Anexos

Anexo 1. Requerimientos de un modelo regulatorio de tercerización de servicios en la nube para instituciones financieras

A. Componentes relacionados con requerimientos de información por parte de la institución financiera:

I. **Notificación y justificación del servicio:** las instituciones financieras deben comenzar el proceso de notificación bajo los requerimientos de la regulación, así como una descripción del tipo de servicio tercerizado y los alcances en términos de sus operaciones. El requisito de notificación debe existir únicamente para procesos críticos, no como un requisito estándar para cualquier proceso.

- Naturaleza, escala y complejidad de operaciones.
- Servicios por contratar: tipo de nube, categoría de funciones (críticas o materiales), tipo información y datos a procesar.

II. **Sistemas de identificación, gestión y diligencia de riesgos operativos de tercerización:** además de presentar un análisis de riesgos asociados a la tercerización de servicios en la nube, los directivos y consejos de las instituciones financieras tienen obligaciones y responsabilidades no delegables para asegurar que dichos servicios sean llevados a cabo en cumplimiento de las normas aplicables las instituciones financieras.[1]

- Evaluación de riesgos asociados con la migración a la nube.
- Plan de monitoreo y mitigación de riesgos.
- Gobernanza, líneas de reporte y definición de responsabilidades en el proceso de tercerización de la institución financiera.
- Identificación de buenas prácticas y requerimientos regulatorios en materia de seguridad, estabilidad de operaciones y protección de datos.
- Consideraciones de divergencia regulatoria transfronteriza.
- Portabilidad (*vendor lock-in*).
- Estrategia de migración de proveedor, terminación del servicio.
- Incorporación de las operaciones en la nube en el plan de continuidad del negocio y respaldo contingente local.
- Capacitación para la correcta gestión de la gobernanza y monitoreo de servicios tercerizados.

B. Componentes relacionados con requerimientos de información por parte del proveedor de servicios en la nube:

III. **Criterios de selección de proveedores:** las instituciones financieras deben evaluar la capacidad de cumplimiento de sus proveedores de servicios en la nube con los requerimientos regulatorios a los que están sujetas. Las guías de los reguladores financieros

[1] Las responsabilidades no delegables a terceros se encuentran establecidas en las regulaciones de Reino Unido (FCA), Estados Unidos (FFIEC) y Australia (APRA).

usualmente indican los requerimientos mínimos y estándares de controles internos que los proveedores deben cumplir en torno a temas de seguridad y manejo de datos. Este requisito debe ser aplicable únicamente para procesos críticos.

a. Garantías externas de provisión de servicios: adhesión y cumplimiento con estándares internacionales relevantes (certificación ISO 27000, ISO 27018 informes SOC, norma ISAE 3402, entre otras) y alcance de auditorías externas.
b. Criterios de disponibilidad de servicio, estabilidad financiera y operativa.
c. Coordinación entre jurisdicciones y reguladores para los criterios de residencia de los procesos, sistemas y almacenamiento de datos.
d. Transparencia, actualización y accesibilidad a documentación de procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado para instituciones financieras y reguladores.
e. Elaboración e informes periódicos del perfil de riesgo del proveedor.

C. Componentes relacionados con requerimientos de información sobre la relación contractual y operativa entre la institución financiera y el proveedor:

IV. **Aspectos contractuales, legales y regulatorios para el modelo de tercerización de servicios:** los reguladores financieros emiten también guías sobre el contenido y cláusulas necesarias en los contratos y acuerdos de provisión de servicios tercerizados. Estos requerimientos buscan establecer con claridad los términos y garantías que aseguren la definición de responsabilidades y la estabilidad de operaciones. También buscan establecer lineamientos contractuales mínimos referentes a los estándares de acceso, protección y propiedad de datos. Por último, se instruye a las instituciones financieras a establecer en sus contratos cláusulas de procedimientos en caso de fallas y vulnerabilidades, terminación de operaciones, planes de cancelación de servicio y mecanismos de transición y portabilidad.[2]

- Condiciones y limitaciones de tercerización por parte del proveedor.
- Definición de responsabilidades.
- Condiciones de seguridad, riesgo de ciberataques y mecanismos de mitigación (certificaciones de seguridad como ISO 27001 e informes de auditoría SOC).
- Política de acceso y residencia de datos: jurisdicción del proveedor y sitios de procesamiento o almacenamiento
- Manejo y transferencia de datos e información sensible: cumplimiento con regulación de protección de datos personales y libertad de elegir la ubicación del almacenamiento y procesamiento.
- Acceso efectivo a datos, sistemas e instalaciones para instituciones financieras, auditores y reguladores: riesgo político, operativo y legal en materia de supervisión y continuación de servicios en jurisdicciones internacionales.
- Política de propiedad y derechos de uso de la información.
- Cláusulas de cumplimiento a lo largo de la cadena de valor o ecosistema del servicio.
- Planes contingentes en caso modificaciones a términos y condiciones de servicio
- Mecanismos de respaldo, independencia y borrado seguro de información.
- Plan de terminación de contrato, mecanismos de transición y portabilidad de servicios.
- Plan de continuidad en caso de suspensión de actividades del proveedor.

[2] Cloud computing, "Outsourcing to the cloud for financial institutions", https://www.bakerinform.com/home/2016/2/22/outsourcing-to-the-cloud-for-financial-institutions

- Vigilancia y monitoreo del proveedor de servicios: las instituciones financieras tienen la obligación de establecer mecanismos de vigilancia y auditoría sobre sus proveedores, tanto para ellos como para los reguladores.

