GUÍA PARA LA AUTORIZACIÓN DE CONTRATACIÓN DE SERVICIOS CON TERCEROS (INSTITUCIONES DE CRÉDITO)

VERSIÓN 2.0
SEPTIEMBRE DE 2022

ÍNDICE

Objetivo de la guía
Definiciones
Presentación del proyecto

Sección I

a) Aviso en términos del artículo 326 de la CUB.

Contenido del aviso en términos del artículo 326 de la CUB:

I. Información relativa a la Institución de crédito.
II. Información del Tercero con el que se pretende celebrar el contrato de prestación de servicios.
III. Servicios que prestará el Tercero.
IV. Información a se refieren los artículos 318, fracciones II, VI y VII de la CUB.
V. Fecha probable de la celebración del contrato de prestación de servicios.
VI. Declaración respecto de si alguno de los servicios estará sujeto a subcontratación, en cuyo caso mencionar a todos y cada uno de los Proveedores que participan.
VII. Anexos del escrito de aviso.
VIII. Puntos petitorios.

b) Escrito de solicitud de autorización en términos del artículo 328 de la CUB.

Contenido del escrito de solicitud de autorización en términos del artículo 328 de la CUB:

I. Información relativa a la Institución de crédito.
II. Información del Tercero con el que se pretende celebrar el contrato de prestación de servicios.
III. Servicios que prestará el Tercero.
IV. Descripción de los mecanismos que permitirán a la Institución de crédito contar con la información detallada y actualizada de cada una de las operaciones y registros, en territorio nacional, en un medio que permita su consulta en caso de interrumpirse el servicio del Proveedor.
V. Información a se refieren los artículos 318, fracciones II y VII de la CUB.
VI. Señalar la fecha probable de la celebración del contrato de prestación de servicios.
VII. Declaración respecto de si alguno de los servicios estará sujeto a subcontratación, en cuyo caso mencionar a todos y cada uno de los Proveedores que participan.
VIII. Anexos del escrito de solicitud.
IX. Puntos petitorios.

Sección II - Requisitos legales

a) Aspectos generales
b) Contrato de prestación de servicios.

Sección III

En materia de seguridad de la información
En materia de riesgo operacional y tecnológico

Formato de Información de Sistemas Aplicativos (F-SA)

Objetivo de la Guía

La presente Guía constituye una herramienta de apoyo a las instituciones de crédito interesadas en contratar con Terceros servicios que tengan por objeto la realización de procesos operativos o administración de bases de datos o sistemas informáticos, en términos de lo dispuesto por el Capítulo XI, Sección Tercera de las Disposiciones de carácter general aplicables a las instituciones de crédito. Su objetivo es facilitar a los promoventes la adecuada integración de los expedientes que constituirán el sustento documental de su solicitud, y de ninguna manera pretende sustituir lo establecido en la Ley de Instituciones de Crédito o en las Disposiciones de carácter general aplicables a las instituciones de crédito, las cuales, a diferencia de esta Guía, sí tienen el carácter de mandatorio para las Instituciones de crédito.

Este documento ha sido elaborado sólo con fines prácticos, utilizando como metodología la exposición ordenada del conjunto de requisitos que establece la regulación vigente -Ley de Instituciones de Crédito y Disposiciones de carácter general aplicables a las instituciones de crédito- para obtener la autorización referida, con explicaciones y orientaciones que coadyuven al cumplimiento de cada requisito en particular.

Con el fin de conocer desde el inicio del proceso los elementos esenciales del proyecto que se presente a la Comisión Nacional Bancaria y de Valores, se mencionan en la Guía aquellos aspectos elementales que es necesario que los promoventes expongan, en su caso, en una reunión introductoria con los funcionarios de las áreas competentes, con respecto a la viabilidad, características y bondades del esquema, sin perjuicio del análisis posterior a la documentación soporte que la propia autoridad llevaría a cabo.

Es preciso señalar que esta Guía de acuerdo con las disposiciones del Capitulo XI de la CUB no serán aplicables cuando las Instituciones contraten los servicios que se indican en el artículo 317 de la CUB.

Definiciones

Para los efectos de la presente Guía se entenderá por:

Banca Electrónica: al conjunto de servicios y operaciones bancarias que las Instituciones realizan con sus Usuarios a través de Medios Electrónicos

CNBV: a la Comisión Nacional Bancaria y de Valores.

CUB: a las Disposiciones de carácter general aplicables a las instituciones de crédito o las que las sustituyan.

Institución: a la Institución de crédito que contrata servicios con un Tercero.

LIC: a la Ley de Instituciones de Crédito.

Medios Electrónicos: a los equipos, medios ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean públicos o privados, a que se refiere el Artículo 52 de la LIC.

Tercero o Prestador de servicios o Proveedor: a la persona con la que la Institución pretenda celebrar un contrato de servicios, que tengan por objeto la realización de procesos operativos o administración de bases de datos o sistemas informáticos relacionados con operaciones diferentes a las que se refiere el Capítulo XI, Sección Segunda de la CUB.

Presentación del proyecto

En esta presentación, exponer de manera general (de preferencia con apoyo audiovisual), los siguientes aspectos:

1. Denominación del Tercero a contratar.
2. Servicios que serán materia de la contratación y lugar en el que se prestarán, procesarán, transmitirán y almacenarán dichos servicios.
3. Presencia en el mercado del Tercero a contratar.
4. Infraestructura tecnológica.

Sección I

a) Aviso en términos del artículo 326 de la CUB

El escrito que contenga el aviso a que se refiere el artículo 326 de la CUB considerando que la prestación del servicio a contratar se realizará en territorio nacional, será en formato libre suscrito por el director general de la Institución y deberá contener la información que describa los aspectos generales de la contratación, de conformidad con los Apartados de esta Sección.

Este aviso se presentará a la Comisión, acompañado de la documentación a que se refiere la normatividad aplicable, con cuando menos veinte días hábiles de anticipación a la fecha en que se pretendan contratar los servicios.

Para el caso de la banca de desarrollo, cuando la contratación se lleve a cabo mediante Licitación Pública o Invitación a cuando menos tres personas, el citado aviso deberá presentarse al inicio del procedimiento de contratación y una vez obtenida la excepción otorgada por la SHCP, a que se refiere el Artículo 47 de la LIC.

<u>Contenido del aviso en términos del artículo 326 de la CUB:</u>

I. Información relativa a la Institución

En este apartado se deberá contener la denominación de la Institución. El aviso correspondiente deberá estar suscrito por el director general de la misma.

II. Información del Tercero con el que se pretende celebrar el contrato de prestación de servicios.

- Incluir la denominación completa del Tercero y, en su caso, los nombres comerciales con los que es conocido, así como una breve reseña de su historia corporativa y de negocios.
- Acompañar copia simple de la escritura constitutiva del Tercero.
- Dirección completa en donde se realizarán cada uno de los procesos, servicios y/o los centros de datos (primario y secundario) en donde se almacenará y procesará la información (calle, número exterior e interior, delegación o municipio, código postal, estado y país).

III. Servicios que prestará el Tercero.

En este apartado se incluirá la descripción del proceso operativo o de administración de base de datos o sistemas informáticos objeto de los servicios, proporcionando una descripción detallada acerca de ellos.

IV. Información a se refieren los artículos 318, fracciones II y VII de la CUB.

En este apartado deberá contenerse la información que se describe en la Sección de requisitos legales de la presente Guía.

V. Señalar la fecha probable de la celebración del contrato de prestación de servicios.

La Institución deberá cuidar que el escrito de aviso se presente con por lo menos veinte días hábiles previos a la fecha en que pretendan contratar dichos servicios.

VI. Declaración respecto de si alguno de los servicios estará sujeto a subcontratación, en cuyo caso mencionar a todos y cada uno de los Proveedores que participan.[1]

VII. Anexos del escrito de aviso.

Incluir un índice de los anexos que servirán de soporte documental para acreditar lo manifestado en el escrito de aviso y el cumplimiento de los requisitos que se mencionan en la Sección II de la presente Guía.

VIII. Puntos petitorios.

Solicitar de manera expresa que se tenga por presentado el aviso a que se refiere el artículo 326 de la CUB, así como sus respectivos anexos, en términos del planteamiento que se presente, para todos los efectos.

b) Escrito de solicitud de autorización en términos del artículo 328 de la CUB

El escrito de solicitud de autorización para la contratación con Terceros de la prestación de servicios, para la realización de un proceso operativo o para la administración de bases de datos o sistemas informáticos, en los que se procese, almacene o transmita información, y que se proporcionen o ejecuten parcial o totalmente fuera de territorio nacional o por residentes en el extranjero, será en formato libre suscrito por el director general de la Institución.

Este escrito se presentará a la Vicepresidencia de la CNBV encargada de su supervisión, acompañado de la documentación a que se refiere la normatividad aplicable, con cuando menos veinte días hábiles de anticipación a la fecha en que se pretendan contratar al Tercero.

[1] Si alguno de los servicios es subcontratado por Proveedores en el extranjero, se deberá requerir autorización.

Contenido del escrito de solicitud de autorización en términos del artículo 328 de la CUB:

I. Información relativa a la Institución de crédito.

En este apartado se deberá contener la denominación de la Institución. El escrito correspondiente deberá estar suscrito por el director general de la misma.

II. Información del Tercero con el que se pretende celebrar el contrato de prestación de servicios.

- Incluir la denominación completa del Tercero y, en su caso, los nombres comerciales con los que es conocido, así como una breve reseña de su historia corporativa y de negocios.
- Acompañar copia simple de la escritura constitutiva del Tercero.
- Dirección completa en donde se realizarán cada uno de los procesos, servicios y/o los centros de datos (primario y secundario) en donde se almacenará y procesará la información (calle, número exterior e interior, delegación o municipio, código postal, estado y país).

III. Servicios que prestará el Tercero.

En este apartado se incluirá la descripción del proceso operativo o de administración de base de datos y sistemas informáticos objeto de los servicios, proporcionando una descripción detallada acerca de ellos.

IV. Descripción de los mecanismos que permitirán a la Institución contar con la información detallada y actualizada de cada una de las operaciones y registros en territorio nacional, en un medio que permita su consulta en caso de interrumpirse el servicio del Proveedor.

Asimismo, mencionar los mecanismos que implementará la Institución para mantener en sus oficinas principales, en territorio nacional, documentación e información de las evaluaciones, resultados de auditorías y reportes de desempeño del Proveedor.

V. Información a se refieren los artículos 318, fracciones II y VII de la CUB.

En este apartado deberá contenerse la información que se describe en la Sección de requisitos legales de la presente Guía.

VI. Señalar la fecha probable de la celebración del contrato de prestación de servicios.

La CNBV tendrá la facultad de requerirle a la Institución el proyecto del contrato y, en su caso, el contrato celebrado, con su traducción al idioma español.

En su caso, las instituciones de banca de desarrollo remitirán el contrato respectivo, una vez concluidos los procedimientos a que se refieren las fracciones I y II del Artículo 26 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de resultar aplicable esta última ley.

VII. Declaración respecto de si alguno de los servicios estará sujeto a subcontratación, en cuyo caso mencionar a todos y cada uno de los Proveedores que participan.[2]

VIII. Anexos del escrito de solicitud.

IX. Incluir un índice de los anexos que servirán de soporte documental para acreditar lo manifestado en el escrito de solicitud y el cumplimiento de los requisitos que se mencionan en la Sección II de la presente Guía.

X. Puntos petitorios.

Incorporar de manera expresa la solicitud relativa a la autorización para la contratación con Terceros de la prestación de servicios, para la realización de un proceso operativo o para la administración de bases de datos, que se proporcionen o ejecuten parcial o totalmente fuera de territorio nacional o por residentes en el extranjero, en los términos del planteamiento que se presente, para todos los efectos legales a que haya lugar.

[2] Si alguno de los servicios es subcontratado por Proveedores en el extranjero, se deberá requerir autorización.

Sección II
Requisitos legales

a) Aspectos generales

I. Escrito de solicitud y Aviso (artículos 326, 328 y 318, fracción II de la CUB)

1. Incorporar que la Institución cuenta con un informe que especifique:

   - Los procesos operativos o de administración de bases de datos o sistemas informáticos que sean objeto de los servicios a contratar, y
   - Los criterios y procedimientos para seleccionar al Tercero. Dichos criterios y procedimientos estarán orientados a evaluar la experiencia, capacidad técnica y recursos humanos del Tercero con quien se contrate para prestar el servicio con niveles adecuados de desempeño, confiabilidad y seguridad, así como los efectos que pudieran producirse en una o más operaciones que realice la Institución.

2. Remitir la certificación o acta que contenga la aprobación del Consejo o del Comité de Riesgos de la Institución de la evaluación del impacto que las contrataciones a que se refiere el Capitulo XI del Título quinto de la CUB, pudieran tener cualitativa o cuantitativamente en las operaciones que realice la Institución, conforme a su objeto, tomando en cuenta para ello, lo siguiente:

   a) La capacidad de la institución para en caso de contingencia mantener la continuidad operativa y la realización de operaciones y servicios con sus clientes.
   b) La complejidad y tiempo requerido para encontrar un Tercero que, en su caso, sustituya al originalmente contratado.
   c) La habilidad de la Institución para mantener controles internos apropiados y oportunidad en el registro contable, así como para cumplir con los requerimientos regulatorios en caso de suspensión del servicio por parte del Tercero.
   d) El impacto que la suspensión del servicio tendría en las finanzas, reputación y operaciones de la Institución.
   e) La vulnerabilidad de la información relativa a los clientes.

   En ambos casos la Institución deberá hacer mención expresa del documento en el que se encuentren contenidos tanto el informe como la aprobación arriba mencionada y agregar un ejemplar del mismo.

3. Adicionalmente para el caso de los servicios a que se refiere el artículo 328 de la CUB, la Institución deberá acompañar a su escrito de solicitud la documentación que acredite el cumplimiento de los requisitos señalados en el artículo 318 de la CUB, así como los siguientes:

   I. Que los Terceros con los que se contrate residan en países cuyo derecho interno proporcione protección a los datos de las personas, resguardando su debida confidencialidad, o bien, los países de residencia mantengan suscritos con México acuerdos internacionales en dicha materia o de intercambio de información entre los organismos supervisores, tratándose de Instituciones financieras.

      En aquellos casos en los que México no tenga suscritos acuerdos internacionales en dicha materia, se acompañará de una opinión legal emitida por un abogado con ejercicio en el país de residencia del Tercero en la que se manifieste que el derecho interno de ese país proporciona protección a los datos de las personas, resguardando su debida confidencialidad.

      Considerar que el presente requisito se deberá acreditar igualmente respecto de cualquier tercero subcontratado por el Proveedor.

   II. Que las Instituciones manifiesten a la CNBV que mantendrán en sus oficinas principales ubicadas en los Estados Unidos Mexicanos, al menos la documentación e información relativa a las evaluaciones, resultados de auditorías y reportes de desempeño. Asimismo, cuando la Comisión lo requiera deberán proporcionar tal documentación en idioma español.

   III. Que se cuente con la aprobación del Consejo o, en su caso, del Comité de Auditoría o del Comité de Riesgos, haciendo constar en el acuerdo respectivo los aspectos siguientes:

      a) Que al contratar los servicios no se pone en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Institución.
      b) Que las prácticas de negocio del Tercero son consistentes con las de operación de la Institución.
      c) Que no habría impacto en la estabilidad financiera o continuidad operativa de la Institución, con motivo de la distancia geográfica y, en su caso, del lenguaje que se utilizará en la prestación del servicio.
      d) Las medidas que implementarán en los supuestos previstos por la fracción VII del Artículo 318 de la CUB.

b) Contrato de prestación de servicios (artículo 318, fracción III de la CUB)

El modelo de contrato de prestación de servicios deberá prever la aceptación incondicional del Tercero que proporcione el servicio, para:

1. De manera expresa:

   a) Recibir visitas domiciliarias por parte del auditor externo de la Institución, de la CNBV o de los Terceros que la propia CNBV designe en términos de lo dispuesto por el Artículo 46 Bis 1 y el Artículo 117 de la LIC, a efecto de llevar a cabo la supervisión correspondiente, con el propósito de obtener información para constatar que los servicios contratados por la Institución le permiten a esta última cumplir con las disposiciones aplicables. Para que se realicen las visitas referidas, las Instituciones podrán designar un representante.
   b) Aceptar la realización de auditorías por parte de la Institución, con relación a los servicios objeto de dicho contrato, a fin de verificar la observancia de las disposiciones aplicables a las Instituciones.
   c) Entregar, a solicitud de la Institución, al auditor externo de la propia Institución y a la CNBV o al Tercero que dicha CNBV designe, libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitir el acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la prestación del servicio en cuestión.
   d) Informar a la Institución con por lo menos treinta días naturales de anticipación, respecto de cualquier reforma a su objeto social o en su organización interna que afecte la prestación del servicio objeto de la contratación.
   e) Guardar confidencialidad respecto de la información a la que se tenga acceso por la prestación del servicio, debiendo, además, establecer las medidas necesarias para mantener la seguridad de las operaciones y proteger la información de los clientes, manifestando entender y aceptar que, por virtud de lo señalado en el Artículo 46 Bis 1, párrafo Tercero de la LIC, lo dispuesto en el Artículo 142 de dicha ley también les será aplicable, así como a sus representantes, directivos y empleados, aun cuando dejen de laborar o prestar servicios a tales Prestadores de servicios.

   En caso de que los Prestadores de servicios subcontraten directamente el servicio prestado a la Institución, total o parcialmente, deberán remitir el contrato respectivo, el cual contemple lo previsto en el presente numeral 1.

2. En adición al numeral anterior, el contrato de prestación de servicios respectivo deberá prever lo siguiente:

   a) Las restricciones o condiciones respecto a la posibilidad de que el Tercero subcontrate, a su vez, la prestación del servicio.
   b) Las obligaciones que correspondan a la Institución y al Tercero, así como los procedimientos para vigilar el cumplimiento de dichas obligaciones.
   c) Los mecanismos para la solución de disputas relativas al contrato de prestación de servicios o comisión mercantil.
   d) Las obligaciones y responsabilidades de las partes para proteger la información de los clientes de la Institución, debiendo esta última considerar los requisitos que establece la legislación en materia de protección de datos personales para el tratamiento y transferencia de este tipo de datos, además de aquella relativa a la defensa de usuarios de servicios financieros y cualquier otra que tenga por objeto proteger los datos de los clientes de la Institución.
   e) La manifestación expresa de que la Institución responde, en todo momento, por el servicio que Terceros contratados por ella proporcionen a los clientes bancarios, aun cuando la realización de las operaciones correspondientes se lleve a cabo en términos distintos a los pactados; así como por el incumplimiento a las disposiciones en que incurran dichos Terceros, conforme a lo previsto en el Artículo 46 Bis 1, primer párrafo de la LIC.
   f) Los términos, condiciones y procesos para que el Prestador de servicios garantice a la Institución la transferencia, devolución y eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.
   g) Establecer medidas correctivas en caso de incumplimiento por parte de los Terceros a la CUB.

   Para los servicios proporcionados por una institución financiera del exterior que controle a las Instituciones filiales operando en México, solo será aplicable el inciso a) del presente numeral 2.

3. Los procesos operativos que serán materia de la contratación.

   Es conveniente que las operaciones que se mencionen en la cláusula respectiva, sean consistentes con las referidas en el escrito de solicitud. Asimismo, en la descripción de los procesos operativos deberán cuidar que estos incluyan de forma detallada cada uno de los servicios que aparecen en el contrato, y deberán ser soportados con un diagrama de flujo por proceso.

4. Declaración respecto de si alguno de los servicios estará sujeto a subcontratación, en cuyo caso mencionar a todos y cada uno de los Proveedores que participan.[3]

[3] Si alguno de los servicios es subcontratado por Proveedores en el extranjero, se deberá requerir autorización.

5. Remitir documento que contenga los lineamientos y mecanismos tendientes a la no afectación y adecuada prestación de los servicios de la Institución al público, su estabilidad financiera o continuidad operativa después de haber finalizado el contrato con el Prestador de servicios, considerando aquellos necesarios para verificar que este no conserve información alguna de la Institución o de sus clientes (artículo 318, fracción IV de la CUB).

6. Remitir el cumplimiento al Anexo 52 de la CUB, para la operación de Medios Electrónicos a contratar con relación a la utilización de infraestructura tecnológica o de telecomunicaciones.

Sección III

En materia de seguridad de la información

Tanto en el aviso en términos del artículo 326, como en la solicitud de autorización en términos del artículo 328 de la CUB, se deberá de incluir lo siguiente:

a) Diagrama de arquitectura en el que se muestren los componentes de seguridad y de redes de la infraestructura relacionada con el servicio que aseguren que solamente el tráfico autorizado es el permitido. Dicho diagrama deberá incluir a cada uno de los participantes en el servicio a contratar.

b) Especificar la información que será almacenada en la infraestructura tecnológica del Proveedor o sus subcontratados, ya sea de manera permanente o temporal.

c) Descripción de los mecanismos para el almacenamiento seguro de información que será resguardada en la infraestructura tecnológica del Proveedor o de sus subcontratados, incluyendo, entre otros, el algoritmo de cifrado y longitud o HASH. Considerar el uso de algoritmos de cifrado y HASH con longitudes de llave seguras.

d) Descripción de los mecanismos para el aseguramiento de los canales de comunicación, considerando cada uno de los nodos, desde el lugar en donde se origina la operación hasta su registro en los sistemas de la Institución, indicando qué información es transmitida por cada canal y los mecanismos de cifrado en cada uno de dichos canales. Considerar el uso de protocolos de comunicación seguros, tales como TLS versión 1.2 o superior, HTTPS, VPN, MPLS, indicando de estas últimas las configuraciones de seguridad que serán utilizadas para su uso.

e) Describir el procedimiento de administración de llaves de cifrado utilizadas por la Institución y por el Proveedor o sus subcontratados, incluyendo, entre otros, herramientas utilizadas y el proceso de intercambio de llaves entre la institución y el Proveedor o sus subcontratados.

f) Describir las herramientas o mecanismos utilizados para la configuración de reglas de seguridad y control de accesos a los sistemas e infraestructura tecnológica que reside en el Proveedor o subcontratado; asimismo, mencionar el área o personal responsable de la Institución o del Proveedor o subcontratado de realizar las actividades mencionadas.

g) Describir las medidas de borrado seguro para la destrucción de la información cuando deja de ser necesaria en el servicio o concluya la relación contractual, mencionando las herramientas o mecanismos utilizados para este fin, así como el personal o área responsable. Considerar, en su caso, la información almacenada de manera permanente y temporal.

h) Resultados de las últimas pruebas de vulnerabilidades y penetración realizadas a la infraestructura tecnológica utilizada para la prestación del servicio, tanto de la Institución como del Proveedor o sus subcontratados, así como la evidencia de las acciones para la mitigación de las vulnerabilidades identificadas en dichas pruebas o, en el caso del Proveedor o sus subcontratados, la evidencia de la certificación y resultados de la última auditoría en seguridad de la información realizada, SOC 2, tipo 2, que correspondan a la infraestructura tecnológica ubicada en los centros de datos del Proveedor que será utilizada en la prestación del servicio.

i) Descripción de los mecanismos utilizados para la gestión de accesos a los sistemas usados para la prestación de los servicios. Asimismo, proporcionar las políticas para la gestión de accesos de la Institución, en las que se incluya el uso de contraseñas robustas. En caso de contratación de servicios con Proveedores de infraestructura en la nube, las cuentas de usuarios con acceso a las consolas de administración o de acceso a servicios de dicha nube deberán autenticarse con al menos dos factores de autenticación (ejemplo OTP vía SMS).

j) Descripción del proceso de gestión de incidentes de seguridad de la información que llevarán a cabo la Institución y el Proveedor o sus subcontratados, en caso de presentarse un incidente de seguridad de la información. Asimismo, proporcionar las políticas y procedimientos de la Institución para la gestión de dichos incidentes, en los que se prevea lo establecido en el artículo 168 Bis 16 de la CUB.

k) Funciones del Oficial de Seguridad de la Institución respecto de los servicios contratados, al menos deberán incluir:

   i. Autorización y vigilancia sobre la administración de usuarios, tanto en México, como fuera del país
   ii. Mecanismos para tener acceso a las bitácoras de sistemas o aplicativos, cuando este lo requiera
   iii. Monitoreo periódico de bitácoras de acceso a la información de la Institución.

Sección IV

En materia de riesgo operacional y tecnológico

a) Descripción detallada de cada uno los servicios que aparecen en el contrato respectivo, la cual deberá incluir un diagrama de flujo por proceso.

b) Detallar la información de la Institución y clientes que será almacenada por el Proveedor en sus equipos o instalaciones, en su caso. El detalle deberá incluir, por ejemplo: nombres, direcciones, números de cuenta, saldos, teléfonos, correo electrónico, historial de crediticio, etc.

c) En caso de que los servicios se proporcionen utilizando algún esquema denominado "nube", detallar lo siguiente:

   i. Tipo de nube(s) (pública, privada o híbrida).
   ii. Tipo de servicio (PaaS, IaaS, SaaS)
   iii. Regiones y localidades en donde se almacenará, transmitirá o procesará la información.
   iv. Nombre del Proveedor de la nube.

   En esquemas de virtualización en infraestructura compartida con otros clientes del Proveedor, deberán proporcionar los controles que serán utilizados por la Institución para garantizar la confidencialidad, integridad y disponibilidad de la información.

   Asimismo, incluir un informe con la evaluación de los riesgos (operacionales y tecnológicos) que implican para la Institución el uso de infraestructura o tecnologías de nube (PaaS, IaaS, SaaS), el cual deberá contener por lo menos los siguientes rubros:

   - Identificación de procesos y funciones del negocio, relacionados con la importancia, criticidad de los sistemas y componentes críticos a contratar.
   - Identificación de responsabilidad compartida para los servicios a contratar.
   - Periodicidad de la evaluación de riesgos respecto a los servicios del Proveedor.
   - Riesgos que se identifiquen de la contratación de servicios en la nube en el caso de autorización como riesgos geográficos, sistema legal, riesgo de concentración, entre otros.

d) Nombre y descripción de la funcionalidad de los sistemas o procesos que, en su caso, serán contratados para la prestación del servicio.

