Bogotá, 11 de noviembre de 2016

Doctor:
Felipe Alarcón Sierra
Subdirector de Coordinación Normativa
Superintendencia Financiera de Colombia
Calle 7 No. 4 – 49
Bogotá, D.C.

Ref: Comentarios de la Cámara Colombiana de Comercio Electrónico al proyecto de Circular: Por medio de la cual se adiciona el "*CAPÍTULO XXIX: REGLAS RELATIVAS PARA EL PROCESAMIENTO DE INFORMACIÓN EN CENTROS DE PROCESAMIENTO DE DATOS, CENTROS ALTERNOS DE PROCESAMIENTO DE DATOS Y CENTROS DE SERVICIOS COMPARTIDOS*".

Estimado Doctor:

En nombre de la Cámara Colombiana De Comercio Electrónico (en adelante, la CCCE) reciba un cordial saludo y un especial agradecimiento por permitirnos presentar comentarios al proyecto de circular de la referencia.

La Cámara Colombiana de Comercio Electrónico es una institución sin ánimo de lucro que agremia a más de trescientas empresas colombianas de comercio electrónico e Internet, y tiene la misión de difundir el desarrollo del comercio electrónico y los negocios en Internet como una forma de interacción entre individuos, empresas y gobierno, toda vez que estas herramientas y tecnologías redundan no solo en la calidad de vida de

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

todos los ciudadanos sino que incrementan la productividad en aras de la consolidación de la economía del país.

Internet y los servicios en Cloud son una nueva oportunidad de desarrollo socioeconómico para todas aquellas naciones que no fueran el centro del impulso industrial de siglos anteriores y es imposible minimizar su creciente impacto en la creación de riqueza y puestos de trabajo. Conforme a los últimos estudios de McKinsey & Cía., Internet contribuye en 3,4 puntos promedio de PBI en las economías, explica el 21% del crecimiento del PBI en países desarrollados, y crea 2,6 puestos de trabajo por cada uno que elimina [1].

En primera medida, nos permitimos reconocer los esfuerzos de la Superintendencia Financiera en la estructuración de este proyecto normativo, que hemos analizado con detenimiento, y por lo cual realizamos los siguientes comentarios con el fin de enriquecer su labor.

Consideraciones generales

Son varios los puntos y aspectos que preocupan a la CCCE en relación con el proyecto de circular. Especialmente, este proyecto de circular puede afectar gravemente el desarrollo de los servicios en Internet y especialmente los servicios de Cloud Computing, ya que establece restricciones no razonables al almacenamiento y procesamiento de datos, pensando en que dicho almacenamiento se hace por medios tradicionales y no mediante servicios de cloud.

Comentarios a los artículos 2.2. y 2.3.

2.2. Centro de Procesamiento de Datos (CPD)

Lugar en donde se concentran los recursos necesarios para el procesamiento de la información de una entidad, independientemente de ser de su propiedad o de un tercero.

2.3 Centro Alterno de Procesamiento de Datos (CAPD)

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Lugar en donde se procesa la información de una entidad cuando no es posible hacerlo en el CPD, independientemente de ser de su propiedad o de un tercero.

(…)"

En primer lugar, es importante determinar con claridad el alcance del proyecto de circular, particularmente en lo referente a las definiciones del CPD (Centro de Procesamiento de Datos) y el CAPD (Centro Alterno de Procesamiento de Datos. Dado que un CPD es un conjunto de una gran cantidad de recursos tecnológicos, y que el lugar de ubicación es sólo uno de sus componentes, respetuosamente solicitamos ampliar la definición de este concepto en el Proyecto de Circular.

Por otra parte, en consonancia con lo que se expresa más adelante en el Proyecto de Circular, solicitamos aclarar que en la definición se debe expresar claramente que el CPD y el CAPD puede estar ubicado tanto en el territorio nacional, como en el extranjero.

Por lo anterior, sugerimos modificar la redacción de la siguiente manera para cada uno de los siguientes artículos:

(…)

2.2. Centro de Procesamiento de Datos (CPD)

Conjunto de recursos necesarios para el procesamiento de la información de una entidad, independientemente de ser de su propiedad o de un tercero, en Colombia o en el exterior.

Siguiendo en línea con el comentario anterior, sugerimos la siguiente redacción para el Centro Alterno de Procesamiento de Datos (CAPD).

2.3. Centro Alterno de Procesamiento de Datos (CAPD)

Lugar en donde se procesa la información de una entidad cuando no es posible hacerlo en el CPD, independientemente de ser de su propiedad o de un tercero, en Colombia o en el exterior.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Comentarios al numeral 3

Con el fin de absolver algunas inquietudes que rutinariamente se presentan en las entidades vigiladas por la Superintendencia Financiera, solicitamos añadir un inciso al final del inciso tercero para señalar expresamente que "*las entidades financieras pueden usar servicios de computación en la nube, prestados desde el territorio nacional o desde el extranjero, para el procesamiento de su información, tanto para procesos misionales y procesos críticos*".

Comentarios al artículo 3.1.1.

3.1.1. Con el propósito de evitar la concentración de riesgo, dentro de los criterios para seleccionar o implementar el CPD o el CAPD, las entidades vigiladas y los operadores de información de la PILA deben considerar si otras entidades que prestan sus servicios en Colombia procesan su información en los mismos CPD y/o CAPD.

3.1. Obligaciones generales

***3.1.4.** Las entidades vigiladas y los operadores de información de la PILA deben contar en Colombia con el personal capacitado y con los recursos necesarios para asumir la administración de los sistemas de información que soportan los procesos misionales y de gestión contable, cuando lo requiera la entidad o la SFC."*

En este artículo se dispone que las entidades vigiladas al seleccionar el CPD o CAPD deben considerar si en ellos procesan su información otras entidades que operen en Colombia, con el propósito de evitar una indebida concentración del riesgo.

Esta provisión desconoce la realidad de los servicios de computación en Internet prestados por compañías serias de tecnología y de Internet. Precisamente, el modelo de computación en Internet tiene dentro de sus características que la información se encuentra almacenada en diferentes servidores con el fin de garantizar el respaldo de la información, así como en servidores espejo que garantizan que la información no se va a perder en caso de verse afectado alguno de los servidores. De esa manera, si varias entidades financieras contrataran con una misma compañía de Internet un CPD o CAPD, no existiría necesariamente una indebida concentración del riesgo. En este punto es esencial garantizar que las entidades financieras

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

contraten los CPD con empresas de Internet que les garanticen el respaldo de la información y servidores espejo en diferentes lugares del mundo, que les otorguen niveles de servicio y seguridad requeridos.

Es de destacar, finalmente, que una instrucción genérica a las entidades financieras de "considerar" si otras entidades usan el mismo centro de procesamiento de datos, para evitar una "indebida concentración del riesgo", sin detallar en qué consiste dicha obligación, genera incertidumbre jurídica al no incluir la definición de lo que se entiende como "concentración indebida del riesgo". Adicionalmente, debe tenerse en cuenta que la lista de clientes de un proveedor constituye información confidencial. Por otra parte, esta disposición insinúa, sin un sustento, que los centros de datos compartidos implican en sí mismo un riesgo superior a otras alternativas de procesamiento. Como se sabe, la seguridad de un centro de datos depende de un conjunto de medidas de seguridad adoptadas para la salvaguarda de la información y no del hecho de que parte de la infraestructura sea usada por distintos clientes.

Consideramos que contar con personal capacitado que puedan soportar el funcionamiento y la administración de los CPD Y CAPD es fundamental para asegurar el correcto funcionamiento de los mismos y garantizar la correcta prestación del servicio en general. Sin embargo, la ubicación de los recursos humanos para la administración de los sistemas de información correspondientes no necesariamente debe ser Colombia, especialmente teniendo en cuenta que los CPD y los CAPD pueden estar ubicados en el extranjero.

En ese orden de ideas, sugerimos modificar la redacción de la siguiente manera:

> *"**3.1. Obligaciones generales***
>
> ***3.1.4.** Las entidades vigiladas y los operadores de información de la PILA deben contar con el personal capacitado y con los recursos necesarios para asumir la administración de los sistemas de información que soportan los procesos misionales y de gestión contable, cuando lo requiera la entidad o la SFC."*

Comentarios al artículo 3.1.6.

3.1. Obligaciones generales

3.1.6. Las entidades vigiladas y los operadores de información de la PILA deben monitorear, en tiempo real y desde Colombia, los equipos servidores, aplicaciones

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

y redes de comunicación del CPD y del CAPD, para realizar o solicitar acciones preventivas o correctivas cuando se requiera.

Este artículo propone monitorear desde Colombia los equipos servidores, aplicaciones y redes de comunicación de CPD y del CAPD para solicitar acciones preventivas o correctivas cuando se requiera. Preocupa que se exija a los proveedores de servicios en Cloud permitir que terceros ajenos a estos servidores puedan monitorearlos, teniendo en cuenta que en dichos servidores y redes de comunicación se almacena y transmite información de terceros que es confidencial. En esa medida, debería especificarse en el proyecto de circular con precisión y certeza cuál es alcance de este monitoreo, y dejarse expreso que dicha facultad de monitoreo no podrá interferir con los derechos contractuales de los usuarios. El monitoreo por terceros puede afectar gravemente la seguridad y confiabilidad de los servicios de Cloud ofrecidos por proveedores.

Comentarios al numeral 3.1.9 (c)

"3.1. Obligaciones generales

3.1.9. *Las entidades vigiladas y los operadores de información de la PILA deben remitir a la SFC, con al menos treinta (30) días de antelación al inicio del procesamiento de su información en un nuevo CPD o CAPD, la siguiente información:*

(…)

(b) Ubicación física del CPD y/o CAPD

(c) *Copia del contrato suscrito con el administrador del CPD y/o CAPD, con sus respectivos anexos, en caso de que aplique.*

(d) Principales características del CPD y/o el CAPD: TIER o cualquier otro estándar reconocido internacionalmente, disponibilidad, seguridad física y electrónica y redundancia de los sistemas de apoyo.

(…)*"*

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Consideramos que la información a la cual se hace alusión en los literales b, c y d del artículo 3.1.9. es confidencial y está protegida en la mayoría de las ocasiones por secretos empresariales en la medida en que está estrechamente relacionada con el funcionamiento y el negocio del proveedor del CPD y/o CAPD. Adicionalmente, es importante tener en cuenta que la mera revelación de la ubicación física de un CPD puede constituir en sí misma una vulneración de prácticas de seguridad establecidas en la industria.

Finalmente, en cuanto al envío de la información, consideramos que: 1) El envío de la información a la Superintendencia Financiera debería estar atado al cambio de proveedor o al cambio de país en el que está almacenada la información y no al cambio del CPD, pues para la entidad financiera no es relevante en realidad la ubicación del CPD o cuál de ellos está usando un proveedor para prestar el servicio, sino cuáles son los requerimientos mínimos de seguridad que debe tener dicho CPD que se usa para procesar la información, requerimientos que pueden no cambiar con el traslado de la información de un CPD a otro; 2) Dicha información no debería remitirse con 30 días de antelación, pues este lapso puede afectar el giro ordinario de los negocios de las entidades vigiladas. Sugerimos que el mismo sea reducido a 5 días.

En virtud de lo anterior, sugerimos modificar la redacción de la siguiente manera:

"3.1. Obligaciones generales

3.1.9. *Las entidades vigiladas y los operadores de información de la PILA deben remitir a la SFC, con al menos cinco (5) días de antelación al inicio del procesamiento de su información con un nuevo proveedor de CPD o CAPD, la siguiente información:*

(…)

~~***Ubicación física del CPD y/o CAPD***~~

~~***(c)*** *Copia del contrato suscrito con el administrador del CPD y/o CAPD, con sus respectivos anexos, en caso de que aplique.*~~

(d) ~~*Principales características del CPD y/o el CAPD: TIER o cualquier otro estándar reconocido internacionalmente, disponibilidad, seguridad física y electrónica y redundancia de los sistemas de apoyo*~~*.*

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

(c) *Las características del CPD y/o el CAPD, necesarias para demostrar el cumplimiento de la presente Circular.*

(…)"

Comentarios al numeral 3.1.9 (e)

"3.1. Obligaciones generales

3.1.9. *Las entidades vigiladas y los operadores de información de la PILA deben remitir a la SFC, con al menos treinta (30) días de antelación al inicio del procesamiento de su información en un nuevo CPD o CAPD, la siguiente información:*

(…)

(e) *Certificaciones otorgadas al CPD y/o CAP, en caso en que aplique.*

(…)"

Al respecto, consideramos que las certificaciones que se deben tener en cuenta no solo son aquellas otorgadas directamente al CPD y/o al CAPD sino también aquellas con las que cuenta el proveedor del servicio. Lo anterior, teniendo en cuenta que, más allá de los recursos que conforman el centro de datos, es el proveedor quien garantiza la seguridad del procesamiento de la información y realiza la administración de los centros mismos. En ese orden de ideas, el prestador del servicio tiene un rol fundamental en la protección de la información que se maneja en los centros, razón por la cual las cualidades y calidades del mismo deben ser tenidas en cuenta a la hora de evaluar el procesamiento de datos en CDP y /o CAPD.

Por tales motivos, sugerimos modificar la redacción de la siguiente manera:

"*3.1. Obligaciones generales*

3.1.9. *Las entidades vigiladas y los operadores de información de la PILA deben remitir a la SFC, con al menos treinta (30) días de antelación al inicio del procesamiento de su información en un nuevo CPD o CAPD, la siguiente información:*

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

(…)

(e) *Certificaciones otorgadas al CPD y/o CAPD o al proveedor del servicio, en caso en que aplique.*

(…)"

Comentarios al artículo 3.2.2.

(…)

3.2.2. *El CPD y/o el CAPD deben contar con un sistema de administración de riesgos operativos que contemple las siguientes etapas: identificación, medición, control y monitoreo de los riesgos, al igual que con un sistema de gestión de seguridad de la información, para lo cual se podrá tomar como referencia el estándar ISO 27001, el estándar complementario ISO 27018, e ISO 19086 para niveles de servicios.*

Este artículo propone que los CPD o CAPD cuenten con un sistema de administración de riesgos operativos. La Superfinanciera no debería imponer estas condiciones a los CPD o CAPD, ya que estas pueden ser entidades que se encuentran fuera del país y que tienen sus propios sistemas de administración de riesgos. Por lo tanto, en razón al principio de neutralidad tecnológica de la Ley 1341 de 2009 (art. 2.6), no deben aplicarse estándares que no permitan la utilización de tecnologías de información novedosas en los CPD y CAPD.

Debería, en cambio, indicarse que las entidades vigiladas contraten CPD o CAPD que tengan sistemas de administración de riesgos operativos propios y que garanticen la seguridad de la información.

Consideramos que aunado al estándar ISO 27001 se debe hacer expresa referencia a la extensión ISO 27018 del estándar, el cual se refiere específicamente a las prácticas de protección de datos en servicios de computación en la nube pública, *e ISO 19086 para niveles de servicios*. Esto es de especial importancia en el sector, teniendo en cuenta que la información que manejan las entidades vigiladas por la SFC en algunas ocasiones, es considerada como datos sensibles.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

En consideración a lo antes expuesto, solicitamos añadir los estándares ISO 27018, e ISO 19086 en el numeral 3.2.2. El texto propuesto es el siguiente:

"3.2. Requerimientos mínimos para el CPD y CPAD

(…)

3.2.2. *El CPD y/o el CAPD deben contar con un sistema de administración de riesgos operativos que contemple las siguientes etapas: identificación, medición, control y monitoreo de los incidentes, al igual que con un sistema de gestión de seguridad de la información, para lo cual se podrá tomar como referencia los estándares ISO 2700, ISO 27018, ISO 19086.*

(…)"

Comentarios a los artículos 3.2.3. y 3.2.4.

"3.2. Requerimientos mínimos para el CPD y CAPD

(…)

3.2.3. *El CDP de las entidades relacionadas en el inciso segundo del numeral 3 debe tomar como referencia los lineamientos establecidos en la norma técnica ANSI/TIA 942, TIER 3 o superior o cualquier otro estándar reconocido internacionalmente que brinde, al menos, el mismo nivel de disponibilidad."*

El uso del estándar ANSI TIA 942 que se plantea como referencia para los CPD de las entidades financieras está orientado a datacenters locales y no hacia la prestación de servicios en la nube. Los grandes proveedores de computación en la nube o de servicios en Internet no cumplen o no están certificados con este requerimiento. La misma TIA ha reconocido que deben revisarse lo estándares TIA para que sean interoperativos con Cloud Computing[2]. Por lo tanto, en razón al principio de neutralidad tecnológica de la Ley 1341 de 2009 (art. 2.6), no deben aplicarse estándares que no permitan la utilización de tecnologías de información novedosas en los CPD y CAPD. Por tal motivo, debería dejarse un estándar más amplio, pero que cumpla con las finalidades de seguridad y protección de la información.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Por otro lado, en relación con el cumplimiento de los lineamientos establecidos en la norma técnica ANSI/TIA 942, Tier 3 o superior, no se entiende si para ello los prestadores deben obtener la certificación correspondiente ante los entes internacionales que la proveen, o si la Superintendencia internamente fijará unos estándares equivalentes que ella misma certificará.

Consideramos que la redacción del presente numeral es ambigua que da lugar a vacíos técnicos que pueden redundar en riesgos para las entidades vigiladas por los siguientes aspectos:

Por una parte, la única forma de garantiza el cumplimiento de un estándar o norma es con la exigencia de la presentación de una certificación, ya que de no presentarse cualquier proveedor de servicios podrán comunicar que cumplen con todos los lineamientos establecidos en alguna de estas normas sin que medie sustento alguno, razón por la cual sugerimos que se establezca la obligatoriedad de presentar dicho certificado para evitar situaciones que no vayan acorde con la normativa internacional.

En virtud de lo anterior, ponemos a consideración la siguiente redacción de texto:

> ***"3.2. Requerimientos mínimos para el CPD y CAPD***
>
> ***(…)***
>
> ***3.2.3.*** *El CDP de las entidades relacionadas en el inciso segundo del numeral 3 debe**rá ser diseñado y desplegado teniendo en cuenta los lineamientos establecidos en el estándar técnico*** ~~*tomar como referencia los lineamientos establecidos en la norma técnica*~~ *ANSI/TIA 942,* ~~*TIER 3 o superior*~~ *o cualquier otro estándar reconocido internacionalmente.* ***Lo anterior será reconocido a través de un certificado que cuente con alguna de las siguientes características:*** ~~*que brinde, al menos, el mismo nivel de disponibilidad.*~~

La construcción de data centers para la prestación de servicios globales de computación en la nube usa como guía las normas referenciadas, a la que se adicionan otras salvaguardas, mecanismos y procedimientos. Al ser una infraestructura global, orientada a niveles de servicio (no solo infraestructura), no resulta eficiente para servicios de nube

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

publica la certificación bajo los parámetros del uptime o icrea. No certificarse en esto no representa riesgo, ya que el servicio cuenta con certificaciones más elevadas (como por ejemplo soc1, soc2, soc3, iso27001, nist sox).

La orientación no debería ser hacia la certificación de edificaciones, sino hacia certificaciones que garanticen la continuidad de los servicios.

