17 de mayo del 2024

CNS-1861/06

Señora

María del Rocío Aguilar Montoya, superintendente

***Superintendencia General de Entidades Financieras***

Estimada señora:

El Consejo Nacional de Supervisión del Sistema Financiero, en el artículo 6 del acta de la sesión 1861-2024, celebrada el 14 de mayo del 2024,

**considerando que:**

**Consideraciones de orden legal y reglamentario**

I. El inciso b), del artículo 171 de la *Ley Reguladora del Mercado de Valores*, Ley 7732, faculta al Consejo Nacional de Supervisión del Sistema Financiero (Conassif) a aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que, conforme a la ley, debe ejecutar la Superintendencia General de Entidades Financieras (Sugef).

II. El inciso c), del artículo 131 de la *Ley Orgánica del Banco Central de Costa Rica*, Ley 7558, establece, como parte de las funciones del Superintendente General de Entidades Financieras, proponer al Conassif, para su aprobación, las normas que estime necesarias para el desarrollo de las labores de supervisión y fiscalización.

III. Mediante artículo 9, del acta de la Sesión 652-2007, celebrada el 11 de junio del 2007, el Conassif aprobó el *Reglamento sobre divulgación de información y publicidad de productos y servicios financieros*, Acuerdo Sugef 10-07, el cual, establece las disposiciones relativas a la divulgación de información y la publicidad sobre productos y servicios financieros que ofrecen los intermediarios financieros y las entidades creadas por Ley especial, supervisados por la Sugef.

IV. Mediante la Ley 8148 de 24 de octubre de 2001 se adicionaron al Código Penal, Ley 4573 de 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, para reprimir y sancionar los delitos informáticos, denominados: Violación de comunicaciones electrónicas, Fraude informático y Alteración de datos y sabotaje informático. Posteriormente, en el 2012, la ley 9048 titulada: ‘Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal’, publicada en el Alcance 172 de La Gaceta 214, introdujo los conceptos de estafa informática, daño informático, violación de datos personales, suplantación de páginas electrónicas y facilitación de delito informático.

**Consideraciones sobre las estafas informáticas**

V. El Comité de Supervisión Bancaria de Basilea, mediante su informe ‘Fraude digital y banca: implicaciones para la supervisión y la estabilidad financiera’, define que las estafas informáticas, también conocidas como fraudes digitales, son todas aquellas actividades fraudulentas perpetradas por partes externas a través de medios digitales (correos electrónicos, sitios web, software malicioso, entre otros) con el objetivo de robar activos bancarios o credenciales de clientes bancarios. Las estafas informáticas se centran principalmente en los clientes de los bancos, aunque estas entidades pueden desempeñar un papel indirecto e involuntario en la facilitación de las estafas.

VI. El Comité de Supervisión Bancaria de Basilea, señala que el fraude digital se agrupa en las siguientes categorías:

a) Fraude digital relacionado con instrumentos de pago en línea:

i. transacciones de pago no autorizadas.

ii. manipulación del pagador para emitir una orden de pago.

b) Fraude digital relacionado con otros productos bancarios de clientes.

c) Fraude digital relacionado con la entidad a través de datos de clientes o sistemas bancarios.

**Consideraciones sobre la responsabilidad objetiva**

VII. En relaciones de consumo, como lo son los servicios financieros suministrados mediante canales digitales, se aplica la normativa establecida en la *Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor*, Ley 7472, la cual, en su artículo 35 instituye una responsabilidad objetiva al productor, proveedor y comerciante que lesionen la esfera jurídica del consumidor por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su uso y riesgos. Por lo que, es necesario que demuestren que han sido ajenos al daño y en caso de una afectación, demuestren que esta se produjo por fuerza mayor o por culpa de la víctima.

VIII. El fundamento de lo anterior se basa en lo que se conoce como la responsabilidad objetiva por riesgo creado, la cual, establece que, quien emplea cosas peligrosas o riesgosas y expone a eventuales daños a los usuarios, debe reparar los daños que cause, aun cuando haya actuado lícitamente. Para determinar esta responsabilidad, debe existir un nexo de causalidad entre la actividad riesgosa puesta en marcha y el daño ocasionado.

IX. Un derecho que adquiere el usuario de servicios financieros suministrados mediante canales digitales y consecuente deber de las entidades financieras, es el resguardo de que las transacciones que se realicen contra la cuenta de fondos del usuario sean las que este ha autorizado.

