RIESGO DE CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÒN, REQUERIMIENTOS MÌNIMOS
Concepto 2019081599-002 del 26 de julio de 2019

Síntesis: *Las entidades vigiladas están obligadas a contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente los riesgos de la seguridad de la información y la ciberseguridad y como mínimo atender las instrucciones contenidas en el Capítulo XXIII de la Circular Básica Contable y Financiera, Capítulo V, Título IV y Capítulo I, Título II de la Parte I de la Circular Básica Jurídica.*

«(…) comunicación mediante la cual consulta acerca de las medidas de seguridad y obligaciones que deben adoptar los bancos frente a los riesgos presentados en las operaciones realizadas por medio cibernético.

En primer lugar, es pertinente mencionar que a esta Autoridad no le está dado, por vía de respuesta a una consulta general, dirimir las controversias particulares que se suscitan entre los consumidores financieros y las entidades vigiladas, ni el alcance de la responsabilidad en el caso descrito en su comunicación, aspecto que corresponde dirimir directamente a las partes interesadas, o en su defecto, al Juez de la República ante el cual se ventile el respectivo asunto.

Precisado lo anterior, debemos indicar que de acuerdo con lo expresado en la jurisprudencia[1], los bancos en ejercicio de los deberes de custodia y cuidado sobre los recursos que les han sido confiados por sus clientes, se encuentran en la obligación de adoptar las medidas, precauciones, cuidados y/o exigencias que consideren necesarios e imprescindibles para la salvaguarda de los mismos. Además, por ser expertos en la intermediación financiera estos deben obrar en forma cuidadosa y precavida con fundamento en sus conocimientos especializados y en su experticia sobre la materia, a fin de que no se llegue a presentar alguna situación de riesgo que incida en el patrimonio de los consumidores financieros.

Adicionalmente, es de anotar que en desarrollo del principio de la debida diligencia consagrado en el Régimen de Protección al Consumidor Financiero (Ley 1328 de 2009, Título I), los consumidores financieros tienen el derecho a recibir de parte de las entidades vigiladas productos y servicios con estándares de seguridad y calidad (artículo 5, letra a) y las entidades vigiladas deberán observar las instrucciones que imparta la Superintendencia Financiera en materia de seguridad y calidad en los distintos canales de distribución de servicios financieros (artículo 3, letra a).

---

[1] Corte Suprema de Justicia, Sala de Casación Civil, mediante la Sentencia SC18614-2016 del 19 de diciembre de 2016, con ponencia del Magistrado Dr. Ariel Salazar Ramirez

En ese contexto, esta Superintendencia en desarrollo de sus facultades legales[2] impartió instrucciones a sus entidades vigiladas en materia de administración de riesgos y requerimientos mínimos de seguridad y calidad de la información que las mismas deben implementar con el fin de velar por la protección de las operaciones realizadas en los diferentes canales e instrumentos de prestación de servicios financieros, las cuales se describen a continuación:

- **SARO - Sistema de Administración de Riesgo Operativo**

El Capítulo XXIII de la Circular Básica Contable y Financiera (Circular Externa 100 de 1995) contiene las instrucciones relativas al Sistema de Administración de Riesgo Operativo (SARO), definido como el: "Conjunto de elementos tales como **políticas, procedimientos**, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas **identifican, miden, controlan y monitorean el riesgo operativo**", mediante el cual se busca obtener una efectiva administración del mencionado.

- **Requerimientos mínimos de seguridad y calidad para la realización de operaciones**

En la Parte I, Título II, Capítulo I "Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros", de la Circular Básica Jurídica (Circular Externa 29 de 2014) se encuentran señaladas las instrucciones en materia de seguridad y calidad de la información que se maneja a través de canales e instrumentos para la realización de operaciones. Las entidades deben implementar los requerimientos exigidos, atendiendo la naturaleza, objeto social y demás características particulares de su actividad, incluyendo en sus políticas y procedimientos, las definiciones, criterios y requerimientos mínimos allí establecidos.

Es así como, en desarrollo de sus servicios y dando cumplimiento a las instrucciones impartidas en la citada circular nuestras vigiladas deben expresamente:

> 2.3.3.1.12. **Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten** o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos. (Negrilla fuera del texto).

