ENTIDADES VIGILADAS, RESPONSABILIDAD POR FRAUDE EN LA REALIZACIÓN DE OPERACIONES
Concepto 2021030098-005 del 24 de mayo de 2021

Síntesis: De manera correlativa al derecho de recibir productos y servicios con estándares de seguridad y calidad los consumidores financieros deben adoptar buenas prácticas de protección propia, como por ejemplo instalar los programas o usar los mecanismos de seguridad puestos a su disposición por la entidad vigilada para el uso de los canales transaccionales. No obstante, la negativa de los consumidores financieros a implementar tales medidas no releva, por ese solo hecho, a los establecimientos de crédito de la responsabilidad que les pueda asistir por el fraude sobre los recursos de sus cuentahabientes, salvo que demuestren que dicha situación se originó por la culpa exclusiva de estos últimos.

«(…) comunicación mediante la cual formula varias inquietudes que serán atendidas en el mismo orden planteado, agrupando las que tengan un objeto común.

1. **¿Los establecimientos bancarios tienen la potestad de obligar a los usuarios a instalar filtros antifraudes en sus computadores de uso personal?**

Sobre el particular, nos permitimos informarle que, conforme a lo ordenado en los artículos 3 (letra a) y 7 (letra b) de la Ley 1328 de 2009, las entidades vigiladas por la Superintendencia Financiera tienen la obligación legal de emplear adecuados estándares de seguridad y calidad en la prestación de sus servicios a través de los distintos canales de distribución disponibles, con sujeción a las instrucciones impartidas por este Supervisor sobre la materia.

En ese orden, aquellas se encuentran llamadas a observar las prescripciones del Capítulo I, Titulo II, Parte I de la Circular Externa 29 de 2014 (Circular Básica Jurídica, en adelante CBJ), especialmente, los requerimientos fijados en los siguientes subnumerales para el ofrecimiento a los consumidores financieros de la realización de operaciones por Internet:

> 2.3.4.9.1. Implementar los algoritmos y **protocolos necesarios para brindar una comunicación segura.**
>
> 2.3.4.9.2. Realizar como mínimo 2 veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, debe realizarse una prueba adicional.
>
> 2.3.4.9.3. **Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión.**
>
> 2.3.4.9.4. Establecer el tiempo máximo de inactividad, después del cual se debe dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
>
> 2.3.4.9.5. Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.

2.3.4.9.6. Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

2.3.4.9.7. Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.

2.3.4.9.8. Las entidades que permitan realizar operaciones monetarias por este canal deben ofrecer a sus clientes mecanismos fuertes de autenticación. (Se resalta).

De otra parte, es preciso anotar que en materia de seguridad de la información y gestión de la ciberseguridad tales entidades deben atender los requerimientos mínimos señalados en el Capítulo V, Titulo IV, Parte I de la CBJ, entre los cuales para efectos de la prevención de incidentes se encuentra el de informar a los consumidores financieros "sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad" (subnumeral 4.1.11.).

Bajo este marco normativo, se advierte que una medida tendiente a prevenir que los consumidores financieros de un banco sean objeto de conductas o hechos que pongan en riesgo la seguridad de su información cuando hacen uso de sus canales transaccionales, podría consistir, precisamente, en poner a disposición de sus clientes programas antifraudes para ser instalados en los equipos desde los cuales estos acceden al respectivo portal bancario.

Es de anotar que las entidades vigiladas tienen el deber legal de dar a conocer a los consumidores financieros entre otra información concerniente a sus derechos y obligaciones, la relativa a las restricciones y requisitos aplicables en los canales de distribución (por ejemplo: mecanismos de seguridad a implementar, montos máximos y mínimos, operaciones o transacciones restringidas y preinscripciones)[1].

Sin perjuicio de lo anterior, es importante indicar que, de manera correlativa al derecho de recibir "productos y servicios con estándares de seguridad y calidad"[2], la Ley 1328 de 2009 dispone que los consumidores financieros deben adoptar buenas prácticas de protección propia, una de las cuales consiste, precisamente, en "Observar las instrucciones y recomendaciones que imparta la entidad vigilada sobre el manejo de productos o servicios financieros"[3].