Comentarios al numeral 3.2.6 del proyecto

> ***"3.2. Requerimientos mínimos para el CPD y CAPD***
>
> *(…)*
>
> ***3.2.6.*** *El CDP y/o el CAPD que operen fuera de la red local principal de la entidad vigilada y de los operadores de información de la PILA deben contar con canales de comunicación redundantes con ella, independientes de extremo a extremo y que en lo posible usen rutas diferentes. Los canales de contingencia deben tener el ancho de banda necesario para soportar la operación eficiente de los sistemas de información de los procesos misionales y de gestión contable.*
>
> *(…)"*

La conectividad entre los CPDs, los CAPDs y las Entidades, es un aspecto fundamental para garantizar que los esquemas de contingencia alrededor de los procesos misionales y procesos críticos, así como los objetivos de RPO y RTO sean realmente cumplidos. Lo anterior, requiere que, así como se estableció un mínimo de redundancia a nivel de la infraestructura que soporta los CPD y lo CAPD, se establezca un mínimo de redundancia para los canales de comunicación.

Nos permitimos poner a consideración la siguiente redacción de texto:

> ***"3.2. Requerimientos mínimos para el CPD y CAPD***
>
> *(…)*
>
> ***3.2.6.*** *El CDP y/o el CAPD que operen fuera de la red local principal de la entidad vigilada y de los operadores de información de la PILA deben contar con canales de*

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

comunicación redundantes con ella, independientes de extremo a extremo y que ~~en lo posible~~ usen rutas diferentes. Los canales de contingencia deben tener el ancho de banda necesario para soportar la operación eficiente de los sistemas de información de los procesos misionales y de gestión contable.

(…)"

Comentarios al numeral 3.2. – Adicionar el numeral 3.2.9

En desarrollo de lo anterior, sugerimos incluir un numeral 3.2.9: "*El CPD y/o CAPD deben cumplir con los estándares de protección de dato personales nacionales e internacionales como ISO 27018*".

Comentarios al numeral 3.3.2.:

Con el fin de aclarar el origen de la información correspondientes, sugerimos modificar la redacción de la siguiente manera: "*Los manuales de las aplicaciones **de la entidad vigilada**, que operan en el CPD y/o CAPD o mecanismo alternativo de procesamiento de datos*".

Comentarios al numeral 3.3.6.

Respetuosamente solicitamos que este texto sea retirado de la redacción de la circular. Consideramos que los beneficios de mantener este inventario no son claros, y por el contario puede resultar difícil de implementar bajo las estructuras de tercerización tecnológica actualmente existentes. Consideramos que el objetivo de la cláusula puede ser logrado a través de los distintos acuerdos de niveles de servicio (ANS) ofrecidos por los proveedores de CPD y CAPD a las entidades vigiladas.

Comentarios al numeral 3.4.3.

Con el fin de facilitar el cumplimiento de esta obligación por parte de las entidades vigiladas, sugerimos la inclusión de la palabra "sustancialmente" para calificar las afectaciones a la prestación del servicio, la redacción sería de la siguiente manera: "La obligación por parte del CPD y/o CAPD de informar oportunamente a la entidad vigilada o a los operadores de información de la PILA contratante sobre cualquier evento o situación que pudiera llegar a afectar gravemente la prestación del servicio y, por ende,

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

el cumplimiento por parte de la vigilada de sus obligaciones frente a los consumidores financieros, a la SFC y a otros entes de control."

Comentarios al artículo 3.3.

3.3. Documentación

Las entidades vigiladas y los operadores de información de la PILA deben mantener actualizada y a disposición permanente de la SFC los documentos que se relacionan a continuación:
(…)

Es importante aclarar que por razones de confidencialidad y de secreto comercial, los proveedores de servicios de Internet o de Cloud no pueden proporcionar esta información completa de sus procesos y procedimientos. Podría en cambio tratarse de pensar en estándares establecidos por terceros como ISO 27001 e ISAE 3402.

Comentarios al numeral 3.3.2.:

Con el fin de aclarar el origen de la información correspondientes, sugerimos modificar la redacción de la siguiente manera: "*Los manuales de las aplicaciones* ***de la entidad vigilada****, que operan en el CPD y/o CAPD o mecanismo alternativo de procesamiento de datos*".

Comentarios al numeral 3.3.6.

Respetuosamente solicitamos que este texto sea retirado de la redacción de la circular. Consideramos que los beneficios de mantener este inventario no son claros, y por el contario puede resultar difícil de implementar bajo las estructuras de tercerización tecnológica actualmente existentes. Consideramos que el objetivo de la cláusula puede ser logrado a través de los distintos acuerdos de niveles de servicio (ANS) ofrecidos por los proveedores de CPD y CAPD a las entidades vigiladas.

Comentarios al numeral 3.4.1.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

"*3.4.1.* ***Establecer condiciones y limitaciones bajo las cuales el tercero contratado puede a su vez subcontratar parte del servicio. Cuando el subcontratista sea el que preste el servicio de colocación o de hospedaje en sus diferentes modalidades, también deberá cumplir con todas las obligaciones establecidas en este capítulo y corresponderá a la entidad vigilada verificar el cumplimiento de las obligaciones por parte del subcontratista***".

Puede resultar una carga excesivamente onerosa la de que la entidad vigilada deba verificar el cumplimiento por parte del subcontratista, pues resultaría suficiente que estableciéramos controles suficientes en el contrato que celebre con el contratista del CPD.

Sugerimos la siguiente redacción:

"*3.4.1. Establecer condiciones y limitaciones bajo las cuales el tercero contratado puede a su vez subcontratar parte del servicio. Cuando el subcontratista sea el que preste el servicio de colocación o de hospedaje en sus diferentes modalidades, también deberá cumplir con todas las obligaciones establecidas en este capítulo y corresponderá a la entidad vigilada exigir el cumplimiento de las obligaciones por parte del subcontratista*".

Comentarios al numeral 3.4.3.

Con el fin de facilitar el cumplimiento de esta obligación por parte de las entidades vigiladas, sugerimos la inclusión de la palabra "sustancialmente" para calificar las afectaciones a la prestación del servicio, la redacción sería de la siguiente manera: "La obligación por parte del CPD y/o CAPD de informar oportunamente a la entidad vigilada o a los operadores de información de la PILA contratante sobre cualquier evento o situación que pudiera llegar a afectar gravemente la prestación del servicio y, por ende, el cumplimiento por parte de la vigilada de sus obligaciones frente a los consumidores financieros, a la SFC y a otros entes de control."

Comentarios al artículo 3.4.4.

Esta norma no prevé los casos en los que los servicios de CPD y CAPD son prestados por terceros fuera del país, ya que la información que se almacena en dichos servidores es confidencial y no puede ser accedida por terceros, ya que violaría normas legales de confidencialidad, privacidad y protección de datos personales, entre otras.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

No cabe duda de la importancia de que la Superintendencia tenga las facultades para poder cumplir con sus funciones. Pero con el fin de no causar un potencial detrimento de los requerimientos de seguridad de los proveedores de servicios de procesamiento de datos. Sugerimos la siguiente redacción:

"La posibilidad de que la SFC pueda verificar las condiciones de operación del CPD, el CAPD o el mecanismo alternativo de procesamiento de datos, cuando lo considere necesario, para lo cual se coordinarán previamente las actividades a desarrollar y se respetarán razonablemente los protocolos de seguridad correspondientes del proveedor. Dicha verificación podrá realizarse de manera remota por la SFC."

Comentarios al artículo 3.4.7.

La posibilidad de que la SFC pueda verificar las condiciones de operación del CPD y el CAPD, cuando lo considere necesario, realizando visitas de inspección, no reconoce la posibilidad de prestar estos CPD y CAPD por terceros proveedores de servicios de Internet o de Cloud que se encuentran por fuera del país y no son sujetos de vigilancia de la SFC. Los proveedores de Internet o de Cloud, por razones de confidencialidad de la información y de seguridad no pueden permitir que terceros (en este caso, la SFC) inspeccionen la información de los servidores ya que esto impactaría la seguridad de un servicio de computación en la nube contratado por millones de clientes. Para esto, los proveedores de servicios de Cloud proveen las certificaciones de seguridad y auditoría que brindan la confianza necesaria.

Comentarios al artículo 3.5.1.

