SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO VI: REGLAS RELATIVAS AL USO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

CONTENIDO

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO VI: REGLAS RELATIVAS AL USO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

1. ÁMBITO DE APLICACIÓN

Las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) pueden soportar todos sus procesos y actividades en servicios computacionales en la nube. Cuando se trate de la operación de sus procesos misionales o de gestión contable y financiera deben cumplir las instrucciones de las que trata este Capítulo.

También pueden hacerlo los operadores de información de la Planilla Integrada de Liquidación de Aportes (PILA) respecto de la actividad del Operador de Información de la Planilla definida en el artículo 2° del Decreto 1465 de 2005 y los Institutos de Fomento y Desarrollo de las entidades territoriales.

2. DEFINICIONES

Las siguientes definiciones se deben tener en cuenta para los fines del presente Capítulo.

2.1. Disponibilidad

Porcentaje de tiempo que el servicio tecnológico utilizado por la entidad está habilitado para la prestación del servicio.

2.2. Procesos misionales

Son aquellos procesos que contribuyen directamente al resultado previsto por la entidad en cumplimiento de su objeto social. Estos procesos están relacionados con la naturaleza, misión, objetivos y función de la entidad y no están asociados a actividades de apoyo o complementarias.

2.3. Servicios de computación en la nube

Tecnología que permite el acceso en condiciones de ubicuidad, configurable y por demanda, a un conjunto compartido de recursos computacionales, que se pueden aprovisionar, configurar y liberar rápidamente, con poco esfuerzo de gestión o de interacción con el proveedor de servicios. Dicha tecnología puede prestarse a través de los siguientes tipos de modelo de servicios y cuatro modelos de implementación:

2.3.1. Software como servicio (SaaS, por su sigla en inglés). Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las aplicaciones que corren en la infraestructura de éste, bajo demanda y que pueden ser utilizadas de forma compartida con otros usuarios. La entidad no administra ni controla la infraestructura del proveedor.

2.3.2. Plataforma como servicio (PaaS, por su sigla en inglés). Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las plataformas en las cuales desarrollan y prueban distintas aplicaciones, mediante el uso de lenguajes y herramientas de programación que son gestionadas por el prestador de servicios. La entidad no administra ni controla la infraestructura del proveedor.

2.3.3. Infraestructura como servicio (IaaS, por su sigla en inglés). Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad la infraestructura que le permite ejecutar software de cualquier tipo, con el propósito de obtener la capacidad de procesamiento informático o de almacenamiento de información mediante servicios estandarizados.

2.4. Implementaciones de nube

Las siguientes son las implementaciones de nube consideradas para la aplicación de este Capítulo:

2.4.1. Nube pública. Servicios disponibles para ser utilizados por el público en general y que son suministrados por un proveedor que comercializa servicios por demanda.

2.4.2. Nube privada. Servicios disponibles que se proporcionan para uso exclusivo de una organización.

2.4.3. Nube comunitaria. Servicios disponibles para el uso exclusivo de una comunidad específica de organizaciones que tienen objetivos similares.

2.4.4. Nube híbrida. Servicios disponibles compuestos de dos o más implementaciones de nube.

2.5. Subcontratistas o *partners*

Terceros contratados por los proveedores de servicios de computación en la nube o de otra forma relacionado con ellos y cuyas actividades comprenden el desarrollo de una parte material de los servicios en la nube que usan las entidades vigiladas. Su actividad puede implicar el acceso a información y datos de la entidad y no está asociada a las actividades auxiliares de mantenimiento y soporte.

3. OBLIGACIONES GENERALES DE LAS ENTIDADES

Las entidades que soporten la operación de sus procesos misionales o de gestión contable y financiera en servicios computacionales en la nube, deben:

3.1. Contemplar dentro de su Sistema de Administración de Riesgo Operativo (SARO) la gestión efectiva de los riesgos derivados de la utilización de servicios computacionales en la nube, considerando, entre otros factores, el tipo de nube

contratada, los sitios de procesamiento, los servicios contratados, el tipo de información a procesar, los controles de seguridad para la protección de los datos en ambientes virtualizados y la protección de las aplicaciones de la entidad.

3.2. Establecer los criterios para seleccionar el proveedor de servicios de computación en la nube.

3.3. Evaluar la conveniencia de implementar en sus filiales y subsidiarias del exterior, en caso de que las tengan, las instrucciones de este Capítulo.

3.4. Verificar que el proveedor de servicios en la nube cuente y mantenga vigente, al menos, la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).

3.5. Verificar que el proveedor ofrezca una disponibilidad de al menos el 99.95% en los servicios prestados en la nube

3.6. Gestionar los riesgos de las API o Servicios Web suministrados por el proveedor de servicios en la nube.

3.7. Verificar que las jurisdicciones en donde se procesará la información cuenten con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.

3.8. Establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de la entidad cuando así lo requiera.

3.9. Garantizar la independencia de su información y de sus copias de respaldo de la información de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.

3.10. Mantener cifrada la información clasificada como confidencial en tránsito o en reposo, usando estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES, RSA o 3DES.

3.11. Tener bajo su control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube, dependiendo del modelo de servicio contratado.