D. Componentes relacionados con requerimientos de reportes sobre el desarrollo de la relación contractual y de monitoreo entre la institución financiera y el proveedor de servicios:

V. Documentación y verificación periódica de cumplimiento para reguladores:

- Notificación de inicio o modificación de contratación de servicios tercerizados.
- Identificación de proveedores y contratistas asociados.
- Descripción de los procesos que serán manejados en la nube (aplicaciones, tipo de datos, productos y servicios asociados).
- Ubicación física o región donde se procesarán y almacenarán los datos.
- Certificaciones otorgadas al proveedor del servicio y/o sitio de procesamiento.
- Relación de auditorías a las que se somete el proveedor de servicios contratado.
- Información sobre los niveles de servicio establecidos.
- Diagrama con la plataforma tecnológica que soportará los servicios contratados.
- Documentación completa de los procesos, procedimientos y aplicaciones que se ejecutan en la nube.
- 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.
- Diagramas de red que permitan identificar la plataforma que soporta el servicio contratado.
- Procedimientos para verificar el cumplimiento de los acuerdos, regulaciones y niveles de servicio establecidos con el proveedor de servicios en la nube.
  Reportes generales de auditoría, pruebas de vulnerabilidades y estado actual de los servicios contratados.

Anexo 2. Requerimientos del modelo regulatorio de la Circular Única de Bancos (Sección Tercera y Cuarta del Capítulo XI) para la tercerización de servicios para instituciones financieras

A. Componentes relacionados con requerimientos de información por parte de la institución financiera:

Justificación y caso de negocio:

- Proyecto de contrato de prestación de servicios y fecha probable de celebración.
- Informe que especifique los procesos operativos o de administración de bases de datos y sistemas informáticos de la Institución que sean objeto de los servicios a contratar.
- Informe técnico que especifique el tipo de operaciones o servicios bancarios que habrán de celebrarse utilizando la base tecnológica que le sea proveída por terceros o comisionistas,

así como la forma en que se dará cumplimiento a los lineamientos mínimos de operación y seguridad, que se señalan en el Anexo 52 de las presentes disposiciones.

Sistemas de identificación, gestión y diligencia de riesgos operativos de subcontratación:

- Establecer los criterios que permitan a las Instituciones evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones que realice la Institución tomando en cuenta:

    - La capacidad de la Institución para en caso de contingencia mantener la continuidad operativa y la realización de operaciones y servicios con sus clientes.
    - La complejidad y tiempo requerido para encontrar un tercero que, en su caso, sustituya al originalmente contratado.
    - La limitación en la toma de decisiones que trasciendan en forma significativa en la situación administrativa, financiera, operacional o jurídica de la propia Institución.
    - 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 o comisionista.
    - El impacto que la suspensión del servicio tendría en las finanzas, reputación y operaciones de la Institución.
    - La capacidad de la Institución de participar eficientemente en el sistema de pagos.
    - La vulnerabilidad de la información relativa a los clientes.

- Las Instituciones, en sus políticas relativas a la contratación de servicios o comisiones, contemplarán como medidas de evaluación respecto de los servicios o comisiones a que se refiere este capítulo, lo siguiente:

    - La capacidad de los terceros o comisionistas para implementar medidas o planes que permitan mantener la continuidad del servicio con niveles adecuados de desempeño, confiabilidad, capacidad y seguridad.
    - La integridad, precisión, seguridad, confidencialidad, resguardo, oportunidad y confiabilidad en el manejo de la información generada con motivo de la prestación de los servicios o comisiones.
    - El acceso a dicha información, a fin de que sólo puedan tener acceso a ella, las personas que deban conocerla.
    - Los métodos con que cuenta la Institución para evaluar el cumplimiento al contrato correspondiente, o bien, la adecuada prestación de los servicios o comisiones.
    - Los criterios y procedimientos para calificar periódicamente la calidad del servicio.
    - La capacidad de las Instituciones de mantener la continuidad en la prestación de los servicios o comisiones que se hubieren contratado, o bien, las opciones externas con que se cuenta en cualquier caso, a fin de disminuir la vulnerabilidad operativa de la Institución.
    - La afectación de los Niveles de Tolerancia al Riesgo.
    - La capacidad de las Instituciones, en la Administración Integral de Riesgos para identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos que puedan derivarse de la prestación de los servicios o comisiones a que se refiere este capítulo.
    - La capacidad del Sistema de Control Interno para cumplir con las políticas y procedimientos que regulen y controlen la prestación de los servicios o comisiones a que se refiere este capítulo.

B. Componentes relacionados con requerimientos de información por parte del proveedor subcontratado de servicios en la nube:

Criterios de selección de proveedores:

- Criterios y procedimientos para seleccionar al tercero.
    - Evaluar la experiencia, capacidad técnica y recursos humanos del tercero
    - Niveles adecuados de desempeño confiabilidad y seguridad
    - Efectos que pudieran producirse en una o más operaciones que realice la Institución.

C. Componentes relacionados con requerimientos de información sobre la relación contractual y operativa entre la institución financiera y el proveedor subcontratado:

Aspectos contractuales, legales y regulatorios para el modelo de subcontratación de servicios:

- Prever en el contrato de prestación de servicios
    - Aceptar la realización de auditorías y visitas domiciliarias por parte del auditor externo de la Institución o de la Comisión
    - Entregar a solicitud de la Institución, al auditor externo de la propia Institución y a la Comisión, libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate.
    - Acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la prestación del servicio en cuestión.
    - Informar a la Institución respecto de cualquier reforma a su objeto social o en su organización interna que pudiera afectar la prestación del servicio objeto de la contratación.
    - Guardar confidencialidad respecto de la información relativa a las operaciones activas, pasivas y de servicios que los comisionistas celebren con los clientes bancarios, así como la relativa a estos últimos.

