SERVICIOS EN LA NUBE, SEGURIDAD Y CALIDAD DE LA INFORMACIÓN
Concepto 2017059546-001 del 20 de junio de 2017

Síntesis: *Esta Superintendencia ha impartido a sus vigiladas instrucciones en materia de seguridad y calidad de la información, normas de control interno para la gestión de la tecnología, así como las reglas relativas a la administración del riesgo operativo SARO, entre otras, que son de obligatorio cumplimiento por parte de las entidades vigiladas por esta Superintendencia objeto de su aplicación, aspectos regulados en la Circular Externa 029 de 2014 (Circular Básica Jurídica) y en la Circular Externa 100 de 1995 de esta Superintendencia (Circular Básica Contable y Financiera) y que tienen plena aplicación frente a los servicios de computación en la nube implementados por las entidades vigiladas*.

«(…) correo electrónico mediante el cual solicita le informemos sobre *"(…) la normatividad a nivel Super financiera (sic) sobre el tratamiento de la información bancaria en la nube o cloud computing a nivel Bancos".*

Sobre el particular, proceden las siguientes consideraciones:

1. En primer lugar, es preciso indicar que en las instrucciones que hasta la fecha ha expedido esta Superintendencia a las entidades objeto de vigilancia, no se ha impartido ninguna en particular sobre el uso de "*cloud computing a nivel Bancos"*. Sin embargo, esta Superintendencia se encuentra trabajando en un proyecto de Circular que imparte una serie de instrucciones y establece los requerimientos y obligaciones que las entidades vigiladas deben cumplir para implementar los servicios de computación en la nube.

2. Sin perjuicio de lo anterior, es importante señalar que esta Superintendencia ha impartido a sus vigiladas instrucciones en materia de seguridad y calidad de la información, normas de control interno para la gestión de la tecnología, así como las reglas relativas a la administración del riesgo operativo SARO, entre otras, que son de obligatorio cumplimiento por parte de las entidades vigiladas por esta Superintendencia objeto de su aplicación, aspectos regulados en la Circular Externa 029 de 2014 (Circular Básica Jurídica) y en la Circular Externa 100 de 1995 de esta Superintendencia (Circular Básica Contable y Financiera) y que tienen plena aplicación frente a los servicios de computación en la nube implementados por las entidades vigiladas, instructivos que están disponibles para el público y pueden ser consultadas a través de nuestra página Web: www.superfinanciera.gov.co, siguiendo esta ruta: Normativa / Normativa General.

3. En efecto, la Circular Externa 029 de 2014, es la instrucción más reciente, mediante la cual se realizó la reexpedición de la Circular Básica Jurídica, la cual incorporó en el numeral 2 del Capítulo I, Título II de la Parte I, en materia de seguridad y calidad una serie de requerimientos de carácter general previstos en el numeral 2.3.3. del citado Capítulo, Título y Parte; y otras de carácter particular para cada uno de los canales de

distribución de servicios financieros, entre los cuales se encuentra el canal internet señalado en el numeral 2.3.4.9, y estipula en el numeral 2.3.6, las exigencias que aplican para las entidades vigiladas que contraten bajo la modalidad de outsourcing, que también resultan aplicables para las entidades que procesen en la nube; al igual que las normas de control interno para la gestión de la tecnología, entre las cuales se encuentran las exigencias relacionadas con la Administración de los datos, incorporadas en el numeral 5.2.1.15 y s.s. del Capítulo IV, Título I de la Parte I de la misma Circular. Por su parte, las *"Reglas Relativas a la Administración del Riesgo Operativo"* se encuentran incorporadas en el Capítulo XXIII de la Circular Básica Contable y Financiera, a partir de las cuales las entidades que vayan a operar a través de la nube, deben identificar, medir, controlar y monitorear eficazmente los riesgos de las actividades tercerizadas (outsourcing).

4. Ahora bien, no sobra advertir, que al hablar de *"el tratamiento de la información bancaria en la nube o cloud computing a nivel Bancos",* deben considerarse las exigencias previstas para la transferencia de datos internacionales, sobre la cual es preciso indicar lo siguiente:

- La Ley 1581 de 2012, estableció en su artículo 26, algunas previsiones frente a la transferencia internacional de datos a responsables y/o encargados que se encuentren dentro o fuera del territorio nacional, disposiciones que se aplican para todos los datos personales que sean objeto de transferencia y/o transmisión internacional, incluyendo **los contemplados en la Ley 1266**, por expresa remisión del parágrafo 2. del precitado artículo 26. (la negrilla es nuestra).

  En esa medida, la información bancaria sí puede salir del País, siempre y cuando se cumpla con los requisitos establecidos en la Ley 1581 de 2012, en lo dispuesto en el artículo 2.2.2.25.5.1. del Decreto 1074 de 2015 , así como en los requisitos exigidos por la Superintendencia de Industria y Comercio.

- Si se pretende realizar transmisión internacional de datos personales se debe contar con la autorización del titular de los datos o con un contrato de transmisión que se sujete a lo dispuesto en el artículo 2.2.2.25.5.2. del Decreto 1074 de 2015 y en ausencia del mismo debe solicitar la declaración de conformidad.

- El Parágrafo 1. del artículo 26 de la Ley 1581 de 2012, delegó en la Superintendencia de Industria y comercio la facultad de proferir la declaración de conformidad relativa la transferencia internacional de datos personales.

Teniendo en cuenta que la citada Superintendencia a la fecha no ha fijado los estándares para determinar si un País ofrece un nivel adecuado de protección de datos, para realizar transferencias internacionales de datos personales, se debe solicitar la respectiva declaración de conformidad a la SIC y aportar los documentos que ese Órgano de Vigilancia y Control exija.

(…).»