X. Durante los últimos años los tribunales en Costa Rica han resuelto casos en favor de usuarios financieros de entidades ante denuncias por estafas informáticas. En la argumentación de las partes se destacan debilidades incurridas por ambas partes; en lo que respecta a la entidad, las deficiencias se encuentran principalmente en la robustez de los controles en relación con la gestión preventiva y de monitoreo del perfil transaccional del cliente, aunque la entidad no haya sido vulnerada en sus sistemas informáticos.

**Consideraciones desde la perspectiva del supervisor financiero**

XI. Desde una perspectiva de estabilidad y funcionamiento eficiente del Sistema Financiero, resulta medular que las entidades cuenten con marcos de control robustos que contribuyan con fomentar la confianza del público en el uso de los canales digitales, cuyo uso es cada vez más extendido.

XII. El Comité de Supervisión Bancaria de Basilea señala dos canales de transmisión del fraude digital para la supervisión y la estabilidad financiera: (i) las pérdidas financieras para las entidades derivadas del fraude digital sufridas por las propias entidades directamente o debido a la necesidad de reembolsar a sus clientes y que podrían reducir los recursos de capital de los bancos, así como tener efectos indirectos sobre otras entidades; y (ii) los riesgos para la reputación de las entidades y los supervisores, derivados de incidentes de fraude digital de gran repercusión que podrían provocar una pérdida de confianza más amplia en el Sistema Financiero.

XIII. El Comité de Supervisión Bancaria de Basilea, señala que la mayoría de las jurisdicciones miembros del Comité han implementado iniciativas para hacer frente al fraude digital, tales como: (i) capacitación de los ciudadanos; (ii) requisitos y directrices sobre controles y protocolos de seguridad; (iii) supervisión de las prácticas de gestión del riesgo de fraude digital de los bancos; (iv) colaboración entre las partes interesadas para una respuesta ecosistémica y (v) cooperación transfronteriza.

**Consideraciones sobre iniciativas nacionales y de los gremios**

XIV. Las asociaciones conformadas por entidades desempeñan un papel transcendental en el aumento de la resistencia a las estafas informáticas, al crear conciencia sobre las amenazas y al preparar el apoyo adecuado para lograr una respuesta efectiva. En Costa Rica se han creado comisiones interinstitucionales para enfrentar las estafas informáticas y las amenazas de seguridad cibernética, cuyos objetivos tratan sobre:

a) Abordar la problemática y acciones de cada institución respecto a las estafas informáticas.

b) Desarrollar tecnologías para identificar la suplantación de identidad de los usuarios financieros.

c) Realizar campañas de prevención de estafas informáticas.

d) Estandarizar las estadísticas para conocer la afectación real a nivel económico producto de las estafas informáticas.

**Consideraciones sobre mecanismos de autenticación robustos**

XV. Los factores de autenticación generalmente se basan en algo que el usuario conoce ‘factor de conocimiento’; algo que el usuario tiene ‘factor de posesión’; y algo que el usuario es ‘factor de inherencia’. Los mecanismos de autenticación robustos funcionan combinando dos o más factores de dichas categorías.

XVI. Actualmente, no se consideran mecanismos de autenticación robustos aquellos que incorporan tecnologías basadas en información que puede ser transferible a un tercero y que permitan la suplantación de identidad del usuario financiero.

XVII. Una forma efectiva de mitigar las estafas informáticas es mediante el uso de mecanismos de autenticación que incorporan tecnologías basadas en dobles factores de autenticación, los cuales, permitan validar y verificar la identidad de los usuarios financieros cuando:

1. Ingresen a los canales digitales.
2. Ejecuten transacciones y acciones que conlleven riesgo en dichos canales,
3. Utilicen mecanismos de autogestión en los canales digitales.

**Consideraciones sobre el fortalecimiento de los controles**

XVIII. El *Reglamento sobre Administración Integral de Riesgos*, Acuerdo Sugef 2-10, aborda parcialmente la problemática de las estafas informáticas al tipificar categorías de eventos de pérdida por riesgo operativo. En lo concerniente a clientes, productos y prácticas empresariales, se refiere a pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

XIX. En lo que respecta a la regulación sobre tecnología de información (TI), también se aborda parcialmente lo referente a las estafas informáticas, dado que se enfoca principalmente al nivel de la gestión de los riesgos tecnológicos y la seguridad cibernética de las entidades.

XX. Es conveniente que a las entidades supervisadas se les requiera gestionar expectativas y controles mínimos para prevenir y mitigar la ocurrencia de estafas informáticas en contra de los usuarios financieros y que el regulador pueda verificar que la aplicación de tales medidas sea consistente entre entidades del sistema financiero. Además, es fundamental el despliegue de programas y campañas de educación en ciberhigiene digital dirigidas a los usuarios financieros, las cuales, incluyan aspectos de concientización de los usuarios para prevenir que sean objeto de estafas informáticas.

**Consideraciones de costo-beneficio**

XXI. Que la evaluación costo-beneficio de la regulación se realiza de conformidad con lo establecido en los artículos 1 y 12 de la *Ley Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos*, Ley 8220 y en los artículos 12, 12 bis, 13, 13 bis y 56 al 60 bis del *Reglamento a la Ley de Protección al Ciudadano del Exceso de Requisitos y Trámites Administrativos*, 37045-MP-MEIC. Dicha regulación indica que la Administración Pública debe realizar un análisis de impacto regulatorio mediante una evaluación costo-beneficio antes de emitir cualquier nueva regulación o reformar las existentes, cuando establezcan trámites, requisitos y procedimientos que deba cumplir el administrado ante la Administración. De dicho análisis se determinó que la regulación no establece ni modifica trámites, requisitos o procedimientos que el administrado deba cumplir ante la Administración Central.

**Otras consideraciones**

XXII. Mediante artículo 13 del acta de las sesiones 1850-2024, celebrada el 18 de marzo del 2024, el Conassif remitió a consulta pública la propuesta de modificación al *Reglamento sobre divulgación de información y publicidad de productos y servicios financieros*, Acuerdo Sugef 10-07, en el entendido que, en un plazo máximo de diez días hábiles, contados a partir del día hábil siguiente del recibo de la respectiva comunicación podían enviar al Despacho de la superintendente general de entidades financieras sus comentarios y observaciones. Posteriormente, mediante artículo 11 del acta de la sesión 1852-2024, celebrada el 8 de abril del 2024, el Conassif dispuso extender, al 16 de abril del 2024, el plazo para la recepción de comentarios y observaciones a la citada propuesta de modificación normativa remitida en consulta.

**dispuso en firme:**

modificar el *Reglamento sobre divulgación de información y publicidad de productos y servicios financieros*, Acuerdo SUGEF 10-07, de conformidad con lo siguiente:

**1**. Modificar el nombre del reglamento, de conformidad con el siguiente texto:

*“Reglamento sobre la transparencia ante el usuario financiero en la prestación de productos y servicios por parte de entidades supervisadas por SUGEF, Acuerdo SUGEF 10-07.”*

**2**.Adicionar un párrafo tercero en el artículo 1. Objeto y alcance, de conformidad con el siguiente texto:

*“[…]*

*Asimismo,**este reglamento establece las disposiciones sobre los controles mínimos con que deben contar las entidades supervisadas por la SUGEF para prevenir y mitigar la ocurrencia de estafas informáticas en contra de los usuarios financieros; así como las disposiciones para crear mayor conciencia y educación sobre ciberhigiene digital en los usuarios financieros para la prevención de estos eventos.*

***3.*** Adicionar *el* *Capítulo III ASPECTOS MÍNIMOS DE CONTROL PARA PREVENIR Y MITIGAR LA OCURRENCIA DE ESTAFAS INFORMÁTICAS EN CONTRA DE LOS USUARIOS FINANCIEROS,* de conformidad con el texto que se incluye a continuación:

“CAPITULO III

ASPECTOS MÍNIMOS DE CONTROL PARA PREVENIR Y MITIGAR LA OCURRENCIA DE ESTAFAS INFORMÁTICAS EN CONTRA DE LOS USUARIOS FINANCIEROS

***Sección I Disposiciones generales***

***Artículo 12. Definiciones***

*Para efectos de este capítulo se utilizan las siguientes definiciones y abreviaturas:*

*a)* ***Ciberhigiene digital:*** *acciones que los usuarios pueden ejecutar para mejorar su seguridad en canales digitales y mantener su sistema protegido. Significa adoptar una mentalidad y unos hábitos centrados en la seguridad que ayuden a los usuarios financieros y las entidades supervisadas a mitigar posibles estafas informáticas.*

*b)* ***Notificaciones push:*** *mensaje corto que aparece como una ventana emergente en el navegador del escritorio, pantalla de inicio del dispositivo móvil o en el centro de notificaciones del dispositivo desde una aplicación móvil. Suelen ser alertas de confirmación que muestran texto y medios enriquecidos, como imágenes o botones, que permiten a un usuario financiero realizar una acción específica.*

*c)* ***URL (Localizador de Recursos Uniforme por sus siglas en inglés):*** *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.*

*d)* ***Usuario financiero:*** *Persona física o jurídica que utiliza un servicio o producto brindado por una entidad supervisada.*

*Los demás términos utilizados en este reglamento se entienden según sus definiciones contenidas integralmente en la reglamentación vigente aprobada por el CONASSIF, así como en la jerga técnica sobre la materia.*

***Sección II Estrategia de mitigación y educación en ciberhigiene digital***

***Artículo 13. Estrategia de mitigación de estafas informáticas***

*Las entidades supervisadas deben establecer una estrategia para minimizar los riesgos de estafas informáticas en contra de los usuarios financieros cuando estos utilizan los canales digitales que las entidades ponen a su disposición.*

*Dicha estrategia debe estar enmarcada en una evaluación de riesgos, realizada de manera conjunta con las unidades de negocio y las funciones de control correspondientes, así como estar alineada con las políticas de seguridad de la entidad, a fin de determinar si los controles implementados son robustos para mitigar las tipologías de estafas informáticas que afectan a los usuarios financieros.*

*La estrategia debe estar aprobada por el Órgano de Dirección. Además, dicha estrategia debe ser objeto de revisiones y actualizaciones de forma periódica según lo defina el Órgano de Dirección, a fin de identificar nuevos riesgos y nuevas tipologías de estafas informáticas que puedan afectar a los usuarios financieros.*

*La evaluación de riesgos debe actualizarse según la periodicidad que defina el Órgano de Dirección. Sin perjuicio de lo anterior, la evaluación de riesgos debe actualizarse cuando la entidad supervisada ponga a disposición de los usuarios financieros el uso de nuevos canales digitales, cuando esta incursione en nuevos productos o servicios financieros, así como cuando se realicen cambios en los ya existentes.*

***Artículo 14. Identificación de nuevas tipologías de estafas informáticas***

*Como parte de la evaluación de riesgos, las entidades supervisadas deben establecer mecanismos basados en un análisis estadístico para identificar y mitigar la ocurrencia de nuevas tipologías de estafas informáticas, así como monitorear la evolución de las existentes.*

*Para el análisis estadístico, se deberán compilar, al menos, los siguientes datos que permitan segmentar información sobre el conocimiento de cada caso de estafa informática y la concentración o comportamiento:*

*a) Monto defraudado.*

*b) Factores de autenticación que se utilizaron en el momento en que sucedió la estafa informática para ingresar, realizar transacciones o ejecutar acciones en los canales digitales.*

*c) Tipología de estafa informática. Las entidades supervisadas deben definir las tipologías de estafas informáticas.*

*d) Medio o canal utilizado para la estafa informática.*

*e) Descripción de la estafa informática.*

*f) Rango de edad del usuario financiero.*

*g) El día de la semana y franja horaria en que ocurrió la estafa informática.*

*h) Fecha de reporte de la estafa informática.*

*i) Fecha de resolución del caso.*

***Artículo 15. Educación al usuario financiero en ciberhigiene digital***

*Las entidades supervisadas deben establecer un programa de educación en ciberhigiene digital para el uso de los servicios y canales digitales, dirigido a los usuarios financieros. Dicho programa debe incluir aspectos relacionados con capacitación, asesoría y concientización de los usuarios financieros para prevenir que sean objeto de estafas informáticas; además, será responsabilidad de las entidades supervisadas definir el alcance del programa.*

*El programa de educación en ciberhigiene digital debe implementarse de forma permanente, mediante canales de comunicación y debe considerar, al menos, los siguientes aspectos:*

*a) Riesgos asociados con el uso de productos y servicios por medio de canales digitales, tipologías existentes de estafas informáticas, así como los derechos y obligaciones de los usuarios financieros en relación con los productos y servicios suministrados.*