Vigilancia y monitoreo del proveedor de servicios:

- Contar con planes para evaluar y reportar a la Institución el desempeño del tercero, así como el cumplimiento de la normativa aplicable relacionada con dicho servicio.
- Prever que la Institución defina y vigile el cumplimiento de los mecanismos para el adecuado manejo, control y seguridad de la información generada, recibida, transmitida, procesada o almacenada en la ejecución de los servicios que se refieran a la utilización de infraestructura tecnológica, de telecomunicaciones o de procesamiento de información, que se realicen parcial o totalmente fuera del territorio nacional.
- Contar con políticas y procedimientos para vigilar el desempeño del tercero y el cumplimiento de sus obligaciones contractuales. Dichas políticas y procedimientos deberán contener aspectos relativos a:
    - Restricciones o condiciones, respecto a la posibilidad de que el tercero o comisionista subcontrate, a su vez, la prestación del servicio.

- La confidencialidad y seguridad de la información de los clientes.
- Las obligaciones de la Institución y del tercero o comisionista, los procedimientos para vigilar su cumplimiento, así como en su caso, las consecuencias legales en el evento de incumplimiento
- Los mecanismos para la solución de disputas relativas al contrato de prestación de servicios y comisión.
- Los planes de continuidad del negocio, incluyendo los procedimientos de contingencia en caso de desastres.
- El uso y la explotación a favor de la Institución sobre las bases de datos producto de los servicios y comisiones.
- El establecimiento de lineamientos que aseguren que los terceros reciban periódicamente una adecuada capacitación e información, en relación con los servicios o comisiones contratados.
- El cumplimiento de los lineamientos mínimos de operación y seguridad que se señalan en los Anexos 52 y 58, en su caso, de las presentes disposiciones, si los servicios o comisiones a contratar se refieren a la utilización de infraestructura tecnológica o de telecomunicaciones.

- En caso de incumplimiento por parte de los terceros o comisionistas a las disposiciones aplicables, las Instituciones deberán implementar las medidas correctivas necesarias.

D. Componentes relacionados con requerimientos de reportes sobre el desarrollo de la relación contractual y de monitoreo entre la institución financiera y el proveedor de servicios:

Documentación y verificación periódica de cumplimiento para reguladores:

- Aviso previo a la contratación
- Documentación que acredite el cumplimiento de los requisitos siguientes:

  - Que los terceros o comisionistas 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 entidades financieras.
  - Que las Instituciones manifiesten a la Comisión 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.
  - Que al contratar los servicios o comisiones no se pone en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Institución.
  - Que las prácticas de negocio del tercero o comisionista son consistentes con las de operación de la Institución.
  - 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.

- Facultad de requerir a la Institución que la prestación de dicho servicio no se realice a través del tercero o comisionista señalado en el aviso a que se refiere el presente artículo, cuando

considere que por los términos y condiciones de contratación del servicio o las políticas y procedimientos de control interno, la infraestructura tecnológica o de comunicaciones materia del servicio, sea previsible que no estarían en posibilidad de cumplir con las disposiciones aplicables a la propia Institución y, en su caso, pueda verse afectada la estabilidad financiera o continuidad operativa de esta última, a juicio de la Comisión.

- Las Instituciones requerirán de la autorización de la Comisión, para la contratación con terceros de la prestación de servicios o comisiones, 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 todo momento, con independencia de que los procesos de que se trate puedan o no afectar cualitativa o cuantitativamente una o más de las operaciones que realice la Institución.
- La Comisión, previo derecho de audiencia que se otorgue a la Institución, podrá ordenar la suspensión parcial o total, temporal o definitiva, de la prestación de los servicios o comisiones a través del tercero de que se trate, cuando a juicio de la propia Comisión, pueda verse afectada la estabilidad financiera, la continuidad operativa de la Institución o en protección de los intereses del público, o bien, cuando las Instituciones incumplan con las disposiciones contenidas en el presente capítulo y las demás que resulten aplicables. Lo anterior, salvo que al ejercer el citado derecho de audiencia, la Institución presente un programa de regularización para ser autorizado por la Comisión, la cual tendrá un plazo de treinta días naturales, contado a partir de que la Institución respectiva presente la solicitud correspondiente, a efecto de resolver lo conducente.
- El programa de regularización citado deberá reunir, cuando menos, los requisitos siguientes:

    - Señalar las acciones que habrán de implementar para dar cumplimiento a las disposiciones aplicables y asegurar la estabilidad financiera o continuidad operativa de la Institución.
    - Especificar las etapas y plazos de cada una de las acciones a implementar. En ningún caso la ejecución y cumplimiento del programa deberá exceder de tres meses, contado a partir de su autorización.
    - Indicar el personal responsable de la instrumentación de cada una de las etapas del programa.

      Las Instituciones deberán contar con un padrón que contenga el tipo y características de cada uno de los servicios y operaciones que tenga contratadas, así como los datos generales de los prestadores de servicios o comisionistas, distinguiendo aquellos que cuentan con residencia en el territorio nacional o en el extranjero.

Anexo 3. Guía para la autorización de contratación con terceros de servicios o comisiones de la SHCP y CNBV

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 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 o comisiones. Para el caso de 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.

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

I. Información relativa a la Institución de crédito. En este apartado se deberá contener la denominación de la Institución. El aviso correspondiente deberá estar suscrito por el director general de la Institución.
II. Información del tercero con el que se pretende celebrar el contrato de prestación de servicios o comisión.
    - Incluir la denominación completa del tercero y, en su caso, los nombres comerciales con los que es conocido y 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, estado y país).
III. Servicios o comisiones 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 o comisiones, proporcionando una descripción detallada acerca de ellos.
IV. Información a la que se refieren los artículos 318, fracciones II y VII de la CUB. En este apartado deberá contener 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 o comisión. La Institución deberá cuidar que el escrito de aviso se presente con por lo menos veinte días hábiles a la fecha en que pretenda 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. Si alguno de los servicios es subcontratado por proveedores en el extranjero, se deberá requerir autorización.
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 los 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 o comisiones, 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, será en formato libre suscrito por el director general de la Institución. Este escrito se presentará a la Vicepresidencia 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 la comisión

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 Institución.
II. Información del tercero con el que se pretende celebrar el contrato de prestación de servicios o comisión.
   - Incluir la denominación completa del tercero y, en su caso, los nombres comerciales con los que es conocido y 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, estado y país).
III. Servicios o comisiones 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 o comisiones, 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 Entidad para mantener en sus oficinas principales, en territorio nacional, documentación e información de las evaluaciones, resultados de auditorías y reportes de desempeño del proveedor de servicios.
V. Información a la que 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 o comisión. 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. Si alguno de los servicios es subcontratado por proveedores en el extranjero, se deberá requerir autorización.
VIII. Anexos del escrito de solicitud. 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.

IX. Puntos petitorios. Incorporar de manera expresa la solicitud relativa a la autorización para la contratación con terceros de la prestación de servicios o comisiones, 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.

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 y sistemas informáticos que sean objeto de los servicios o comisiones 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. Indicar que la Institución ha establecido los criterios que le permitan, a través de su director general, evaluar la medida en que las respectivas contrataciones pudieran afectar cualitativa o cuantitativamente las operaciones que realice la propia Institución, conforme a su objeto, tomando en cuenta para determinar tal circunstancia, 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 limitación en la toma de decisiones que trasciendan en forma significativa en la situación administrativa, financiera, operacional o jurídica de la propia Institución.
d) 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.
e) El impacto que la suspensión del servicio tendría en las finanzas, reputación y operaciones de la Institución.
f) La capacidad de la Institución de participar eficientemente en el sistema de pagos.
g) 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 los criterios arriba mencionados y agregar un ejemplar del mismo.

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

3. Adicionalmente para el caso de los servicios o comisiones 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 y los siguientes:

   I. Que los terceros o comisionistas 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 entidades financieras. En los casos en México no tenga suscritos acuerdos internacionales en dicha materia, se acompañará de una opinión legal emitida por un abogado del 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.

   II. Que las Instituciones manifiesten a la Comisión 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 o comisiones no se pone en riesgo el adecuado cumplimiento de las disposiciones aplicables a la Institución. b) Que las prácticas de negocio del tercero o comisionista 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.

   IV. Que cuenten con políticas y procedimientos para vigilar el desempeño del tercero o comisionista y el cumplimiento de sus obligaciones contractuales. Dichas políticas y procedimientos deberán contener aspectos relativos a: a) Las restricciones o condiciones, respecto a la posibilidad de que el tercero o comisionista subcontrate, a su vez, la prestación del servicio. b) La confidencialidad y seguridad de la información de los Socios. c) Las obligaciones del tercero, los procedimientos para vigilar su cumplimiento, así como en su caso, las consecuencias legales en el evento de incumplimiento. d) Los mecanismos para la solución de disputas relativas al contrato de prestación de servicios. e) Los planes de continuidad del negocio, incluyendo los procedimientos de contingencia en caso de desastres. f) El uso y la explotación a favor de la Institución sobre las bases de datos producto de los servicios y comisiones. g) El establecimiento de lineamientos que aseguren que los terceros reciban periódicamente una adecuada capacitación e información, en relación con los servicios contratados. h) El cumplimiento de los lineamientos mínimos de operación y seguridad que se señala el Anexo 52, si los servicios a

contratar se refieren a la utilización de infraestructura tecnológica o de telecomunicaciones. La Institución deberá hacer mención expresa del documento en el que se encuentren contenidas las políticas y procedimientos arriba mencionados, así como agregar un ejemplar del mismo.

V. Que cuenten con planes para evaluar y reportar al Consejo de Administración, al Comité de Auditoría, al Auditor Interno o al Director de la Institución, según la importancia del servicio contratado, el desempeño del tercero o comisionista, así como el cumplimiento de la normativa aplicable relacionada con dicho servicio. Tratándose de servicios de procesamiento de información, la Institución deberá practicar al menos cada dos años, auditorías que tengan por objeto verificar el grado de cumplimiento del presente capítulo, así como de lo establecido en el Anexo 52.

VI. Que prevean que el Director, el Comité de Auditoría, así como el Auditor Interno de la Institución definan y vigilen, acorde a su competencia, el cumplimiento de los mecanismos para el adecuado manejo, control y seguridad de la información generada, recibida, transmitida, procesada o almacenada en la ejecución de los servicios o comisiones que se refieran a la utilización de infraestructura tecnológica, de telecomunicaciones o de procesamiento de información, que se realicen parcial o totalmente fuera del territorio nacional.

b) Contrato de prestación de servicios o comisión (artículo 327 de la CUB). El modelo de contrato de prestación de servicios o comisión deberá contener cláusulas relativas a:

1. La aceptación incondicional de quien proporcione el servicio, para:

a) Recibir visitas domiciliarias por parte del auditor externo de la Institución, de la CNBV o de los terceros que la propia Comisión designe en términos de lo dispuesto por el artículo 117 de la LIC, a efecto de llevar a cabo la supervisión correspondiente, con el exclusivo propósito de obtener información para constatar que las comisiones contratados por la Institución, le permiten a esta última cumplir con las disposiciones de la LIC que le resultan 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, en relación con los servicios o comisiones 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 Comisión o al tercero que ésta designe, libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitirá que se tenga acceso al personal responsable y a sus oficinas e instalaciones en general, relacionados con la comisión 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 pudiera afectar la realización de la comisión objeto de la contratación.
e) En su caso, guardar confidencialidad respecto de la información relativa a las operaciones activas, pasivas y de servicios que los comisionistas celebren con los clientes bancarios, así como la relativa a estos últimos

2. Los procesos operativos que serán materia de la contratación o de la comisión. 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 éstos 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.

