22 de marzo del 2024

CNS-1850/13

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 13 del acta de la sesión 1850-2024, celebrada el 18 de marzo del 2024,

**considerando que:**

A. El numeral 2 del artículo 361 de la *Ley General de la Administración Pública*, Ley 6227, establece que se concederá a las entidades representativas de intereses de carácter general o corporativo afectadas por la disposición, la oportunidad de exponer su parecer.

B. Se elaboró la propuesta de modificación al *Reglamento sobre divulgación de información y publicidad de productos y servicios financieros*, Acuerdo Sugef 10-07, en cumplimiento del *Procedimiento para la Tramitación ante el Consejo Nacional de Supervisión del Sistema Financiero Costarricense de proyectos de emisión o reforma de reglamentos del sistema financiero*, el cual debe ser sometido en consulta a las entidades supervisadas, cámaras y gremios, así como a los grupos y conglomerados financieros.

**dispuso en firme:**

remitir en consulta, en cumplimiento de lo establecido en el numeral 2, artículo 361, de la *Ley General de la Administración Pública*, Ley 6227, a las entidades financieras supervisadas por la Sugef, 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, deberán adicionar sus comentarios y observaciones en el formulario que está disponible en el apartado *Formularios para remitir observaciones de normativa en consulta*, ubicado en la dirección electrónica de la página oficial de la Sugef:

<https://www.sugef.fi.cr/normativa/Formularios%20Normativa%20en%20Consulta.aspx>

Sin detrimento de lo anterior, las entidades consultadas pueden presentar de manera consolidada sus observaciones y comentarios a través de los gremios y cámaras que les representan. Asimismo, el correo electrónico normativaenconsulta@sugef.fi.cr será utilizado únicamente como mecanismo de notificación sobre la completitud de dicho formulario.

“PROYECTO DE ACUERDO

“El Consejo Nacional de Supervisión del Sistema Financiero *(*Conassif).

**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 N.º 172 de La Gaceta N.º 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 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. Los tokens de seguridad son muy utilizados como factores de autenticación, sin embargo, con el aumento del el uso de tokens, también ha [aumentado el riesgo](https://fastercapital.com/es/contenido/Aumento-de-su-comercializacion-con-certificacion-de-riesgo-de-credito--un-movimiento-ganador.html) de estafas informáticas. El Equipo de Detección y Respuesta (DART, por sus siglas en inglés) de Microsoft advirtió de un aumento en el robo de tokens por parte de cibercriminales.

XVII. Actualmente, no se consideran mecanismos de autenticación robustos aquellos que incorporan tecnologías basadas en dobles factores de autenticación que utilicen elementos lógicos como: token, códigos de un solo uso o tarjetas de coordenadas. Lo anterior, ya que, pueden olvidarse, perderse o ser robados.

XVIII. 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, tales como: firmas digitales, estándar FIDO, factores biométricos o autenticación basada en comportamiento, los cuales, son difíciles de replicar o falsificar.

**Consideraciones sobre el fortalecimiento de los controles**

XIX. 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.

XX. 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.

XXI. 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**

XXII. 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.

**dispuso:**

*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:*** *pasos que los usuarios de ordenadores u otros dispositivos pueden seguir 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****. FIDO (acrónimo en inglés de Fast Identity Online):*** *permite que los usuarios puedan utilizar sus propios dispositivos (smartphones o portátiles con biometría, llaves de seguridad USB, entre otros) para realizar la autenticación en canales digitales, tanto en entornos móviles como de escritorio.*

*c****. 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.*

*d****. 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.*

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

*f****. VPN (Red Privada Virtual por sus siglas en inglés):*** *Red que permite a los usuarios conectarse a internet de forma segura y privada mediante técnicas de encriptación.*