*b) Posibles prácticas criminales que utilizan los estafadores para obtener información confidencial de los usuarios financieros.*

*c) Prácticas de protección de las credenciales del usuario financiero, así como aspectos a considerar para la adquisición de seguros de tarjetas o contra estafas informáticas, entre otras tipologías emergentes.*

*d) Concientización a los usuarios financieros sobre información y acciones relacionadas con sus productos financieros, las cuales, la entidad supervisada nunca les solicitará por medio de canales digitales o llamadas telefónicas.*

*e) Protección del correo electrónico que el usuario financiero tiene registrado para uso de los canales digitales de la entidad supervisada, así como la protección por medio de factores de autenticación robustos y el uso de contraseñas seguras.*

*f) Recomendaciones para que el usuario financiero pueda detectar un ataque de secuestro de número telefónico (SIM Swapping), a fin de identificar la suplantación de su tarjeta SIM y aplicar oportunamente el bloqueo de las cuentas de fondos.*

*g) Promover el uso de los canales digitales oficiales de la entidad supervisada. En el caso de aplicaciones, los usuarios financieros deberán estar enterados que la aplicación oficial de la entidad se debe descargar desde las tiendas oficiales de aplicaciones móviles o desde el sitio que la entidad supervisada indique. Además, se debe recomendar a los usuarios financieros que el acceso a los sitios web oficiales de la entidad se realice digitando las direcciones electrónicas y evitar hacerlo por medio de enlaces o buscadores de internet.*

*h) Orientación a los usuarios financieros para que sean capaces de reconocer una URL fraudulenta, cuentas falsas en productos de mensajería, llamadas fraudulentas, correos falsos, instalación de aplicaciones solicitadas por los estafadores, uso de software pirata, así como para el uso de productos antimalware o antivirus y los riesgos de utilizar redes públicas.*

*Además,**las entidades supervisadas deben desarrollar sus propias campañas de concientización para prevenir que los usuarios financieros sean objeto de estafas informáticas, de conformidad con los aspectos particulares de sus canales digitales, sean estos propios o tercerizados, así como del tamaño, enfoque de negocio y complejidad de las operaciones de la organización. Lo anterior, sin perjuicio de las campañas de concientización que desarrollen los gremios de los que forman parte.*

***Sección III Responsabilidad de la entidad supervisada***

***Artículo 16. Responsabilidad***

*En los casos en que el usuario financiero rechace haber autorizado una operación, las entidades supervisadas deberán verificar que dicha operación fue autorizada por el usuario financiero y que se encuentra registrada a su nombre.*

*Ante el reclamo de los usuarios financieros, las entidades supervisadas deberán demostrarle al usuario financiero que han cumplido con las disposiciones establecidas en el presente capítulo para prevenir y mitigar la ocurrencia de estafas informáticas en contra de dichos usuarios. Asimismo, las entidades supervisadas deberán verificar que los sistemas informáticos de las entidades no han sido vulnerados.*

*La auditoría interna o función equivalente deberá verificar, semestralmente, el cumplimiento por parte de la entidad supervisada de las disposiciones establecidas en el presente capítulo. En casos particulares, la función interna de control podrá manejar revisiones específicas.*

***Artículo 17. Controles preventivos, detectivos y correctivos***

*Las entidades supervisadas deben establecer controles preventivos, detectivos y correctivos para proteger las cuentas de fondos y la información de los usuarios financieros ante la ocurrencia de estafas informáticas por medio de canales digitales.*

*Dichos controles deben permitir a las entidades supervisadas identificar y tomar medidas respecto a transacciones atípicas por medio de un análisis integral y multifactorial sobre el usuario financiero, el cual, incluya, al menos, los siguientes aspectos:*

*a) Patrones transaccionales de los usuarios financieros, preferencias en cuanto a días o fechas de sus operaciones, destinatarios frecuentes de envíos de fondos, monto y tipo de transacciones realizadas habitualmente (transferencias, pagos, retiros, entre otros), así como otros aspectos relevantes para definir su comportamiento y detectar posibles actividades atípicas.*

*b) Dispositivos electrónicos utilizados habitualmente por el usuario financiero para acceso a los canales digitales, considerar elementos como el historial de dispositivos electrónicos utilizados, sistema operativo y horarios habituales de uso.*

