políticas y procedimientos que le permitan realizar bloqueos temporales y congelamiento de fondos de forma expedita, cuando sean notificados por otras Instituciones Supervisadas de la transferencia de fondos hacia la Institución, que se hayan realizado mediante fraudes y estafas a los usuarios financieros.

ARTÍCULO 16.- CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Institución Supervisadas adicionalmente deben contar como mínimo, según corresponda, con políticas, procedimientos y controles de seguridad de la información y ciberseguridad, en lo relacionado a:

a) Certificación de autenticidad de los sitios web y aplicaciones móviles de las Instituciones Supervisadas.

b) Mecanismos que garanticen al cliente la autenticidad de la comunicación proveniente de la Institución Financiera.

c) Cultura de contraseñas robustas.

d) Mecanismos para la protección de marca.

e) Tiempos de expiración por inactividad en las sesiones.

f) Doble factor de autenticación.

g) Límites de intentos de inicio de sesión o autenticación.

h) Límite de tiempo para la validez del OTP (One Time Password).

i) Límites diferenciados para transferencias a terceros, ACH, LBTR y otros, conforme a necesidades particulares de los clientes.

ARTÍCULO 17.- REPORTE DE EVENTOS

Las Instituciones Supervisadas deberán reportar a la Comisión los incidentes de fraude cibernético en contra de los usuarios financieros, al día hábil siguiente luego de identificado el incidente, indicando los datos de los usuarios afectados, así como la información general orientada a proporcionar una descripción del incidente, identificando el contacto dentro de la Institución para posteriores comunicaciones.

ARTÍCULO 18.- NOTIFICACIÓN Y RECLAMACIÓN DE TRANSACCIONES ELECTRÓNICAS NO AUTORIZADAS

El usuario financiero deberá notificar a la Institución Supervisada la ocurrencia de la transacción electrónica no autorizada, en un plazo no mayor de cuarenta y ocho (48) horas a partir de la fecha en que se haya enterado o se le hubiere notificado sobre dicha transacción, debiendo presentar a la institución supervisada, en caso de que no se le haya resuelto la gestión de forma inmediata, el reclamo mediante la hoja de reclamación autorizada por la Comisión, el cual deberá ser admitido para el trámite legal correspondiente.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

En el momento de la notificación sobre transacciones electrónicas no autorizadas, las Instituciones Supervisadas deberán proporcionar un número o código de recepción de la notificación para seguimiento por parte del usuario financiero, que incluya la fecha y hora en que dicha notificación fue recibida. Asimismo, la Institución Supervisada deberá proceder al bloqueo inmediato del servicio por medio del canal digital y ofrecerle una alternativa segura al usuario financiero para que pueda realizar sus operaciones.

Las Instituciones Supervisadas deberán resolver los reclamos presentados por los usuarios financieros por la ocurrencia de transacción electrónica no autorizada, en un plazo no mayor de diez (10) días hábiles contados a partir de la recepción del reclamo, prorrogables hasta por diez (10) días más. En caso de que lo resuelto por la Institución Supervisada no sea satisfactorio para el usuario financiero, este podrá acudir a la Comisión para interponer su reclamo ante este Órgano Supervisor, siguiendo los procedimientos establecidos en las Normas para el Fortalecimiento de la Transparencia, la Cultura Financiera, Conducta de Mercado y Atención al Usuario Financiero en las Instituciones Supervisadas, o la que la sustituya, emitidas por esta Comisión.

Las transacciones electrónicas no autorizadas que se realicen a partir de la fecha de entrada en vigencia de los presentes Lineamientos, podrán ser objeto de reclamo ante las Instituciones Supervisadas hasta con un (1) año calendario posterior a la fecha que se haya realizado dicha transacción.

ARTÍCULO 19.- DENUNCIA ANTE LAS AUTORIDADES COMPETENTES
Las Instituciones Supervisadas deben requerir a los titulares de las cuentas afectadas con operaciones fraudulentas, que interpongan la denuncia ante las autoridades judiciales correspondientes. Lo anterior, no es un requisito para la admisión de los reclamos de los usuarios financieros, sin embargo, si es un requisito para la resolución de los mismos.

CAPÍTULO IV
DISPOSICIONES FINALES

ARTÍCULO 20.- RESPONSABILIDAD
Las Instituciones Supervisadas serán responsables de la totalidad del monto reclamado por el usuario financiero por transacciones electrónicas no autorizadas en caso de no haber aplicado los Lineamientos descritos en la presente Resolución relacionados con la tipología de fraude materializada.

Las inversiones que realicen las Instituciones Supervisadas en la aplicación de estos Lineamientos no deben generar costos para el usuario financiero.

Los usuarios financieros deberán atender lo referente a sus obligaciones, según lo establecido en las Normas de Transparencia vigentes, emitidas por la Comisión.

ARTÍCULO 21.- CASOS NO PREVISTOS
Los casos no previstos en estos Lineamientos serán resueltos por la Comisión de conformidad con el marco legal y normativo.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

ARTÍCULO 22.- VIGENCIA
Lo descrito en los presentes Lineamientos no tiene efecto retroactivo y son de cumplimiento inmediato a partir de su publicación en el Diario Oficial La Gaceta.

2. Comunicar la presente Resolución a las Instituciones Supervisadas, para los efectos legales correspondientes y a la Superintendencia de Bancos y Otras Instituciones Financieras, Superintendencia de Seguros, Superintendencia de Pensiones y Valores, Gerencia de Riesgos, Gerencia de Protección al Usuario Financiero y Gerencia Legal, para su conocimiento.

3. Instruir a la Secretaría General de esta Comisión, que remita la presente Resolución a la Gerencia Administrativa, para que ésta la envíe a la Empresa Nacional de Artes Gráficas (ENAG), para efectos de su publicación en el Diario Oficial La Gaceta.

4. La presente Resolución entrará en vigencia a partir de su publicación en el Diario Oficial La Gaceta. … Queda aprobado por unanimidad. … F) **MARCIO GIOVANNY SIERRA DISCUA**, Presidente; **ALBA LUZ VALLADARES OCONNOR**, Comisionada Propietaria; **ESDRAS JOSIEL SÁNCHEZ BARAHONA**, Comisionado Propietario; **ANA GABRIELA AGUILAR PINEDA**, Secretaria General".

ANA GABRIELA AGUILAR PINEDA
Secretaria General

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán