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

CONTENIDO

1. Entidades exceptuadas

Las oficinas de representación de instituciones financieras y reaseguradoras del exterior, del mercado de valores del exterior, sociedades fiduciarias sin establecimiento de comercio y organismos financieros del exterior sin establecimiento de comercio están exceptuadas de la aplicación de las instrucciones contenidas en este capítulo.

2. Definiciones

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

2.1. Análisis de Impacto del Negocio (BIA)

Análisis por medio del cual la entidad determina cuáles son los procesos y recursos críticos para su operación y el impacto para la misma cuando se presenten eventos que los afecten.

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)

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.

2.4. Centro de Servicios Compartidos (CSC)

Es una unidad que se encarga de gestionar procesos y actividades de soporte de varias entidades, entre estos, recursos humanos, tecnologías de la información y comunicaciones, administración de riesgos, servicios generales y adquisiciones de bienes y servicios.

2.5. Plan de Contingencia

Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

2.6. Plan de Continuidad del Negocio

Conjunto de procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido aceptable, en caso de interrupciones.

2.7. Procesos Misionales

Son aquellos procesos que proporcionan el resultado previsto por la entidad en el cumplimiento de su objeto social.

2.7.1. Procesos Críticos

Son aquellos procesos que debido a su importancia deben estar disponibles y operativos constantemente o lo antes posible, después de un incidente, emergencia o desastre.

2.8. Punto objetivo de recuperación (RPO)

Punto en el cual la información usada por una actividad debe ser restaurada para permitir la reanudación de la operación.

2.9. Tiempo objetivo de recuperación (RTO)

Tiempo después de un incidente en el que la operación o el servicio deben ser reanudados.

3. CPD y CAPD

Las entidades vigiladas y los operadores de información de la PILA deben contar con un CPD para la operación de los sistemas de información que soportan sus procesos misionales y de gestión contable.

Los establecimientos de crédito, aseguradoras, sociedades fiduciarias, sociedades administradoras de sistemas de pago de bajo valor, sociedades administradoras de fondos de pensiones y cesantías, bolsas de valores, bolsas de bienes y productos agropecuarios, agroindustriales o de otros *commodities*, sociedades administradoras de sistemas de negociación de valores, sociedades administradoras de sistemas de registro de operaciones sobre valores, sociedades administradoras de sistemas de compensación y liquidación de divisas, sociedades administradoras de sistemas de compensación o liquidación de valores, sociedades administradoras de sistemas de negociación y de registro de operaciones sobre divisas, sociedades comisionistas de las bolsas de valores, sociedades administradoras de inversión, sociedades administradoras de depósitos centralizados de valores, cámaras de riesgo central de contraparte, proveedores de precios, Fondo Nacional del Ahorro, Colpensiones, el Banco de la República, las sociedades especializadas en depósitos y pagos electrónicos y los operadores de información de la Planilla Integrada de Liquidación de Aportes (PILA) deben contar con un CAPD.

Las demás entidades, dependiendo de las actividades que desarrollen, del número de operaciones, del número de clientes, de los canales dispuestos para la prestación de servicios, de las interconexiones con otras entidades, del RTO y el RPO que determinen, deben contar un mecanismo alternativo que les permitan procesar su información en un sitio diferente al CPD, cuando ello se requiera, o pueden hacerlo en un CAPD.

3.1. Obligaciones generales

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.

3.1.2. Las entidades vigiladas y los operadores de información de la PILA deben contemplar, dentro de sus sistemas de administración del riesgo operativo, los riesgos relacionados con el procesamiento de la información en un CPD o CAPD, independientemente de que estén ubicados en Colombia o en el exterior y sean centros propios o de un tercero.

3.1.3. Las entidades vigiladas y los operadores de información de la PILA deben tener a disposición de la SFC la información de los indicadores de disponibilidad y de las alarmas generadas por advertencias o fallas de los sistemas de energía, comunicaciones, ambientales, seguridad física y logística de los últimos dos años.

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.