*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***

*Como parte del Marco de Administración Integral de Riesgos, 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 y ser objeto de revisiones y actualizaciones de forma periódica, 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 la entidad supervisada defina. 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 del Marco de Administración Integral 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, a fin de complementar la evaluación de riesgos e incluir alertas en las campañas de concientización dirigidas a los usuarios financieros en relación con nuevas tipologías de estafas identificadas.*

*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) Zona geográfica en que ocurrió la estafa informática, con indicación de la provincia y cantón en caso del territorio costarricense o del país en caso de que la estafa informática suceda en el exterior.*

*c) Factores de autenticación existentes en el momento en que sucedió la estafa informática.*

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

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

*f) Descripción de la estafa informática.*

*g) Rango de edad del usuario financiero.*

*h) Género del usuario financiero.*

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

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

*k) 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 la concientización de los usuarios financieros para prevenir que sean objeto de estafas informáticas.*

*El programa de educación en ciberhigiene digital debe implementarse de forma permanente, mediante canales de comunicación efectivos 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) 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 que la entidad supervisada nunca les solicitará por medio de canales digitales.*

*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.*

*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.*

***Artículo 16. Campañas de concientización***

*Las entidades supervisadas deben desarrollar sus propias campañas de concientización para prever 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 a nivel gremial o general desarrollen las asociaciones de las que forman parte.*

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

***Artículo 17. Responsabilidad***

*En los casos en que el usuario financiero desconozca haber autorizado una operación, las entidades supervisadas deberán demostrar que dicha operación fue autorizada por el usuario financiero y que se encuentra registrada a su nombre. Lo anterior, mediante bitácoras que indiquen, al menos, la fecha de la estafa informática, la hora en que se realizó dicha estafa, el monto defraudado; asimismo, que indiquen el dispositivo electrónico utilizado, marca, modelo, geolocalización y el país desde el cual se registró la conexión, a fin de validar que estos corresponden a los conocidos para el usuario financiero.*

*Ante el reclamo de los usuarios financieros, las entidades supervisadas deberán demostrar que han cumplido con las disposiciones establecidas en el presente capítulo para prevenir y mitigar la ocurrencia de estafas informáticas en contra de los usuarios o que los sistemas informáticos de las entidades no han sido vulnerados. El solo registro de la operación no bastará para demostrar que esta fue autorizada o realizada por el usuario financiero, ni que este actuó con culpa o descuido que le sean imputables.*

*La función interna de control 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 18. 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) Histórico de usuarios utilizados para acceso a los canales digitales.*

*c) Preferencias de dispositivos electrónicos utilizados 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.*

*d) Ubicación del dispositivo electrónico utilizado, así como la frecuencia de cambio de ubicaciones.*

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

*f) Navegadores utilizados habitualmente.*

*g) Direcciones IP utilizadas en las transacciones y su posible inclusión en listas negras, así como el uso de herramientas para ocultar las direcciones IP.*

*h) Verificación de las formas de autenticación preferidas por el usuario financiero.*

*i) 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.*

*j) Uso de un dispositivo electrónico para acceder, simultáneamente, a más de una cuenta, producto o servicio financiero.*

*k) 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 19. 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 ingresen a los canales digitales, así como para la ejecución de transacciones y de acciones que conlleven riesgo en dichos canales.*

*Asimismo, las entidades supervisadas deben implementar mecanismos de autenticación robustos para validar y verificar la identidad de los usuarios financieros cuando 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, tales como: firmas digitales, estándar FIDO, factores biométricos o autenticación basada en comportamiento. Se debe evitar el uso de tecnologías que provoquen exclusión financiera.*

*Además, las entidades supervisadas no deben incorporar en sus mecanismos de autenticación, tecnologías basadas en dobles factores de autenticación que utilicen elementos lógicos como: token, códigos de un solo uso o tarjetas de coordenadas; lo anterior, a fin de evitar que tecnologías basadas en información transferible a un tercero permitan suplantar la identidad del usuario financiero.*