2. En el evento en que el usuario se niegue a instalarlos "¿puede la entidad financiera o bancaria exonerarse y trasladar la responsabilidad al usuario por algún fraude en su cuenta bancaria?"

Al respecto, es de mencionar que la Ley 1328 de 2009 dispone que el no ejercicio de las prácticas de protección propia por parte de los consumidores financieros no exime a las entidades vigiladas de las obligaciones especiales consagradas en dicho régimen (entre ellas, la de entregar los productos o servicios ofrecidos en condiciones de seguridad y calidad) ni de la responsabilidad que les sea imputable por su incumplimiento.

Adicionalmente, cabe resaltar que el artículo 11 de la citada ley prohíbe que en los contratos de adhesión se incorporen estipulaciones contractuales que exoneren, atenúen o limiten la responsabilidad de las entidades y que puedan ocasionar perjuicios al consumidor financiero. Como ejemplo de tales cláusulas, esta Superintendencia, en ejercicio de la facultad legal que le atribuye la letra e del mismo artículo, señaló[4], entre otras, las siguientes:

6.1.4.1. Las que exoneran de toda responsabilidad a las entidades vigiladas en caso de pérdida o hurto de instrumentos, títulos o claves y limitan el derecho del consumidor financiero de demostrar que efectivamente la entidad vigilada incurrió en dolo o culpa.

6.1.4.2. Sin perjuicio de los deberes de custodia y diligencia del consumidor financiero, las que imponen que este asuma de manera anticipada toda la responsabilidad derivada del uso de los diferentes instrumentos o claves para la realización de operaciones (tarjetas

[1] Artículo 9 de la Ley 1328 de 2019 y numeral 3 del Capítulo I, Titulo III, Parte I de la CBJ.
[2] Letra a, artículo 5 de la Ley 1328 de 2009.
[3] Letra c, artículo 6 ibídem.
[4] Capítulo I, Título III, Parte I de la CBJ.

débito, crédito, talonarios, dispositivos móviles, títulos, entre otros), así como por cualquier falsedad, adulteración, extravío o uso indebido que de ellos se haga por un tercero.

6.1.4.3. Las que establecen que la entidad vigilada no será responsable por los retiros realizados con documentación adulterada, falsificada o indebidamente diligenciada, cuando la entidad vigilada no haya dispuesto de mecanismos idóneos para verificar adulteraciones o falsificaciones a dichos documentos o, cuando habiendo dispuesto de ellos, las adulteraciones o falsificaciones eran notorias.

6.1.4.4. Las que establezcan que la entidad vigilada no es responsable respecto de los perjuicios o daños derivados de virus, equipos o programas inadecuados o fraudulentos que puedan afectar la confidencialidad o integridad de la información administrada por la entidad.

Conforme al marco normativo expuesto, es dable deducir que la negativa de los consumidores financieros a instalar los programas o usar los mecanismos de seguridad puestos a su disposición para el uso de los canales transaccionales no releva, **por ese solo hecho**, a tales entidades de la responsabilidad que les pueda asistir por el fraude sobre los recursos de sus cuentahabientes.

De otra parte, es de agregar que la Sala de Casación Civil de la Corte Suprema de Justicia manifestó en Sentencia SC 5176-2020 del 18 de diciembre de 2020 (M.P. Luis Alonso Rico Puerta) que **la aplicación del régimen de responsabilidad objetiva en la actividad financiera no implica *per se* una responsabilidad automática de las entidades**, dado que se requiere demostrar que el hecho dañoso es atribuible a la conducta del agente, y **aquellas pueden exonerarse** de la carga indemnizatoria que se les endilga cuando **prueben** que las circunstancias que originaron el daño obedecieron a causas que no les resultan imputables, concretamente a la **"culpa exclusiva de la víctima"**, es decir del depositario.