3. Confidencialidad de la información. La Institución debe establecer claramente la obligación por parte del prestador del servicio de mantener controles adecuados que garanticen guardar la debida confidencialidad de los datos e información en la realización de las operaciones contratadas.

4. Propiedad de la información (que la misma permanezca en la Entidad).

5. Las sanciones y, en su caso, penas convencionales por los incumplimientos al contrato, incluyendo lo dispuesto por los artículos 330 y 331 de la CUB

6. 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. Si alguno de los servicios es subcontratado por proveedores en el extranjero, se deberá requerir autorización.

Sección IV (sic) Anexos

Anexo 52

a) Descripción detallada de cada uno de los servicios que aparecen en el contrato respectivo, la cual deberá incluir un diagrama de flujo por proceso.
b) Detallar la información de la Entidad 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 crediticio, etc.
c) En caso de que los servicios se proporcionen utilizando algún esquema denominado "nube", detallar lo siguiente:

   i. Tipo de nube (pública, privada o híbrida)
   ii. Localidades específicas en donde se almacenará y procesará la información
   iii. Nombre del proveedor de la nube
   iv. Proyecto de contrato

   Tratándose de procesos de clientes o de procesos necesarios para la operación de la Entidad no se permitirá el uso de "nubes públicas". En esquemas de virtualización en infraestructura compartida con otros clientes del proveedor, deberán proporcionar los controles que serán utilizados por la Entidad para garantizar la confidencialidad, integridad y disponibilidad de la información.

   Tratándose de "nubes privadas o híbridas" el proveedor deberá permitir las revisiones por parte de la Comisión, por lo que la Entidad deberá proporcionar la ubicación exacta del lugar de procesamiento de información (país y población o ciudad) y solamente será aceptable en países con los que se cuenten con convenios de colaboración con las Autoridades Financieras.

   Asimismo, incluir un informe con la evaluación de los riesgos (operacionales y tecnológicos) que implican para la Entidad el compartir infraestructura con otras Entidades, el cual deberá

contener por lo menos los siguientes rubros: Soporte técnico, Ambiente de pruebas, Integridad, disponibilidad y confidencialidad de la información, y Control de accesos de terceros.

d) Nombre y descripción de la funcionalidad de los sistemas 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 Entidad. Los sistemas o aplicaciones subcontratados deberán venir incluidos en el esquema de interrelación
f) Diagrama de telecomunicaciones en donde se pueda apreciar la conexión existente entre cada uno de los participantes en la prestación del servicio (proveedores, centros de datos, Entidad, etc.), incluyendo los esquemas de redundancia, así como la descripción de los enlaces de comunicación y proveedores de los mismos (ancho de banda, tipo de servicio, etc.).
g) Características técnicas de los sistemas, equipos y aplicaciones objeto de la contratación. (Formato F-SA)
h) Descripción de la estrategia de continuidad de negocios del proveedor de servicios, en caso de contingencias, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo principales.
i) Descripción de la estrategia de continuidad de negocios (Business Continuity Plan) de la Entidad en caso de interrupción de servicios por parte del proveedor.
j) Políticas y procedimientos de respaldo de información del proveedor de servicios (periodicidad de los respaldos, tipo de información que se respalda, ciclo de vida de la cinta y mecanismos de resguardo).
k) Mecanismos de la Entidad 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 Entidad (horarios y canales de atención), considerando que no deberá afectar la diferencia en husos horarios y días hábiles.
m) Mecanismos de cifrado para la transmisión de información sensible de punto a punto, así como en cada uno de los nodos (desde el lugar en donde se origina la operación hasta su registro en los sistemas de la Entidad).
n) Funciones del Oficial de Seguridad de la Entidad 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 Entidad
o) Políticas y procedimientos relativos a la realización de auditorías sobre los servicios prestados por el proveedor, dichas auditorías deberán realizarse por lo menos una vez cada 2 años.
p) Descripción de los mecanismos a través de los cuales los usuarios de la Entidad podrán tener acceso a los aplicativos, objeto del servicio, en su caso.
q) Describir el medio a través del cual accederán los usuarios privilegiados (administradores de sistemas operativos y de bases de datos) a los aplicativos, sistemas y bases de datos.

Anexo 4. Requerimientos del modelo regulatorio de la Circular Única de Bancos (Anexo 52) para la subcontratación de servicios para instituciones financieras

Lineamientos mínimos de operación y seguridad para la contratación de servicios de apoyo tecnológico

Las Instituciones deberán considerar los aspectos siguientes:

I. Aspectos en materia de operación.

   a. Esquemas de redundancia o mecanismos alternos en las telecomunicaciones de punto a punto que permitan contar con enlaces de comunicación que minimicen el riesgo de interrupción en el servicio de telecomunicaciones.
   b. Estrategia de continuidad en los servicios informáticos que proporcionen a la Institución la capacidad de procesar y operar los sistemas en caso de contingencia, fallas o interrupciones en las telecomunicaciones o de los equipos de cómputo centrales y otros que estén involucrados en el servicio de procesamiento de información de operaciones o servicios.
   c. Mecanismos para establecer y vigilar la calidad en los servicios de información, así como los tiempos de respuesta de los sistemas y aplicaciones.
   d. Esquema de soporte técnico, a fin de solucionar problemas e incidencias, con independencia, en su caso, de las diferencias en husos horarios y días hábiles.