De igual modo, el mismo aparte del instructivo establece requerimientos especiales para cada uno de los canales de prestación de servicios financieros que las entidades decidan utilizar, previstos de la siguiente manera: oficinas (numeral 2.3.4.1), cajeros automáticos (numeral 2.3.4.2), receptores de cheques (numeral 2.3.4.3), receptores de dinero en efectivo (numeral 2.3.4.4.), POS (numeral 2.3.4.5), sistemas de audio respuesta (numeral 2.3.4.6), centros de atención telefónica (numeral 2.3.4.7), sistemas de acceso remoto para clientes (numeral 2.3.4.8), internet (numeral 2.3.4.9), Prestación de servicios a través de nuevos canales (numeral 2.3.4.10), Banca Móvil. (numeral 2.3.4.11), Obligaciones específicas para tarjetas débito y crédito (numeral 2.3.4.12) y Operaciones por medio de códigos QR (numeral 2.3.4.13).

- **Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad**

Teniendo en cuenta que el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos, entre otros elementos, han derivado en

[2] Numeral 6, artículo 11.2.1.4.2 del Decreto 2555 de 2010.

un incremento de la exposición a riesgos cibernéticos, esta Autoridad mediante la Circular Externa 007 de 2018, incorporada en el Capítulo V, Título IV, Parte I, "Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad" de la Circular Básica Jurídica, impartió instrucciones complementarias a aquellas relacionadas con la administración de riesgos operativos y la seguridad en la información.

En las mencionadas instrucciones se precisó la obligación de las entidades sometidas a la inspección y vigilancia de esta Superintendencia de contar con **políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad**. Con este objetivo, dichas entidades deben adoptar, como mínimo, las medidas y las etapas de: i) Prevención, ii) Protección y detección, iii) Respuesta y comunicación, y iv) Recuperación y aprendizaje, que allí se relacionan.

Con fundamento en lo expuesto, si el consumidor financiero considera que el establecimiento de crédito desatendió las normas e instrucciones antes mencionadas, se encuentra en libertad de interponer una queja ante el Defensor del Consumidor Financiero de la entidad con la cual se contrató el respectivo producto, o en su defecto, ante esta Superintendencia, a efectos de que en el marco de la correspondiente investigación administrativa evalúe el proceder de dicha vigilada y determine si hay lugar a adoptar alguna medida respecto de la misma en los términos previstos en la ley.

Para la presentación de quejas puede hacer uso de cualquiera de los siguientes canales que esta Entidad ha dispuesto para ello: e-mail super@superfinanciera.gov.co; portal web www.superfinanciera.gov.co, haciendo uso del aplicativo denominado: "Formule su Queja", que se encuentra en la ruta: Inicio/Consumidor financiero/Información general/Quejas contra entidades vigiladas/Quejas de los Consumidores Financieros - Cómo presentar una queja; o, enviarla a nuestras oficinas ubicadas en la Calle 7 No. 4-49 de la ciudad de Bogotá.

Por último, si el consumidor financiero lo estima del caso, puede ejercer la acción judicial de protección al consumidor financiero, conforme a la cual estos podrán a su elección someter a conocimiento de este Organismo "los asuntos contenciosos que se susciten entre ellos y las entidades vigiladas sobre las materias a que se refiere el presente artículo para que sean fallados en derecho, con carácter definitivo y con las facultades propias de un juez", de acuerdo con lo previsto en el artículo 57 de la Ley 1480 de 2011 (Estatuto del Consumidor), que atribuye facultades jurisdiccionales a la Superintendencia Financiera para conocer las controversias entre sus entidades vigiladas y los consumidores financieros "relacionadas exclusivamente con la ejecución y el cumplimiento de las obligaciones contractuales que asuman con ocasión de la actividad financiera, bursátil y aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos captados del público".

El texto completo de las normas e instrucciones citadas, se encuentra disponible para consulta del público en nuestro portal web antes citado, siguiendo el enlace: Inicio/Normativa/Normativa General.

(…).»

Este documento fue tomado directamente de la página oficial de la entidad que lo emitió.