INSTITUCIONES DESCENTRALIZADAS

SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS

RESOLUCIÓN DE SUPERINTENDENCIA GENERAL DE ENTIDADES FINANCIERAS
SGF-RES-0036-2026

San José a las once horas del once de agosto del dos mil veintiséis.

La Superintendente General de Entidades Financieras;

CONSIDERANDO QUE:

A. Consideraciones de orden legal y reglamentario

I. Mediante la Ley de Protección a las personas consumidoras en la custodia de su dinero que administra cualquier entidad financiera en Costa Rica, ya sea pública o privada autorizada para este fin, Ley 10889, publicada en el Alcance 40 del diario oficial La Gaceta 73 del 22 de abril de 2026, se introduce un marco legal orientado a resguardar los fondos de los consumidores financieros frente a riesgos asociados a estafas informáticas y operaciones no autorizadas.

II. La Ley 10889 reforma, entre otras disposiciones, el artículo 35 de la Ley 7472, Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, estableciendo un régimen de responsabilidad aplicable a las entidades financieras ante una eventual custodia de fondos inadecuada y ante la sustracción de dinero por parte de terceros no autorizados, bajo un enfoque de responsabilidad independiente de la existencia de culpa.

III. La Ley 10889 incorpora modificaciones a la Ley General de la Administración Pública y al Código Procesal Civil, específicamente al régimen procesal aplicable en materia de protección al consumidor financiero, introduciendo la inversión de la carga de la prueba en favor de las personas usuarias en

casos relacionados con estafas informáticas y servicios financieros, tanto en sede administrativa como judicial.

IV. La Ley 10889 establece obligaciones específicas para las entidades financieras supervisadas por esta Superintendencia, relativas a la atención de reclamos, la investigación de estafas informáticas, la implementación de mecanismos de control y monitoreo de transacciones, así como la adopción de medidas de mitigación y compensación a favor de los consumidores financieros afectados por estafas informáticas y operaciones no autorizadas.

V. De conformidad con lo dispuesto en el artículo 10 de la Ley 10889, corresponde a la Superintendencia General de Entidades Financieras (SUGEF) emitir normativa de acatamiento obligatorio orientada a prevenir, reducir y procurar erradicar las estafas informáticas en perjuicio de los usuarios financieros.

VI. El artículo 119 de la Ley Orgánica del Banco Central de Costa Rica (LOBCCR), Ley 7558, dispone que, con el propósito de velar por la estabilidad, la solidez y el eficiente funcionamiento del Sistema Financiero Nacional, la SUGEF ejercerá sus actividades de supervisión y fiscalización sobre todos los intermediarios financieros, con estricto apego a las disposiciones legales y reglamentarias, velando porque cumplan con los preceptos que les sean aplicables. Para efectos de la LOBCCR, los términos "fiscalización" y "supervisión" aluden, en general, a las funciones y responsabilidades atribuidas por esa ley a la Superintendencia.

VII. De conformidad con la competencia especial conferida a la SUGEF por la Ley 10889, corresponde a esta Superintendencia establecer estándares mínimos de control que permitan mitigar los riesgos asociados a las estafas informáticas y preservar la confianza en el sistema financiero.

VIII. 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 año 2012, la Ley de Reforma de varios artículos y modificación de la Sección VIII, denominada delitos informáticos y conexos, del Título VII del Código Penal, Ley 9048, 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".

B. Consideraciones sobre las estafas informáticas

IX. El Comité de Supervisión Bancaria de Basilea, mediante su informe titulado "Fraude digital y banca: implicaciones para la supervisión y la estabilidad financiera", publicado en el sitio web del Banco de Pagos Internacionales (BIS), en la sección "Committees &associations", apartado "Basel Committee on Banking Supervision", subsección "Publications", 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 sustraer activos o credenciales de los clientes bancarios sin su consentimiento.

X. En el informe citado en el considerando anterior, el Comité de Supervisión Bancaria de Basilea señala que el fraude digital se agrupa en las siguientes categorías:

a) 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.

C. Consideraciones sobre la responsabilidad objetiva

XI. La Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley 7472 del 20 de diciembre de 1994, establece el marco jurídico para la protección de los derechos de las personas consumidoras, asegurando condiciones de equidad, seguridad y transparencia en las relaciones de consumo.