II. Aspectos en materia de seguridad.

   a. Medidas para asegurar la transmisión de la Información Sensible del Usuario en forma cifrada punto a punto y elementos o controles de seguridad en cada uno de los nodos involucrados en el envío y recepción de datos.
   b. Establecimiento de funciones del oficial de seguridad. Para efectos de que la Institución contratante se mantenga enterada del acceso y uso de la información, deberá designar a una persona que se desempeñe como oficial de seguridad en la Institución, quien gozará de independencia respecto de las áreas operativas, de auditoría y de sistemas, y cuya función consistirá, entre otras cosas, en administrar y autorizar los accesos. Dichos accesos deberán corresponder a la necesidad de conocer la información de acuerdo a las funciones documentadas del puesto. Asimismo, el oficial de seguridad deberá contar en todo momento con los registros de todo el personal que tenga acceso a la información relacionada con las operaciones de la Institución, incluso de aquél ubicado fuera del territorio nacional, en cuyo caso el personal autorizado para acceder a dicha información deberá ser autorizado por el responsable de las funciones de contraloría interna señaladas en la fracción V del Artículo 166 de las presentes disposiciones.
   c. Esquema mediante el cual se mantendrá en una oficina de la institución de crédito contratante, la bitácora de acceso a la información por el personal debidamente autorizado.

III. Auditoría y Supervisión.

a. Políticas y procedimientos relativos a la realización de auditorías internas o externas sobre la infraestructura, controles y operación del centro de cómputo del tercero, relacionado con el ambiente de producción para la institución de crédito, al menos una vez cada dos años con el fin de evaluar el cumplimiento de lo mencionado en el presente anexo. Tratándose de las operaciones a que se refiere la fracción X del Artículo 319 de las disposiciones que se realicen a través de Administradores de Comisionistas, la auditoría a que se refiere el párrafo anterior, deberá realizarse por la propia Institución, al menos una vez al año.
Mecanismos de acceso al ambiente tecnológico, incluyendo información, bases de datos y configuraciones de seguridad, desde las instalaciones de la Institución en territorio nacional.

Anexo 5. Requerimientos del modelo regulatorio de la Ley para Regular las Instituciones de Tecnología Financiera

Artículo 39.- Las solicitudes para obtener las autorizaciones de la CNBV previstas en el presente Capítulo deberán acompañarse de lo siguiente:

X. La relación de los convenios o contratos con otras ITF o proveedores de servicios tecnológicos necesarios para la realización de procesos clave de negocio, gestión de bases de datos e Infraestructura Tecnológica para la realización de sus actividades;

Artículo 40.- La ITF que reciba la autorización en términos del presente Capítulo, deberá acreditar a la CNBV, con al menos treinta días hábiles de anticipación al inicio de operaciones, el cumplimiento de los requisitos siguientes: IV. Cuenta con la Infraestructura Tecnológica, controles internos necesarios para realizar sus actividades y otorgar sus servicios, así como con las políticas, procedimientos, manuales y demás documentación que conforme a esta Ley y las disposiciones que de ella emanen deban tener.

La CNBV podrá practicar las visitas de inspección que considere necesarias a efecto de verificar el cumplimiento de los requisitos a que se refiere este artículo. Tratándose de instituciones de fondos de pago electrónicos, las visitas de inspección deberán efectuarse por la CNBV y el Banco de México a fin de verificar el cumplimiento de lo dispuesto en este artículo, en el ámbito de sus respectivas competencias.

La CNBV podrá negar el inicio parcial o total de operaciones cuando no se acredite el cumplimiento de lo previsto en este artículo.

Artículo 54.- Las ITF podrán pactar con terceros, localizados en el territorio nacional o el extranjero, la prestación de servicios necesarios para su operación, de conformidad con las disposiciones de carácter general que para tal efecto emitan la CNBV respecto de instituciones de financiamiento colectivo y conjuntamente con el Banco de México respecto de las instituciones de fondos de pago electrónico. Dichas Autoridades Financieras podrán señalar en estas disposiciones el tipo de servicios que requerirán de autorización.

La contratación de los servicios a que se refiere el presente artículo no eximirá a las ITF, ni a sus directivos, empleados y demás personas que ocupen un empleo, cargo o comisión en ellas, de la obligación de observar lo establecido en el presente ordenamiento legal y en las disposiciones de carácter general que emanen de este.

La CNBV, con respecto a las disposiciones que le corresponda emitir de manera individual, así como a las disposiciones que emita conjuntamente con el Banco de México de conformidad con la presente Ley, y el Banco de México, con respecto a las otras disposiciones que emita en términos de esta Ley, estarán facultados en todo momento para efectuar actos de supervisión a los prestadores de servicios que sean contratados por las ITF en términos del primer párrafo de este artículo, o bien, para ordenar a las ITF la realización de auditorías a dichos terceros, quedando obligadas a rendir un informe a la CNBV o al Banco de México. La CNBV o el Banco de México deberán especificar el objeto de las inspecciones o auditorías, las cuales deberán circunscribirse a la materia del servicio contratado y al cumplimiento de lo previsto en esta Ley y las disposiciones que de ella emanen. Al efecto, las ITF deberán pactar en los contratos mediante los cuales se formalice la prestación de estos servicios, la estipulación expresa de que el tercero contratado acepta apegarse a lo establecido en el presente artículo.

Artículo 56.- Las ITF podrán utilizar equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos para otorgar sus servicios y podrán permitir el uso de la firma electrónica avanzada o cualquier otra forma de autenticación para dar acceso a sus Clientes a su Infraestructura Tecnológica, contratar sus productos y servicios o realizar Operaciones.

El funcionamiento y uso de tales equipos, medios y formas de autenticación se sujetará a los requisitos establecidos en las disposiciones de carácter general que para tal efecto emita la CNBV, respecto de las instituciones de financiamiento colectivo, o la propia CNBV y el Banco de México, de manera conjunta, respecto de las instituciones de fondos de pago electrónico.

Dichas formas de autenticación producirán los mismos efectos que las leyes otorgan a los documentos suscritos con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio, siempre que cumplan con las disposiciones a que se refiere este artículo.