3.1.5. Las entidades vigiladas y los operadores de información de la PILA deben contar con copias de respaldo actualizadas de la información que se procesa en el CPD, considerando el RPO. Dichas copias deben estar disponibles para los empleados en Colombia de la entidad vigilada. Las copias se deben probar con el objetivo de verificar su disponibilidad y se deben poder restaurar en el momento en que se requieran.

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

3.1.7. Las entidades vigiladas y los operadores de información de la PILA deben mantener la independencia de los elementos relacionados en el numeral 4 de este capítulo, asociados al manejo de la información de sus procesos misionales y de gestión contable, en el CPD y/o en el CAPD.

3.1.8. Las entidades vigiladas y los operadores de información de la PILA con filiales en el exterior deben hacer un análisis para evaluar la conveniencia de implementar en sus filiales las instrucciones de este capítulo, con el fin de mitigar el riesgo operativo.

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:

a) Nombre de la entidad con la cual se suscribió el contrato para el uso del CPD y/o el CAPD, en caso de que aplique.

b) Ubicación física del CPD y/o el 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.

e) Certificaciones otorgadas al CPD y/o CAPD, en caso en que aplique.

f) Gestión del riesgo operativo y de la seguridad de la información, realizada por la entidad vigilada o por el operador de información de la PILA, asociada al procesamiento en el nuevo CPD y/o CAPD.

3.1.10. Las entidades vigiladas deben garantizar que en el evento de toma de posesión, la SFC, Fogafin, Fogacoop o quienes estas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en el CPD y en el CAPD o en el mecanismo alternativo de procesamiento de datos.

3.2. Requerimientos mínimos para el CPD y CAPD

Las entidades vigiladas y los operadores de información de la PILA deben verificar que el CPD y el CAPD cumplan con los siguientes requerimientos mínimos:

3.2.1. Contar con el soporte técnico que permita solucionar problemas o incidentes tan pronto se presenten.

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.

3.2.3. El CPD 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.

3.2.4. El CAPD 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.

3.2.5. El CAPD de las entidades relacionadas en el inciso segundo del numeral 3 debe estar separado del CPD, previendo que un mismo acontecimiento no afectará de manera simultánea la operación del CPD y el CAPD.

3.2.6. El CPD 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.

3.2.7. El personal asignado para administrar los recursos informáticos utilizados para el procesamiento de la información en el CPD y en el CAPD debe estar disponible de manera inmediata para atender cualquier actividad relacionada con sus funciones, cuando se requiera por parte de la entidad vigilada, de los operadores de información de la PILA o de la SFC.

3.2.8. El CAPD debe tener la capacidad de soportar los procesos misionales y de gestión contable que se ejecutan en el CPD.

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:

3.3.1. La documentación completa de los procesos y procedimientos que se ejecutan en el CPD y/o en el CAPD o los que emplearían cuando hagan uso del mecanismo alternativo de procesamiento de datos.

3.3.2. Los manuales de las aplicaciones que operan en el CPD y/o CAPD o mecanismo alternativo de procesamiento de datos.

3.3.3. Los diagramas de red que permiten identificar los equipos de cómputo y equipos de comunicaciones del CPD y/o CAPD y la forma como están conectados con las distintas sedes de la entidad y con los terceros que atienden servicios en su nombre.

3.3.4. Los procedimientos para verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el CPD y/o el CAPD.

3.3.5. Los documentos en donde se evidencien los eventos de riesgo operativo presentados en el CPD, el CAPD o en los mecanismos alternativos que hubieran afectado el funcionamiento normal de los sistemas de información que soportan los procesos misionales y de gestión contable de la entidad y los documentos que permitan confirmar la implementación de los planes establecidos para su mitigación. Estos incidentes también deben incluirse en el registro de eventos del Capítulo XXIII de la CBCF.

3.3.6. El registro actualizado de los equipos, aplicaciones y elementos de comunicaciones que soportan los procesos misionales y de gestión contable que operan en el CPD y CAPD, que describa para cada uno de ellos las características técnicas, su función y los procesos, productos o servicios del negocio que soporta.

3.4. Acuerdos o contratos de servicios

Los acuerdos o contratos que suscriban las entidades vigiladas y los operadores de información de la PILA con terceros que presten el servicio de CPD o CAPD, deben cumplir como mínimo con los siguientes requerimientos:

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.