> ***"3.5. Requerimientos adicionales para los CDP y CAPD que operan fuera de Colombia"***
>
> *(…)*
>
> ***3.5.1.*** *Verificar que el CDP y/o CAPD ubicado(s) en el exterior esté(n) en jurisdicciones que tengan como mínimo (i) normas de Habeas Data y (ii) normas sobre penalización de atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.*
>
> *(…)**"***

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Este artículo exige que los CPD o CAPD que se encuentren por fuera del país tienen que ubicarse en países con dos condiciones: (i) que tenga normas de habeas data; y (ii) normas sobre penalización de atentados contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.

Es importante especificar qué se entiende por normas de protección de habeas data, ya que por ejemplo en Estados Unidos se encuentran los más importantes servicios de computación en Internet, así como sistemas de protección de información altamente confiables y seguros, pero no es claro si puede entenderse que Estados Unidos tenga normas de protección de datos como se refiere el proyecto de circular. Además, por razones de seguridad, los servidores de los proveedores de servicios de Cloud pueden encontrarse en varios países a la vez con el fin de replicar la información y proveer redundancia entre otros, por lo cual no es razonable esta exigencia.

Con el fin de alinear el texto propuesto con la normativa interna colombiana, así como por los estándares a nivel internacional, se pone a consideración la siguiente redacción de texto:

> ***"3.5. Requerimientos adicionales para los CDP y CAPD que operan fuera de Colombia"***
>
> *(…)*
>
> ***3.5.1.*** *Verificar que el CDP y/o CAPD ubicado(s) en el exterior esté(n) en jurisdicciones que tengan como mínimo (i) normas de habeas data**, (ii) normas* ***equivalentes a las colombianas sobre la penalización de atentados*** *contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos**, y (iii) los CPDs y/o CAPDs cuenten con la certificación ISO 27001 como requerimiento mínimo**.*
>
> *(…)"*

Comentarios al artículo 4.
Centros de servicios compartidos

Como ocurre con los numerales anteriormente comentados, en este aparte no se definen los elementos "asociados a la ejecución de sus procesos misionales y su gestión financiera" y, consecuentemente, no resulta claro el alcance de la obligación que se busca imponer.

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico

Adicionalmente, reiteramos que la imposición de obligaciones de manejo independiente de estos elementos, además de la falta de claridad sobre los procesos a los que aplica, restringe indebidamente la libertad de las entidades financieras de elegir su infraestructura tecnológica posibilidad de compartir un centro de procesamiento de datos y atenta contra el principio de neutralidad tecnológica establecido en ley 1341 y de raigambre constitucional, pues es corolario del derecho a la igualdad.

Creemos que, en lugar de lo anterior, se debería permitir a las entidades vigiladas por la SFC hacer uso de los CSC para el almacenamiento tanto de los elementos descritos en el artículo 4 como de otros, buscando que las CSC cumplan con estándares mínimos de seguridad reconocidos internacionalmente (como SSAE 16 o ISO 27001) para garantizar la integridad e invulnerabilidad de la información de las entidades, independientemente de su naturaleza.

Esperamos que las anteriores consideraciones sean de utilidad para la Superintendencia Financiera de Colombia. Finalmente, le solicitamos muy respetuosamente nos otorgue una reunión para poder profundizar en estos comentarios y aclarar ciertos puntos de esta discusión.

De antemano agradecemos su atención y quedamos a su a disposición para ampliar estos comentarios.

Cordialmente,

F.D.O.

VICTORIA EUGENIA VIRVIESCAS CALVETE
Directora Ejecutiva

---

[1] McKinsey & Cia. “Internet matters: The Net’s sweeping impact on growth, jobs, and prosperity”. Mayo de 2011.

[2] TIA, “White Paper on Cloud Computing”. Disponible en: http://www.tiaonline.org/standards/TIA_Cloud_Computing_White_Paper.pdf. 2011

Carrera 10 # 97A-13 Ofc. 304 - Bogotá, Colombia - Tel: (57-1) 300 4537, (57) 320 425 8673 Skype: cccelectronico