Lo dispuesto en este artículo se aplicará sin perjuicio de aquellas otras facultades con que cuenta el Banco de México para regular las operaciones que efectúen las ITF relacionadas con las características de las Operaciones de estas últimas instituciones, así como sus actividades vinculadas con los sistemas de pagos.

Anexo 6. Requerimientos del modelo regulatorio de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf

Artículo 14.- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del

responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Artículo 20.- Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

Anexo 7. Requerimientos del modelo regulatorio del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Figura del encargado

Artículo 49. El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Obligaciones del encargado

Artículo 50. El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:

I. Tratar únicamente los datos personales conforme a las instrucciones del responsable;
II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables;
IV. Guardar confidencialidad respecto de los datos personales tratados;

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente.

Relación entre el responsable y el encargado

Artículo 51. La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.

Tratamiento de datos personales en el denominado cómputo en la nube

Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:
a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y

II. Cuente con mecanismos, al menos, para:
a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y
e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales. Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente. Las dependencias

reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube.

Remisiones de datos personales

Artículo 53. Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento. El encargado, será considerado responsable con las obligaciones propias de éste, cuando:
I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o
II. Efectúe una transferencia, incumpliendo las instrucciones del responsable

El encargado no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable conforme a lo previsto en el presente Reglamento.

Subcontratación de servicios

Artículo 54. Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. La persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado en la Ley, el presente Reglamento y demás disposiciones aplicables. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.

Autorización de la subcontratación

Artículo 55. Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el artículo anterior se entenderá como otorgada a través de lo estipulado en éstos. En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos a los que refiere el párrafo anterior, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación. En ambos casos, se deberá observar lo previsto en el artículo anterior.

Factores para determinar las medidas de seguridad

Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:
I. El riesgo inherente por tipo de dato personal;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico, y
IV. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

I. El número de titulares;
II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Acciones para la seguridad de los datos personales

Artículo 61. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:
I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
II. Determinar las funciones y obligaciones de las personas que traten datos personales;
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
VII. Llevar a cabo revisiones o auditorías;
VIII. Capacitar al personal que efectúe el tratamiento, y
IX. Realizar un registro de los medios de almacenamiento de los datos personales. El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.

Anexo 8. Criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

http://inicio.inai.org.mx/nuevo/ComputoEnLaNube.pdf

Sección II. Criterios mínimos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales

A. Criterios mínimos previos a la contratación o adhesión

I. Identifique los datos, procesos o funciones que se pretendan migrar al servicio de cómputo en la nube.
II. Defina el modelo de aprovisionamiento que garantice de mejor manera el control sobre el tratamiento de datos personales, según los datos, procesos o funciones que se pretenden migrar a la nube.
III. Defina de manera interna, las políticas y medidas de seguridad para el uso del servicio de cómputo en la nube.
IV. Evalúe todos los aspectos del servicio, así como los términos y condiciones a los que se sujeta el servicio a contratar.

Criterios

A.1. Reputación del Proveedor
- nivel de cumplimiento y la calidad del servicio que presta, o bien, si el Proveedor es un actor reconocido en el mercado de prestación de servicios de cómputo en la nube
- incidentes importantes, y si después de un incidente, el Proveedor es diligente con sus clientes, al tomar acciones que mitiguen su impacto.
- denunciado de manera pública medidas de seguridad deficientes
- sujetos de denuncias o investigaciones por autoridades de protección de datos personales alrededor del mundo, ASÍ COMO SU RESPUESTA
- claro y transparente respecto a su modelo de negocio, sus prácticas en el tratamiento de datos personales y su política de privacidad
- consultar las normas ISO/IEC 27018:2014 e ISO/IEC 19086-1:2016, como referencia para la contratación

A.2. Identidad del Proveedor
- Es importante que el Cliente cuente con información de la identidad y medios para contactar al Proveedor

A.3. Jurisdicción aplicable y ubicación geográfica de los datos personales
- La jurisdicción o normatividad que rige al Proveedor y al contrato
- ubicación geográfica de los centros de tratamiento de información. r preferencia por las jurisdicciones o zonas geográficas que cuenten con normativa en materia de protección de datos personales que sea similar a la aplicable en México
- ámbito geográfico en el cual se respalda la prestación del servicio

B. Criterios mínimos que se sugiere al Cliente considerar para controlar la prestación del servicio

I. Se recomienda al Cliente que opte por Proveedores que establezcan cláusulas que eviten que el Proveedor y sus subcontrataciones reclamen, en cualquier momento, la propiedad de la información proporcionada por el Cliente

II. Se recomienda al Cliente que elija Proveedores que cuenten con cláusulas, políticas, mecanismos o sistemas automatizados para:
- utilicen la información del Cliente únicamente para las finalidades establecidas en los términos del servicio.
- que el Cliente restrinja o modifique el tipo de tratamiento en el servicio, así como para limitar al Proveedor sobre el uso y divulgación de la información.
- Para mantener al Cliente informado sobre quiénes acceden a su información y para qué propósito, evitando los accesos no autorizados.
- que el Cliente pueda acceder, modificar o borrar información en cualquier momento durante la vigencia del servicio.
- Para eliminar o destruir la información del Cliente con métodos de borrado seguro,
- Para notificar al Cliente de cualquier cambio o actualización en la prestación del servicio,
- Para notificar las acciones del Proveedor en caso que ocurra un incidente que afecte la información del Cliente.

III. Se recomienda al Cliente elegir, de manera preferente, Proveedores que aseguren diligencia para:
- Notificar al Cliente cualquier falla o interrupción del servicio.
- Notificar al Cliente el acceso o solicitud de acceso de terceros a la información (incl.. autoridades competentes, nacionales o extranjeras)

- a identificación y la mitigación o remediación de una vulneración a la seguridad de los datos personales
- Ofrecer compensaciones o primas a los Clientes en caso de una falla o interrupción del servicio, o bien debido a una vulneración a la seguridad de los datos personales.
- Ofrecer al Cliente instrumentar acciones proactivas para proteger los datos personales.