3.4.2. Incluir cláusulas que establezcan la continuidad en la prestación del servicio después de adoptada la toma de posesión, durante el tiempo que sea necesario, para que la entidad vigilada continúe cumpliendo con sus obligaciones.

3.4.3. 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 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.

3.4.4. 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.

3.5. Requerimientos adicionales para los CPD y CAPD que operen fuera de Colombia

Las entidades vigiladas y los operadores de información de la PILA que procesen la información de sus procesos misionales y de gestión contable en un CPD y/o en un CAPD que se encuentre(n) en el exterior, además de cumplir con lo dispuesto en los numerales 3.1 a 3.4, tienen las siguientes obligaciones:

3.5.1. Verificar que el CPD 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.

3.5.2. Incluir dentro de las políticas de seguridad de la información de la entidad vigilada las relacionadas con el procesamiento de datos en el exterior.

4. Centros de servicios compartidos (CSC)

En adición a lo establecido en el numeral 3 del presente capítulo, las entidades vigiladas y los operadores de información de la PILA que se apoyen en CSC para la gestión de las tecnologías de la información y las comunicaciones, deben disponer de los recursos técnicos y procedimentales que sean necesarios para mantener la independencia de:

4.1. Los datos manejados por las aplicaciones que soportan la ejecución de los procesos misionales y de gestión contable de cada entidad.

4.2. Las copias de respaldo de la información de cada entidad.

4.3. Las credenciales de autenticación que permitan el acceso a los recursos y a la información de cada entidad.

4.4. La administración de la información de cada entidad.

5. Administración de la continuidad del negocio

En adición a lo definido en el numeral 3.1.3.1 del Capítulo XXIII de la Circular Básica Contable y Financiera, se debe dar cumplimiento a lo siguiente:

5.1. Plan de contingencia y continuidad del negocio

Los establecimientos bancarios, las sociedades administradoras de sistemas de pago de bajo valor, las bolsas de valores, bolsas de bienes y productos agropecuarios, agroindustriales o de otros *commodities*, sociedades administradoras de sistemas de negociación de valores, sociedades administradoras de sistemas de registro de operaciones sobre valores, sociedades administradoras de sistemas de compensación y liquidación de divisas, sociedades administradoras de sistemas de compensación o liquidación de valores, sociedades administradoras de sistemas de negociación y de registro de operaciones sobre divisas, las cámaras de riesgo central de contraparte, los proveedores de precios, el Banco de la República, las sociedades especializadas en depósitos y pagos electrónicos y los operadores de información de la PILA deben cumplir con los siguientes requerimientos:

5.1.1. Considerar en el BIA los riesgos operativos que afecten la interacción con las demás entidades financieras, en particular a aquellos que puedan tener un efecto de contagio en el mercado. Para el cumplimiento de este propósito las entidades deben coordinar entre sí la ejecución de las actividades que resulten necesarias.

5.1.2. Contar con planes de contingencia y continuidad del negocio que permitan que los sistemas centrales que soportan los procesos críticos estén disponibles para continuar la prestación de los servicios a lo sumo dos (2) horas después de haberse presentado el evento que los afectó. Las actividades programadas, tales como mantenimientos, actualizaciones, migraciones y traslados, que se realicen sobre los sistemas centrales, se deben adelantar en los horarios que afecten en menor medida a los consumidores financieros y ellas no se considerarán dentro de los tiempos señalados anteriormente.

5.2. Operación en el CAPD, pruebas de contingencia y continuidad del negocio

Las entidades relacionadas en el inciso segundo del numeral 3 y las que procesen su información fuera de Colombia deben:

5.2.1. Soportar la operación de sus procesos misionales y de gestión contable al menos una vez al año desde el CAPD.

5.2.2. Mantener a disposición de la SFC los resultados de la operación en el CAPD a que hace referencia el numeral 5.2.1, así como los escenarios y las conclusiones de las pruebas realizadas el año anterior a los planes de contingencia y continuidad del negocio que soporten los procesos misionales y de gestión contable.