*c) Variables del dispositivo electrónico utilizado como: user agent, sistema operativo del dispositivo, idioma, entre otros.*

*d) Navegadores utilizados habitualmente.*

*e) Verificación de las formas de autenticación utilizadas habitualmente por el usuario financiero.*

*f) Redes de conexión, canales digitales utilizados, comportamiento de uso de los dispositivos electrónicos tales como: la forma de teclear del usuario financiero, movimiento del mouse, entre otros.*

*g) Uso de un dispositivo electrónico para acceder a diferentes cuentas, productos o servicios que pertenecen a diferentes usuarios financieros de la entidad supervisada, a fin de analizar si se trata de actividades sospechosas.*

*h) Uso de un dispositivo electrónico que haya sido utilizado anteriormente para cometer estafas electrónicas.*

*Las entidades supervisadas deben incorporar parámetros para aprobar o denegar transacciones. En caso de que identifiquen la ocurrencia de transacciones atípicas, deberán requerir a los usuarios financieros, previo a hacerlas efectivas, una confirmación que asegure la autenticidad de estos.*

***Artículo 18. Mecanismos de autenticación robustos***

*Las entidades supervisadas deben establecer mecanismos de autenticación robustos que permitan validar y verificar la identidad de los usuarios financieros cuando estos:*

*a) Ingresen a los canales digitales.*

*b) Ejecuten transacciones y de acciones que conlleven riesgo en dichos canales.*

*c) Utilicen mecanismos de autogestión en los canales digitales, para la creación de nuevos usuarios, cambio de token, cambio de claves, bloqueo de cuentas de fondos, recuperación de credenciales, entre otros.*

*Dichos mecanismos de autenticación deben incorporar tecnologías basadas en dobles factores de autenticación.*

*Además, las entidades supervisadas deben evitar incorporar en sus mecanismos de autenticación, tecnologías basadas en información transferible a un tercero que permitan suplantar la identidad del usuario financiero.*

***Artículo 19. Protección de la información de los usuarios financieros***

*Las entidades supervisadas deben implementar en sus canales digitales, al menos, los siguientes mecanismos para proteger de la información de los usuarios financieros:*

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

*b) Elementos que permitan a los usuarios financieros corroborar la autenticidad de los comunicados remitidos por las entidades supervisadas.*

*c) Política de contraseñas robustas.*

*d) Tiempos de expiración por inactividad en las sesiones.*

*e) Límites de intentos de inicio de sesión o autenticación.*

*f) Límites de tiempo para que las sesiones iniciadas se cierren automáticamente cuando se detecte inactividad.*

*g) Límites diferenciados para la cantidad y monto de las transferencias realizadas por los usuarios financieros a terceros mediante canales digitales, tanto a nivel local como internacional, de conformidad con las necesidades particulares de los usuarios financieros.*

***Artículo 20. Notificación de transacciones***

*Las entidades supervisadas deben enviar una notificación a los usuarios financieros, en menos de un minuto, cuando se realicen transacciones en sus productos financieros; asimismo, cuando sucedan eventos como: inicios de sesión, cambios de contraseñas, cambios en mecanismos de seguridad, actualización de número de teléfono o correo electrónico, aumento de límites para transacciones, nuevos dispositivos electrónicos detectados, entre otros.*

*Dichas notificaciones deben enviarse mediante correo electrónico, mensajes de texto SMS o notificaciones push. Además, las notificaciones podrán enviarse mediante otros mecanismos que hayan sido autorizados por los usuarios financieros, en cuyo caso, las entidades supervisadas deberán informar a los usuarios financieros las implicaciones que tiene el mecanismo y la responsabilidad que tienen los usuarios de comunicar a las entidades cuando realicen cambios en sus direcciones de correo electrónico o en sus números de teléfono celular.*

*Cuando las entidades supervisadas envíen notificaciones a los usuarios financieros con el propósito de requerirles una confirmación o validación sobre las gestiones señaladas anteriormente u otras gestiones sensibles, deberán verificar la identidad de los usuarios financieros.*

***Artículo 21. Envío de enlaces en notificaciones***

*Las entidades supervisadas no deben incluir enlaces acortados en las notificaciones indicadas en el artículo 20 del presente capítulo cuando se envíen por medio de correos electrónicos dirigidos a los usuarios financieros.*