Criterios
B.1. Transparencia en el servicio

- el Cliente debe conocer la existencia de las subcontrataciones que, en su caso, realice el Proveedor, s mecanismos implementados por los terceros subcontratados para garantizar la confidencialidad de los datos personales, La posibilidad de atender solicitudes de ejercicio de derechos ARCO y La supresión de los datos personales a través de métodos de borrado seguro u otro mecanismo
- el Cliente o responsable elija proveedores que tomen responsabilidad completa por los servicios subcontratados, sin que lo anterior implique que el Cliente pueda perder su calidad de responsable de los datos personales
- informes de transparencia respecto a las solicitudes de información que reciben por parte de autoridades locales, internacionales o constituidas en países terceros.

B.2. Cambios en los términos del servicio

- es obligatoria la contratación de servicios que garanticen la información oportuna al Cliente sobre cualquier cambio en el servicio, pero también es recomendable que, de manera proactiva, el Cliente monitoree esta información.

C. Criterios mínimos a considerar por el cliente para asegurar que el proveedor cuente con medidas de seguridad

I. Para cumplir con lo dispuesto por el inciso c, fracción II del artículo 52 del Reglamento, es recomendable que el Cliente elija Proveedores cuyos servicios cuenten con cláusulas, políticas, mecanismos o sistemas automatizados, al menos sobre las siguientes medidas de seguridad para:

- a la protección de la confidencialidad de la información almacenada en los sistemas del Proveedor y de sus subcontrataciones (cifrado y mecanismos de autenticación para el acceso)
- a protección de la confidencialidad de la información en tránsito (cifrado del canal de comunicaciones)
- la protección de la disponibilidad e integridad de la información del Cliente. Por ejemplo, a través de copias de seguridad o almacenamiento redundante.
- el aislamiento de la información de un cliente, respecto a la de otros clientes con los que se comparten elementos de cómputo en común. Por ejemplo, la administración de entornos virtuales.
- que el Cliente tenga control sobre el acceso y gestión de los datos, procesos o servicios. Por ejemplo, con contraseñas, gestión de identidades o certificados digitales

II. Se recomienda que el Cliente opte por Proveedores que además cuenten con las medidas siguientes:

- evidencia de estar sujetos a revisiones o auditorías por terceros de reconocido prestigio, o en cumplimiento con estándares internacionales, en particular de estándares como son ISO-27017 e ISO-27018. Asimismo, permitir revisiones o auditorías por parte del Cliente.

- evidencia de que sus servicios consideran la protección de datos personales desde el diseño o rediseño, como una característica intrínseca en sus operaciones
- Mostrar o estar en proceso de certificación por un organismo reconocido nacional o internacional, o bien contar con esquemas de seguridad o protección de datos personales apegados a estándares y mejores prácticas internacionales.

Criterios
C.1. Evaluación de riesgos para los datos personales

- es necesario que previo a la contratación de un servicio de cómputo en la nube, el Cliente realice un análisis de riesgos con relación al tratamiento de datos personales que efectúa en su organización
- Se recomienda tomar en consideración para la contratación de un Proveedor, las siguientes situaciones, que pueden convertirse en riesgos vinculados con el tratamiento de datos personales en el cómputo en la nube:
    - Falta de control en el ciclo de vida de los datos personales: Este riesgo podría presentarse cuando el Cliente no cuenta con un control adecuado sobre los datos y procesos sujetos a los servicios de cómputo en la nube
    - Falta de entendimiento o de claridad sobre el tratamiento de los datos personales. Este riesgo podría presentarse debido a la falta de entendimiento del Cliente respecto del modelo de aprovisionamiento

No obstante, en este punto debe tenerse en cuenta que la LFPDPPP y su Reglamento prevén la posibilidad de que se lleve a cabo el tratamiento de datos personales en un país distinto, siempre que se establezcan cláusulas contractuales que aseguren que el proveedor cumplirá con los requerimientos de las normas mexicanas.

Para la evaluación de estos riesgos, se recomienda solicitar información al Proveedor que permita conocer los términos y alcances de los temas antes señalados, así como tomar como referencia las Recomendaciones en materia de seguridad de datos personales del INAI,4 la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, o bien, algún estándar o esquema de buenas prácticas como son: ISO 31000, ISO 27001, ISO 27002, entre otros.

C.2. Devolución y destrucción de los datos personales al finalizar el servicio

- Se recomienda que el Cliente evite aquellos proveedores que no ofrezcan cláusulas, políticas, mecanismos o sistemas automatizados para que pueda recuperar su información una vez terminado el servicio
- es indispensable que el Cliente opte por Proveedores que establezcan cláusulas, políticas, mecanismos o sistemas para el borrado seguro de la información

C.3. Interoperabilidad y portabilidad

- Se recomienda que el Cliente se entere de las condiciones y prácticas del Proveedor en materia de interoperabilidad y portabilidad de la información bajo su resguardo, ya que de ello depende que se puedan realizar transferencias o remisiones de datos personales a otros proveedores de servicio de cómputo en la nube, a otros responsables o encargados.

C.4. Adhesión o contratación del servicio

- se sugiere tener preferencia por Proveedores que permitan contratos sujetos a negociación, respecto a los contratos de adhesión, ya que es la mejor manera de adecuar las características de la prestación del servicio y los requerimientos del Cliente en materia de protección de datos.

- Es importante que el Cliente procure que los criterios mínimos antes señalados se incluyan en las cláusulas del contrato de servicio.

.

INSTITUTO MEXICANO PARA LA COMPETITIVIDAD A.C.