XII. Mediante la Ley 10889, se reformó el artículo 35 de la Ley 7472, con el propósito de actualizar el régimen de responsabilidad aplicable en las relaciones de consumo. El artículo 35 establece un régimen de responsabilidad en materia de protección al consumidor caracterizado por su amplitud y objetividad. Dicho artículo, dispone que el productor, el proveedor y el comerciante deben responder de forma concurrente y sin

necesidad de que exista culpa, cuando el consumidor resulte perjudicado por el bien o servicio, por información inadecuada o insuficiente, o por los riesgos derivados de su uso. Esta responsabilidad solo cesa si el sujeto logra demostrar que no tuvo relación alguna con el daño ocasionado. Asimismo, se extiende la responsabilidad a la estructura organizativa de las empresas, señalando que los representantes legales o encargados del negocio responden tanto por sus propios actos como por los de sus dependientes o auxiliares. De igual manera, los técnicos y responsables de los procesos de elaboración y control pueden responder solidariamente cuando se configuren infracciones que perjudiquen al consumidor.

XIII. Asimismo, el artículo 35 incorpora una regla específica para las entidades financieras supervisadas, las cuales deben responder, también bajo un criterio objetivo, por los daños y perjuicios derivados de la sustracción de dinero o de la afectación patrimonial en las cuentas de las personas usuarias, así como por la inadecuada custodia de sus fondos, cuando dichas situaciones provengan de terceros no autorizados, sin importar el mecanismo utilizado. Sin embargo, estas entidades podrán eximirse de responsabilidad cuando se configure alguna causa de exoneración prevista en la legislación.

XIV. El fundamento de lo indicado en el considerando anterior es el principio de 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.

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

XVI. Durante los últimos años los tribunales en Costa Rica han resuelto casos a 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.

D. Consideraciones desde la perspectiva del supervisor financiero

XVII. Desde una perspectiva de estabilidad y funcionamiento eficiente del Sistema Financiero, resulta medular que los intermediarios financieros cuenten con marcos de control robustos de cara a la confianza que el público ha depositado en ellos, independientemente del canal por el que se presten los servicios financieros, en particular en el uso de los canales digitales cuyo uso es cada vez más extendido y fomentado por los propios intermediarios financieros.

XVIII. El Comité de Supervisión Bancaria de Basilea, mediante su informe titulado "Fraude digital y banca: implicaciones para la supervisión y la estabilidad financiera", publicado en el sitio web del Banco de Pagos Internacionales (BIS), en la sección "Committees &associations", apartado "Basel Committee on Banking Supervision", subsección "Publications", 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.

XIX. En el informe citado en el considerando anterior, 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.

E. Consideraciones sobre mecanismos de autenticación robustos

XX. Los factores de autenticación generalmente se basan en algo que el usuario conoce y a lo que se le denomina "factor de conocimiento"; algo que el usuario tiene, llamado "factor de posesión"; y algo que el usuario es, designado como "factor de inherencia". Actualmente es ampliamente reconocido que los mecanismos de autenticación robustos funcionan combinando dos o más de dichos factores, siendo que 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.

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

a) Ingresen a los canales digitales.
b) Ejecuten transacciones y acciones que conlleven riesgo en dichos canales,
c) Utilicen mecanismos de autogestión en los canales digitales.

F. Consideraciones sobre el fortalecimiento de los controles

XXII. 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, dicho Acuerdo 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.

XXIII. En lo que respecta al marco regulatorio sobre tecnología de información aprobado por el CONASSIF, 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.

XXIV. 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 perjuicio 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 víctimas de estafas informáticas.

G. Consideraciones de costo-beneficio

XXV. 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.

H. Otras consideraciones

XXVI. Mediante oficio SGF-RES-0017-2026 del 4 de junio de 2026, la Sugef remitió a consulta externa la propuesta de Reglamento sobre aspectos mínimos de control para prevenir y mitigar estafas informáticas en perjuicio de los usuarios financieros, Acuerdo SUGEF 5-26, 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, las entidades supervisadas por la SUGEF podían enviar sus comentarios y observaciones.