***Artículo 22. Políticas y procedimientos para bloqueos preventivos de fondos***

*Las entidades supervisadas deben establecer políticas y procedimientos para realizar bloqueos preventivos de fondos de transferencias cuyo origen o destino se presuma que corresponde a una estafa informática.*

***Artículo 23. Mecanismos de autogestión para el bloqueo temporal de productos y servicios financieros***

*Las entidades supervisadas deben habilitar en sus canales digitales y en sus centros de atención telefónica, mecanismos de autogestión que les permitan a los usuarios financieros realizar bloqueos temporales de sus productos y servicios financieros de forma expedita.*

***Artículo 24. Registros***

*Las entidades supervisadas deben mantener registros de las cuentas de fondos que hayan sido utilizadas en estafas informáticas, a fin de adoptar las medidas correspondientes de monitoreo y debida diligencia.*

***Artículo 25. Reporte de estafas informáticas***

*Las entidades supervisadas deben remitir a la SUGEF un reporte histórico de los casos constatados como estafas informáticas en contra de los usuarios financieros, así como de las lecciones aprendidas.*

*La SUGEF comunicará el contenido, la periodicidad, los plazos y los canales de remisión de dicho reporte.*

***Artículo 26. Notificación y reclamación de transacciones electrónicas no autorizadas***

*Cuando los usuarios financieros rechacen haber autorizado una transacción electrónica, deberán notificarlo a la entidad supervisada. Lo anterior, deberá ser comunicado a los usuarios financieros por medio de las campañas de concientización que realicen las entidades supervisadas según lo establecido en el artículo 15 del presente capítulo a fin de que los usuarios puedan informarse sobre el deber de cumplimiento de dicha notificación.*

*Los canales o servicios que facilite la entidad supervisada para la notificación deben estar a disposición incluso encontrándose los usuarios financieros fuera del país.*

*En el momento de la notificación sobre transacciones electrónicas no autorizadas, las entidades supervisadas deberán proporcionar un número o código de recepción de la notificación para seguimiento por parte de los usuarios financieros, el cual, incluya la fecha y hora en que dicha notificación fue recibida.*

*Las entidades supervisadas deberán bloquear de forma inmediata el producto o servicio suministrado a los usuarios y ofrecerles una alternativa contingente para que puedan realizar sus operaciones.*

*Cuando los usuarios financieros presenten reclamos por la ocurrencia de transacciones electrónicas no autorizadas, las entidades supervisadas deberán atender dichos reclamos de conformidad con lo dispuesto en la Sección 2, Capítulo II, del presente reglamento.*

***Artículo 27. Debido proceso ante la SUGEF***

*Cuando los usuarios financieros presenten reclamos por la ocurrencia de transacciones electrónicas no autorizadas y dichos reclamos no sean atendidos por las entidades supervisadas de conformidad con lo establecido en la Sección 2, Capítulo II, del presente reglamento, los usuarios podrán presentar una queja mediante oficio ante la SUGEF siguiendo los procedimientos establecidos en relación con la atención de quejas o denuncias establecidos en el sitio web de la Superintendencia.*

*La SUGEF gestionará el traslado del reclamo recibido a la entidad supervisada aludida para que esta le brinde directamente la respuesta que en derecho corresponda al usuario financiero.*

*Cuando los conflictos que se presenten entre las entidades supervisadas y sus usuarios financieros, como consecuencia de los contratos privados suscritos entre ambos, no logren dirimirse por los procedimientos administrativos contemplados en nuestro ordenamiento jurídico, dichos conflictos deberán resolverse en las instancias judiciales correspondientes.*

***Artículo 28. Denuncia ante las autoridades competentes***

*Como parte del proceso de atención de reclamos, las entidades supervisadas podrán requerir a los titulares de las cuentas de fondos afectadas con estafas informáticas, que presenten la denuncia ante las autoridades judiciales correspondientes en aquellos casos que lo ameriten. Queda a criterio de la entidad supervisada, de conformidad con sus políticas y procedimientos para la atención y solución de quejas o reclamos, determinar los casos en que será requerida la denuncia del usuario financiero ante las autoridades judiciales.*

*Rige a partir del 1° de junio de 2025.”*

Atentamente,

Celia Alpízar Paniagua

***Secretaria interina del Consejo***