Ahora, dado que la determinación de la responsabilidad civil es un asunto de competencia de los jueces de la República, la Corte precisó que aquel que asuma el conocimiento del caso respectivo será el encargado de sopesar las circunstancias particulares del mismo, incluida la relevancia jurídica de las causas de exoneración que aduzca la institución financiera, para establecer de esa manera el antecedente determinante en la producción del daño, y, consecuentemente, si es el establecimiento bancario, el consumidor financiero o ambos los que deban asumir las consecuencias del mismo.

En ese orden, por considerar que puede resultar de su interés, le informamos que en nuestra página web[5] se encuentra disponible para consulta del público la jurisprudencia emitida por la Delegatura para Funciones Jurisdiccionales, incluidos los fallos relacionados con la responsabilidad contractual por la ocurrencia de fraudes electrónicos sobre cuentas de ahorro en eventos en que el consumidor financiero ha desatendido recomendaciones de seguridad impartidas por la institución financiera, entre los cuales se resaltan las decisiones con número de radicado 2017034137 del 14 de marzo de 2018 y 2018070566 del 26 de febrero de 2019.

3. **"¿Puede la entidad bancaria negar el acceso a la sucursal virtual y a realizar transacciones si el usuario no descarga el programa?"**
4. **"¿Qué pasa con las personas que no tienen acceso a un computador personal para instalar este tipo de programas o qué pasa con las personas que teniendo computador personal, no tienen capacidad en el mismo para instalarlos, no pueden tener acceso a la virtualidad del sistema?"**

Conforme a lo señalado de modo precedente, entre las obligaciones especiales de las entidades vigiladas se encuentran la de suministrar a los consumidores financieros información comprensible, transparente, clara, veraz y oportuna acerca de sus productos y servicios, así como la de entregarlos o suministrarlos en las condiciones informadas, ofrecidas o pactadas con los clientes y bajo adecuados estándares de seguridad y calidad (letras b y c del artículo 7 de la Ley 1328 de 2009).

[5] www.superfinanciera.gov.co, en la ruta: Inicio/Consumidor Financiero/Funciones jurisdiccionales/Jurisprudencia Superintendencia Financiera de Colombia.

En virtud de la primera obligación referida, dichas instituciones deben informar a los consumidores financieros acerca de las características y condiciones de los productos y servicios, las medidas para el manejo seguro de los mismos, sus derechos y obligaciones, y las consecuencias derivadas del incumplimiento del contrato (artículo 9 de la Ley 1328 de 2009). Adicionalmente, las mismas están obligadas a dar a conocer a los clientes los canales de prestación de servicios habilitados para la realización de operaciones, las medidas de seguridad que deben adoptar para su uso, así como las demás condiciones y restricciones a las que se encuentran sujetos[6].

Por su parte, conforme con la segunda obligación mencionada, las entidades vigiladas deben observar las instrucciones generales y especiales (por tipo de canal de distribución de servicios) que en materia de seguridad y calidad ha impartido este Organismo, una de las cuales consiste en: "Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten" así como las medidas operativas y de seguridad para la reactivación de los mismos[7].

De acuerdo a lo expuesto, es de concluir que se requiere el examen de las estipulaciones contractuales que rigen la relación entre las entidades vigiladas y los consumidores financieros con el objetivo de esclarecer si la negativa en permitir el acceso a la sucursal virtual cuando el cliente no instala un programa antifraude se encuentra pactada en dicho contrato por las partes y la misma fue informada previamente al consumidor financiero.

No obstante, si el consumidor financiero se considera afectado con la actuación de una entidad vigilada puede formular la queja ante el Defensor del Consumidor Financiero de la respectiva institución o, si lo estima pertinente, puede interponerla ante esta Superintendencia, a fin de que a través de la correspondiente actuación administrativa particular y el análisis de los elementos probatorios se evalúe el proceder de la institución correspondiente, se determine si hay lugar a adoptar alguna medida respecto de la misma en los términos previstos en la ley.

(…).»

[6] Subnumerales 3.2.4.3, 3.2.4.4, y 3.2.6.11 del Capítulo I, Titulo III, Parte I de la CBJ.
[7] Subnumerales 2.3.3.1.12 y 2.3.3.2.8 del Capítulo I, Título II, Parte I de la CBJ.