3.12. Monitorear los servicios contratados para detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera.

3.13. Establecer procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el proveedor de servicios en la nube y sus subcontratistas o *partners*, cuando sean estos quienes prestan el servicio.

3.14. Contar con canales de comunicación con el proveedor de servicios en la nube cifrados de extremo a extremo y que en lo posible usen rutas diferentes.

3.15. Contemplar dentro de los criterios para seleccionar las firmas que tendrán a su cargo la auditoria interna o externa de la entidad, las competencias técnicas necesarias para evaluar servicios en la nube.

3.16. Establecer las medidas necesarias para garantizar que, en el evento de toma de posesión, la SFC, Fogafín, Fogacoop, o quienes éstas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en la nube.

4. ACUERDOS O CONTRATOS DE SERVICIOS

Los acuerdos o contratos que suscriban las entidades para la prestación de servicios de computación en la nube deben contemplar como mínimo los siguientes elementos:

4.1. Las condiciones referentes a capacidad, disponibilidad, tiempos de recuperación, la existencia de planes de continuidad, resolución de incidentes y horarios de atención del proveedor del servicio, las cuales deben prever niveles de servicio que permitan cumplir, cuando menos, con las instrucciones señaladas en el numeral 3 de este Capítulo.

4.2. Las condiciones de seguridad de la información y ciberseguridad de los servicios en la nube y las condiciones establecidas para proteger la privacidad y confidencialidad de los datos de los clientes, las cuales deben prever niveles de servicio que permitan cumplir, cuando menos, con las instrucciones señaladas en el numeral 3 de este Capítulo sobre la información procesada en la nube.

4.3. La propiedad de la información que se procese en los servicios de computación en la nube, haciendo claridad que los datos son propiedad de la entidad vigilada y que no se pueden usar para ningún propósito diferente al establecido en el contrato.

4.4. Las condiciones y limitaciones bajo las cuales se puede subcontratar parte del servicio o realizar cambios a los acuerdos establecidos con sus subcontratistas o *partners*.

4.5. Las causales de terminación del contrato por parte de la entidad, incluyendo, el incumplimiento de los acuerdos o niveles de servicio o el cambio de las condiciones que generen impacto negativo al servicio contratado.

4.6. La entrega a la entidad vigilada de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, así como la vigencia de las certificaciones enunciadas en el numeral 3.4 de este Capítulo.

4.7. La obligación del proveedor del servicio de informar, en cuanto le sea posible, a la entidad vigilada sobre cualquier evento o situación que pudiera afectar significativamente 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 otras entidades.

4.8. El borrado seguro de los datos existentes en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite la entidad o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios.

4.9. La corrección oportuna y eficaz de las vulnerabilidades informáticas detectadas.

4.10. La utilización de técnicas de múltiple factor de autenticación para el acceso a las consolas de administración por parte de la entidad vigilada.

5. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Las entidades vigiladas deben considerar dentro del plan de continuidad del negocio la operación en la nube y realizar las pruebas que resulten necesarias para confirmar la efectividad de los procedimientos contingentes.

Asimismo, deben contar con la estrategia de migración a otra plataforma en caso de terminación del contrato por cualquiera de las partes, por la interrupción o la degradación en la prestación del servicio de parte del proveedor de servicios en la nube o por cualquier otro motivo que considere razonable la entidad vigilada.

6. REMISIÓN DE INFORMACIÓN A LA SFC

Dentro de los 15 días anteriores al inicio del procesamiento de información en la nube, relacionada con procesos misionales o de gestión contable y financiera, las entidades deben remitir a la SFC la siguiente información:

6.1. El nombre del proveedor que prestará los servicios en la nube y de los subcontratistas o *partners* que le prestarán servicios asociados al objeto del contrato.

6.2. La relación de los procesos que serán manejados en la nube, incluyendo las aplicaciones, tipo de datos, productos y servicios asociados a éstos.

6.3. La ubicación física o región donde se procesarán y almacenarán los datos.

6.4. Las certificaciones otorgadas al proveedor del servicio y/o sitio de procesamiento.

6.5. La relación de auditorías a las que se somete el proveedor de servicios contratado.

6.6. La información sobre los niveles de servicio establecidos.

6.7. El diagrama con la plataforma tecnológica que soportará los servicios contratados.

7. DOCUMENTACIÓN

Las entidades deben mantener actualizada y a disposición permanente de la SFC, a través de los medios verificables que establezcan para el efecto, la información que se relaciona a continuación:

7.1. La documentación completa de los procesos y procedimientos que se ejecutan en la nube.

7.2. La documentación de las aplicaciones que operan en la nube.

7.3. La documentación de los flujos de datos de los procesos misionales o de gestión contable y financiera que alimentan o consumen las aplicaciones dispuestas por el proveedor de servicios en la nube, cuando aplique.

7.4. Los diagramas de red que permitan identificar la plataforma que soporta el servicio contratado.

7.5. Los procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el proveedor de servicios en la nube.

7.6. Los reportes generales de auditoria, pruebas de vulnerabilidades y estado actual de los servicios contratados.