DISPUSO:

Aprobar el Reglamento sobre aspectos mínimos de control para prevenir y mitigar estafas informáticas en perjuicio de los usuarios financieros, Acuerdo SUGEF 5-26, de conformidad con el siguiente texto:

REGLAMENTO SOBRE ASPECTOS MÍNIMOS DE CONTROL PARA PREVENIR Y MITIGAR ESTAFAS INFORMÁTICAS EN PERJUICIO DE LOS USUARIOS FINANCIEROS, ACUERDO SUGEF 5-26

Capítulo I Disposiciones generales

Artículo 1. Objeto y alcance

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 perjuicio 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.

Este reglamento aplica a los casos de estafas informáticas que impliquen la sustracción de dinero o la afectación del patrimonio asociado a cuentas de fondos, así como a la inadecuada custodia de los fondos depositados en dichas cuentas, administradas por las entidades supervisadas.

Artículo 2. Definiciones

Para efectos del presente reglamento se utilizan las siguientes definiciones y abreviaturas:

a) Canales digitales: medios electrónicos puestos a disposición de los usuarios financieros por las entidades supervisadas para el acceso, consulta, gestión y ejecución de operaciones relacionadas con cuentas de fondos y los productos y servicios financieros asociados a estas, tales como aplicaciones móviles, sitios web, plataformas en línea, entre otros.

b) Ciberhigiene digital: Conjunto de prácticas, hábitos y medidas de seguridad que los usuarios financieros pueden adoptar y ejecutar para proteger su información, sus credenciales y sus dispositivos al utilizar canales digitales, con el fin de mitigar el riesgo de ser víctimas de estafas informáticas.

c) Estafas informáticas: manipulación o influencia en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro, en perjuicio de una persona física o jurídica.

d) 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.

e) Token: elemento físico o digital que el usuario financiero utiliza en los canales digitales que las entidades supervisadas ponen a su disposición, el cual permite autenticar su identidad o validar operaciones, y que puede consistir en códigos, dispositivos o credenciales que generan o contienen información verificable.

f) 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.

g) User agent: programa o aplicación que actúa en nombre del usuario financiero al utilizar los canales digitales que las entidades supervisadas ponen a su disposición, y que proporciona información técnica sobre el usuario o el dispositivo desde el cual se accede a dichos canales, como el tipo de aplicación, el sistema operativo o el dispositivo utilizado.

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

Capítulo II Estrategia de mitigación y educación en ciberhigiene digital

Artículo 3. Estrategia de mitigación de estafas informáticas

Las entidades supervisadas deben establecer una estrategia para minimizar los riesgos de estafas informáticas en perjuicio 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 4. 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.

La información indicada deberá mantenerse a disposición de la SUGEF y remitirse en la forma, periodicidad y formato que ésta disponga, con el fin de construir y actualizar indicadores recurrentes sobre la eficacia y eficiencia de las entidades supervisadas en la prevención y mitigación de estafas informáticas, fraudes electrónicos y rebajos no autorizados.

Artículo 5. 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 delictivas 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 o coberturas 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.

Capítulo III Responsabilidad de la entidad supervisada

Artículo 6. Reclamos de transacciones electrónicas no autorizadas

Cuando los usuarios financieros rechacen haber autorizado una operación, en la que han sido víctimas de estafas informáticas o rebajos no autorizados, o denuncien que su cuenta ha sido utilizada por terceros para realizar estas acciones en perjuicio de terceros, podrán presentar su reclamo ante las entidades supervisadas en el plazo establecido en la Ley 10889.

Los reclamos deberán presentarse mediante un formulario que las entidades supervisadas pondrán a disposición del usuario financiero, el cual permita exponer de forma clara los hechos acontecidos. Además, el reclamo deberá acompañarse de una copia de la denuncia interpuesta ante el Organismo de Investigación Judicial (OIJ).

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 5 del presente reglamento a fin de que los usuarios puedan informarse sobre el adecuado cumplimiento de dichas disposiciones.

