SUPERINTENDENCIA FINANCIERA

SEGURIDAD EN TRANSACCIONES BANCARIAS, CONFIDENCIALIDAD, CÓDIGO OTP

Concepto 2018085479-002 del 17 de julio de 2018

Síntesis: *El código "OTP (One Time Password), en combinación con un segundo factor de autenticación", es uno de los mecanismos fuertes de autenticación previsto en el numeral 2.2.6.3. del Capítulo I, Título II de la Parte I de la Circular Externa 029 de 2014 (Circular Básica Jurídica), consistente en un código temporal que llega al celular del consumidor financiero a través de mensaje de texto SMS, para que de manera segura pueda realizar sus operaciones bancarias (retiros, consultas, pagos y transferencias) a través de Internet o de la aplicación para teléfonos móviles (APP). El código OTP que es enviado por MSM o correos electrónicos, no es propiamente una "información confidencial", conforme la definición anotada en el numeral 4. anterior, razón por la cual se considera que su envío no debe ser cifrado; máxime que solo sirve para realizar una sola operación y que su durabilidad es de contados minutos*

«(…) correo electrónico relacionada con el numeral 2.3.3.1.3 de la Circular Externa 008 de 2018, mediante la cual consulta si este numeral *"(…) implica que por ejemplo, los códigos OTP enviados por SMS o mail para que el cliente pueda ejecutar transacciones, deben enviarse cifrados? Adicionalmente, (sic) hay alguna condición respecto al algoritmo de cifrado?"*

Sobre el particular, proceden las siguientes consideraciones:

En primer lugar, es preciso indicar que esta Superintendencia, en desarrollo de sus facultades legales, ha expedido varios instructivos, que propenden por la

seguridad y calidad para la realización de operaciones, entre los cuales se encuentra la Circular Externa 052 de 2007, modificada por las Circulares Externas 022 de 2010 y 042 de 2012, incorporadas en el Capítulo XII, Título Primero de la Circular Básica Jurídica (Circular Externa 007 de 1996), y en la Parte I, Título II, Capítulo I de la Circular Externa 029 de 2014, mediante la cual se realizó la reexpedición de la Circular Básica Jurídica, modificada por la Circular Externa 008 de 2018.

La Circular Externa la Circular Externa 008 de junio 5 de 2018, es la instrucción más reciente, mediante la cual se realizaron, entre otros, algunas modificaciones a los subnumerales 1.2.2.1.2.7, 1.3., 2.1., 2.3.3.1.3., 2.3.3.1.12, 2.3.3.1.16, 2.3.4.1., 2.3.4.1.3., 2.3.4.2.1., 2.3.4.5.3., 2.3.4.7.5., 2.3.4.9.4., 2.3.4.11., 2.3.4.11.2., y 2.3.4.12.11. de la Parte I, Título II, Capítulo I de la Circular Básica Jurídica, en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones, relacionados con los canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros y realización de operaciones, modificaciones que rigen a partir del **1º de diciembre de 2018**.

El numeral 2.3.3.1.3 de la Circular Externa 008 de 2018, por el que pregunta establece que las entidades sujetas a su aplicación deben: *"Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico,* ***mensajería instantánea o cualquier otra modalidad de comunicación electrónica,*** *ésta debe estar cifrada".*

Ahora bien, para absolver su inquietud debemos acudir a la definición de *"información confidencial"* que traía la Circula Externa 052 de 2007, según la cual *"(…) se considerará confidencial para efectos de la aplicación del presente Capítulo toda aquella información amparada por la reserva bancaria V.gr. número de cuenta; número de identificación personal (PIN); número de tarjeta física; información sobre depósitos o inversiones de cualquier tipo, créditos, saldos, cupos y movimientos de cuenta, siempre que vayan acompañados del nombre o número de identificación del cliente".*

Así mismo, el código *"OTP (One Time Password), en combinación con un segundo factor de autenticación"*, es uno de los mecanismos fuertes de autenticación previsto en el numeral 2.2.6.3. del Capítulo I, Título II de la Parte I de la Circular Externa 029 de 2014 (Circular Básica Jurídica), consistente en un **código temporal** que llega al celular del consumidor financiero a través de mensaje de texto SMS, para que de manera segura pueda realizar sus operaciones bancarias (retiros, consultas, pagos y transferencias) a través de Internet o de la aplicación para teléfonos móviles (APP). Este código solo tiene un único uso y vigencia de unos pocos minutos (lo que defina cada entidad); no sirve

para realizar otras operaciones posteriores, aunque éstas se realicen el mismo día, por lo que cada operación necesita su propio OTP.

De acuerdo con lo anterior, el código OTP que es enviado por MSM o correos electrónicos, no es propiamente una *"información confidencial"*, conforme la definición anotada en el numeral 4. anterior, razón por la cual se considera que su envío no debe ser cifrado; máxime que solo sirve para realizar una sola operación y que su durabilidad es de contados minutos.

De otra parte, respecto de su pregunta de si *"(…) hay alguna condición respecto al algoritmo cifrado",* consideramos pertinente señalar la definición que trae el numeral 2.2.2. del Capítulo I, Título II de la Parte I de la Circula Externa 029 de 2014 –Circular Básica Jurídica-, que señala lo siguiente: *"2.2.2. Cifrado fuerte: Técnicas de codificación para protección de la información que utilizan algoritmos reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES o AES."*

Si bien la Superintendencia Financiera en desarrollo de sus facultades legales, imparte instrucciones sobre la forma como las entidades vigiladas deben acatar las disposiciones que regulan su actividad, fijando criterios técnicos y jurídicos que faciliten su observancia, en cumplimiento del principio de neutralidad tecnológica, este Organismo no determina el cómo las instituciones financieras implementan el cumplimiento de los distintos requerimientos señalados en el Capítulo I, Título II de la Parte I de la Circular Básica Jurídica, en razón a la autonomía de la voluntad de que gozan las entidades vigiladas para administrar los diferentes riesgos propios de su objeto social, estructura, tamaño y según el tipo de entidad definido en el Estatuto Orgánico del Sistema Financiero y demás disposiciones que lo modifiquen o adicionen.

(…).»

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