e) Esquema de interrelación de aplicaciones o sistemas sujetos a la contratación, incluyendo los sistemas de la Institución.[4]

f) Diagrama de telecomunicaciones o esquemas de redundancia de punto a punto, para contar con enlaces de comunicación que minimicen el riesgo de la interrupción, de forma que se pueda apreciar la conexión existente entre cada uno de los participantes en la prestación del servicio (Proveedores, centros de datos, Institución, etc.), incluyendo los esquemas de redundancia, así como la descripción de los enlaces de comunicación y Proveedores de estos (ancho de banda, tipo de servicio, etc.).

g) Descripción de la estrategia de continuidad de negocio del Proveedor, en caso de contingencias, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo principales, así como indicar el responsable de revisión o validación por parte de la Institución de los resultados las pruebas de continuidad de negocio del Proveedor.

h) Descripción de la estrategia de continuidad de negocio de la Institución en caso de contingencias, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo principales presentadas por el Proveedor.

i) Clasificación de criticidad de los servicios proporcionados por el Proveedor.

j) Políticas y procedimientos de respaldo de información (periodicidad de los respaldos, tipo de información que se respalda, ciclo de vida de la cinta o discos, pruebas de respaldos y mecanismos de resguardo), incluyendo los responsables del proceso de elaboración de respaldos.

k) Mecanismos de la Institución para monitorear y vigilar la calidad en los servicios, así como vigilar los tiempos de respuesta de los sistemas y aplicaciones (sistemas o herramientas utilizadas, reportes generados, periodicidad, etc.).

l) Esquema de soporte técnico que el Proveedor de servicios brindará a la Institución (horarios y canales de atención), considerando que no deberá afectar la diferencia en husos horarios y días hábiles.

m) Políticas y procedimientos relativos a la realización de auditorías internas y externas sobre los servicios prestados por el Proveedor, dichas auditorías deberán realizarse por lo menos una vez cada 2 años.

4 Los sistemas o aplicaciones subcontratados deberán venir incluidos en el esquema de interrelación

n) Descripción de los mecanismos a través de los cuales los usuarios o clientes de la Institución podrán tener acceso a los aplicativos objeto del servicio, en su caso.

o) Mecanismos que permitirán a la Institución mantener bajo su resguardo, ya sea en infraestructura tecnológica propia o de terceros, en ambos casos en territorio nacional, los registros detallados de todas las operaciones que se realicen, así como de sus registros contables, de forma que se asegure la continuidad operativa en todo momento en el caso de tener información almacenada, transmitida o procesada en el extranjero.

   Los registros deberán mantenerse en formatos que permitan su consulta, operación y uso por parte de la CNBV en todo momento, con independencia de que cuente con el proceso operativo, servicio o sistema contratado por el Tercero, por lo que se deberá especificar el tipo de formato en el que se mantendrán dichos registros, así como el procedimiento para su consulta, operación y uso.

p) En caso de contratación de Terceros para procesos operativos o sistemas informáticos en los que un usuario o cliente instruya vía telefónica a realizar operaciones[5] a través de los representantes de la Institución o de los operadores de un Tercero debidamente autorizado y que impliquen almacenar las grabaciones de voz de clientes fuera de las oficinas de la Institución, detallar los mecanismos para mantener en sus instalaciones copia de las mismas en un formato y herramientas que permitan su acceso y consulta de forma inmediata, por los periodos que establecen en las disposiciones aplicables, especificando el tipo de formato en el que se mantendrán dichas grabaciones de voz, así como el procedimiento para su consulta y uso.

q) Describir mecanismos para mantener y actualizar una bitácora de acceso a la información por el personal autorizado.

r) En caso de contratación de servicios asociados al Capítulo X Del Uso del servicio de Banca Electrónica de la CUB, remitir la identificación del servicio y forma en que dará cumplimiento con los servicios a la CUB.

s) Características técnicas de los sistemas, equipos y aplicaciones objeto de la contratación. (Formato F-SA)

FIN DEL DOCUMENTO

5 Operaciones Monetarias. la transacción que implique transferencia o retiro de recursos dinerarios.