Asimismo, sin que su uso sea obligatorio para el usuario financiero, las entidades supervisadas deberán asegurar la disponibilidad continua de canales telefónicos, medios tecnológicos y mecanismos de autogestión para la presentación de reclamos, los cuales el usuario financiero podrá utilizar o, alternativamente, presentar su reclamo de forma presencial en las oficinas de la entidad supervisada. Además, deberán mantener registros del momento y del canal mediante el cual se presentó el reclamo.

Dichos canales deberán cumplir con los controles mínimos dispuestos en el presente reglamento para prevenir y mitigar la ocurrencia de estafas informáticas, así como con los estándares de seguridad establecidos en el marco regulatorio sobre tecnología de información aprobado por el CONASSIF.

Artículo 7. Codificación de recepción de reclamos y medidas de protección

En el momento de la presentación y registro de reclamos sobre transacciones electrónicas no autorizadas, las entidades supervisadas deberán proporcionar un número o código de recepción del reclamo para seguimiento por parte de los usuarios financieros, el cual, incluya la fecha y hora en que el reclamo fue recibido.

Las entidades supervisadas deberán bloquear de forma inmediata el producto o servicio suministrado respecto de su funcionalidad para realizar transacciones electrónicas a los usuarios y ofrecerles una alternativa contingente para que puedan realizar sus operaciones. Además, deberán remitir al usuario financiero, a la mayor brevedad posible y por el medio previamente acordado o registrado ante la entidad supervisada, una comunicación que confirme el bloqueo e indique el número o código de recepción correspondiente.

Cuando se registren transacciones no autorizadas por el usuario financiero con posterioridad a la presentación del reclamo ante la entidad supervisada, esta será responsable por dichas transacciones y por las consecuencias económicas derivadas de estas.

Artículo 8. Investigación y resolución de reclamos de los usuarios financieros

Ante el reclamo de los usuarios financieros, las entidades supervisadas deberán investigar los hechos y resolver si el reclamo procede o no.

Las investigaciones que realicen las entidades supervisadas deberán demostrar al usuario financiero el cumplimiento de las disposiciones establecidas en el presente reglamento para prevenir y mitigar la ocurrencia de estafas informáticas, así como demostrar, con base en los controles establecidos en el artículo 12, que sus sistemas informáticos no han sido vulnerados.

Una vez verificado el cumplimiento de lo señalado anteriormente, las entidades supervisadas procederán al análisis del comportamiento del usuario financiero en los hechos investigados.

La investigación, resolución y el tratamiento de los reclamos procedentes y no procedentes se regirán por los plazos y demás disposiciones establecidas en Ley 10889. Asimismo, cuando las entidades supervisadas resuelvan un reclamo en forma extemporánea, deberán aplicar lo dispuesto en dicha Ley, sin perjuicio de la procedencia o no del reclamo principal.

Artículo 9. Causales de rechazo de los reclamos de los usuarios financieros

Las entidades supervisadas podrán rechazar el reclamo cuando cuenten, para el caso analizado, con elementos probatorios específicos y suficientes que permitan determinar fehacientemente:

a) Que la entidad supervisada, en el análisis y comprobación de alguna de las causales de rechazo establecida en los incisos b), c) y d) del presente artículo, cumplió con las disposiciones establecidas en el presente reglamento para prevenir y mitigar la ocurrencia de estafas informáticas.

b) Cuando haya existido autofraude, entendido como la acción intencional realizada por una persona con el fin de inducir a error a una entidad financiera, con el propósito de obtener un beneficio.

c) Cuando haya existido dolo, entendido como toda conducta deliberada de una persona orientada a cometer un acto ilícito, con pleno conocimiento de su ilegalidad.

d) Cuando la transferencia haya sido entre cuentas del mismo titular.

Las entidades supervisadas deberán comunicar al usuario financiero la resolución denegatoria del reclamo, la cual deberá incluir las evidencias e incidentes de seguridad que la sustentan, tales como el análisis forense o la bitácora elaborada de conformidad con los aspectos mínimos de control para prevenir y mitigar la ocurrencia de estafas informáticas en perjuicio de los usuarios financieros dispuestos en el presente reglamento, así como lo dispuesto en la Ley 10889.