***Artículo 20. Análisis de riesgos en mecanismos de autogestión***

*Las entidades supervisadas deben implementar análisis de riesgos a los mecanismos de autogestión que incorporan en sus canales digitales para, al menos, las siguientes acciones ejecutadas por el usuario financiero: creación de nuevos usuarios, cambio de contraseñas, bloqueo de cuentas de fondos, recuperación de credenciales.*

*Dichos análisis de riesgos deben considerar, al menos, los siguientes aspectos:*

*a) Producto o servicio financiero analizado en el canal digital.*

*b) Riesgos inherentes asociados por producto o servicio financiero.*

*c) Controles implementados por riesgo.*

*d) Análisis de riesgo residual.*

*e) Monitoreo de efectividad de los controles definidos.*

*f) Plan de acción a implementar para la mitigación de riesgos.*

*g) Acuerdos formales de aceptaciones de riesgo**.*

***Artículo 21. 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) Mecanismos para la protección de marca.*

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

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

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

*h) 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 22. Notificación de transacciones***

*Las entidades supervisadas deben notificar 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 realizarse mediante correo electrónico, mensajes de texto SMS, notificaciones push u 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 utilizar un mecanismo distinto al correo electrónico.*

***Artículo 23. Envío de enlaces o links en comunicaciones***

*Las entidades supervisadas no deben incluir enlaces o links cortos en las comunicaciones que realicen por medio de correos electrónicos dirigidos a los usuarios financieros.*

***Artículo 24. 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 25. 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 26. Registros de atención especial***

*Las entidades supervisadas deben mantener registros especiales de los usuarios financieros cuyas cuentas de fondos hayan sido utilizadas en estafas informáticas y de los que hayan sido afectados con transacciones electrónicas no autorizadas. Lo anterior, a fin de adoptar las medidas correspondientes de monitoreo y debida diligencia, de conformidad con el perfil de riesgo del usuario, el cual, debe considerar los aspectos del análisis integral y multifactorial sobre el usuario financiero definidos en el artículo 18 del presente reglamento.*

*Asimismo, se deben mantener registros de lecciones aprendidas de los casos de estafas informáticas atendidos, a fin de generar experiencia aplicable a otros casos.*

*Las entidades supervisadas deben mantener registros de la información técnica relacionada con los dispositivos electrónicos e interacciones digitales utilizados por los estafadores involucrados en los casos atendidos, así como intercambiar, trimestralmente, dichos registros con las demás entidades supervisadas a fin de promover la colaboración y cooperación para la prevención de estafas informáticas. Será responsabilidad de las entidades definir el medio por el cual realizarán el intercambio de dichos registros.*

***Artículo 27. Reporte de estafas informáticas***

*Las entidades supervisadas deben remitir a la SUGEF un reporte histórico de las estafas informáticas en contra de los usuarios financieros, de conformidad con el contenido, la periodicidad, los canales, y los plazos de remisión que disponga la Superintendencia.*

*La SUGEF comunicará, mediante acto administrativo, el contenido, la periodicidad, los plazos y los canales de remisión del reporte histórico de las estafas informáticas.*

***Artículo 28. Notificación y reclamación de transacciones electrónicas no autorizadas***

*Cuando los usuarios financieros desconozcan haber autorizado una transacción electrónica, deberán notificarlo a la entidad supervisada en un plazo no mayor de setenta y dos (72) horas a partir de la fecha en que se haya enterado o se le hubiere notificado sobre dicha transacción. 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 17 del presente capítulo a fin de que los usuarios puedan informarse sobre el deber de cumplimiento de dicho plazo.*

*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 29. Debido proceso ante la SUGEF***

*Cuando los usuarios financieros presenten reclamos por la ocurrencia de transacciones electrónicas no autorizadas y no obtengan respuesta de las entidades supervisadas en un plazo de diez días hábiles, 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 30. 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. Lo anterior, no será un requisito para la recepción de los reclamos de los usuarios financieros.*

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

Atentamente,

Celia Alpízar Paniagua

***Secretaria interina del Consejo***