Asimismo, las entidades supervisadas deberán remitir copia de dicha información al OIJ y a la SUGEF, para que esta última, mediante acto razonado y en el plazo establecido en la Ley 10889, valide si la decisión adoptada se encuentra debidamente ajustada y respaldada en las pruebas aportadas por la entidad supervisada.

La SUGEF emitirá un protocolo para la atención de los casos en los que las entidades supervisadas emitan resoluciones denegatorias de reclamos, en el cual se especificará la información que estas deberán remitir, así como el canal dispuesto para su remisión a la Superintendencia.

Las actuaciones que resulten de la validación de la resolución del reclamo por parte de la SUGEF, cuando esta no ratifique la resolución denegatoria de la entidad supervisada, deberán realizarse de conformidad a lo dispuesto en la Ley 10889.

Artículo 10. Protocolo de emergencia y atención ante estafas informáticas

Las entidades supervisadas deberán definir e implementar un protocolo de emergencia para atender a los usuarios financieros que informen, ya sea de forma presencial o por cualquier canal de comunicación, que han sido víctimas de una estafa informática o que se encuentran en riesgo inmediato de serlo.

Dicho protocolo deberá estar alineado con los aspectos mínimos de control para prevenir y mitigar la ocurrencia de estafas informáticas en perjuicio de los usuarios financieros dispuestos en el presente reglamento.

El protocolo deberá ser previamente autorizado por la SUGEF, la cual comunicará el contenido de la solicitud de autorización y el canal para su remisión.

La SUGEF verificará, al momento de la presentación de la solicitud de autorización, que la información se encuentre completa. Si la solicitud no contiene la totalidad de los requisitos establecidos, no será aceptada.

Las entidades supervisadas deberán actualizar el protocolo al menos una vez al año y remitirlo a la SUGEF para su autorización. Asimismo, deberán publicar el protocolo en sus páginas web, incorporando al inicio un resumen visual con los principales cambios respecto de versiones anteriores. Asimismo, deberán capacitar de forma periódica a su personal para asegurar la aplicación eficaz, ágil y consistente del protocolo.

Artículo 11. Devolución de montos bajo umbrales predefinidos

Las entidades supervisadas deberán establecer en sus políticas internas, los criterios y umbrales para determinar en qué casos devolverán al usuario financiero el monto sustraído sin necesidad de realizar un análisis detallado, cuando este sea menor al límite previamente establecido por la entidad supervisada, con base en un análisis de costo-beneficio.

Artículo 12. 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.

Asimismo, las entidades supervisadas deberán considerar cualquier otro aspecto que establezca la SUGEF, en complemento de los indicados anteriormente.

Artículo 13. 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 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 14. Protección de la información de los usuarios financieros

Las entidades supervisadas deben implementaren sus canales digitales, al menos, los siguientes mecanismos para proteger 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) Límites de tiempo para que las sesiones iniciadas se cierren automáticamente cuando se detecte inactividad.

e) 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 opciones de configuración disponibles para los usuarios financieros.

Artículo 15. 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 cuentas de fondos; 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.

Las entidades supervisadas deberán conservar evidencia verificable de la fecha, hora, medio y contenido mínimo de las notificaciones remitidas.

Artículo 16. Envío de enlaces en notificaciones

Las entidades supervisadas no deben incluir enlaces acortados en las notificaciones indicadas en el artículo 15 del presente reglamento cuando se envíen por medio de correos electrónicos dirigidos a los usuarios financieros.

Artículo 17. 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 18. 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, particularmente respecto de su funcionalidad para realizar transacciones electrónicas desde sus cuentas de fondos, de forma expedita.

Artículo 19. Reporte, comunicación y registro de cuentas utilizadas en estafas informáticas

Las entidades supervisadas deberán reportar, a la SUGEF y al OIJ, mediante protocolos seguros y conforme a la normativa de protección de datos personales, las cuentas y los nombres de sus titulares, cuando exista una resolución judicial firme que determine

que dichas cuentas fueron utilizadas para recibir fondos provenientes de estafas informáticas

La SUGEF comunicará esta información a las entidades supervisadas, mediante los mecanismos que estime pertinentes y exclusivamente para fines regulatorios y de supervisión, para que estas adopten las medidas correspondientes de monitoreo y debida diligencia.

Artículo 20. Vigencia

El presente reglamento rige a partir de su publicación en el Diario Oficial La Gaceta.

Hazel Valverde Richmond
Superintendente
Superintendencia General de Entidades Financieras

1 vez.—(IN202601125157).

ANEXO 1

PROTOCOLO PARA LA ATENCIÓN DE LOS CASOS EN LOS QUE LOS INTERMEDIARIOS FINANCIEROS SUPERVISADOS RECHACEN RECLAMOS CONFORME A LA LEY 10889

A partir de un análisis de costo – beneficio, las entidades financieras deben establecer un umbral por debajo del cual las reclamaciones de los clientes serán atendidas favorablemente sin la aplicación del procedimiento de investigación previsto en este Reglamento.

Únicamente podrán remitirse a la SUGEF aquellas reclamaciones cuya cuantía supere el umbral definido por la entidad financiera y que, como resultado de la evaluación realizada, no hayan sido acogidas. En la comunicación remitida a la SUGEF deberá indicarse expresamente que el caso excede el umbral definido por la entidad financiera, debiendo indicar en la remisión del caso el umbral definido.

Para los casos de denegatoria presentados a la SUGEF las entidades deberán remitir lo siguiente:

A. El intermediario financiero deberá remitir, por el medio que la SUGEF determine, el oficio de remisión de la denegatoria para cada caso,

debidamente firmado por un representante legal del supervisado, especificando:

- Descripción de la(s) transacción(es) reclamada(s) como estafa informática, incluyendo nombre del cliente, número de identificación, cuentas IBAN involucradas, fecha, hora, monto de la transacción, nombre del comercio (cuando resulte aplicable según la naturaleza de la transacción), medio por el cual se realizó la estafa (tarjeta de débito, sitio web, aplicación móvil u otro mecanismo asociado a la cuenta de fondos afectada) y país en el que se llevó a cabo la transacción.

- Fecha de presentación del reclamo ante el intermediario financiero y fecha de emisión de la resolución denegatoria.

- Resumen ejecutivo con el motivo concreto de la denegatoria, la justificación técnica para ello y la evidencia correspondiente que sustenta dicha decisión, de forma que se identifique claramente la razón por la cual el supervisado considera procedente el rechazo del reclamo conforme a la Ley 10889.

B. La remisión de la denegatoria deberá acompañarse de la siguiente documentación:

<u>De carácter general</u>:

- Copia del reclamo presentado por el usuario ante el intermediario financiero, especificando claramente la fecha de presentación con miras a valorar que la resolución del caso por parte del supervisado está dentro del plazo de preclusión establecido en la ley (120 días naturales, según el Art.5).

- Copia del oficio de denegatoria formal mediante el cual el supervisado resuelve el reclamo recibido, detallando los elementos probatorios que sustenten la denegatoria.

- Copia del informe de investigación interna elaborado por el intermediario financiero.

<u>De carácter técnico</u>:

1. Bitácora que demuestre que se usó el doble factor de autenticación habilitado por el cliente o en su defecto que el cliente no tiene configurado el doble factor de autenticación.

2. Bitácora de notificación de inicio de sesión remitida al cliente.

3. Bitácora de notificación de la transacción realizada por el cliente, sin que el cliente la haya objetado.

4. Indicación de si el día de la transacción se presentó algún incidente de ciberseguridad:

   a) En caso negativo, se debe remitir la bitácora de registro de incidentes.

   b) En caso positivo, se debe remitir el reporte de análisis y atención del incidente de ciberseguridad que demuestre que no está relacionado con la estafa informática aludida.

5. Otras consideraciones:

   a) Si la transacción fue realizada desde un dispositivo de confianza autorizado por el cliente:

      - Bitácora donde se notificó la autorización del registro del dispositivo.

      - Bitácora que demuestre que para la transacción se utilizó el dispositivo de confianza.

   b) Si la transacción fue realizada desde un dispositivo no declarado como de confianza por parte del cliente:

      - Bitácora de que el ingreso se realizó en cumplimiento de los mecanismos de seguridad establecidos.