CRITERIOS MÍNIMOS SUGERIDOS PARA LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

SE
SECRETARÍA DE ECONOMÍA

ESTADOS UNIDOS MEXICANOS

Contenidos

Considerandos

El cómputo en la nube es un fenómeno global que representa una oportunidad económica y social para México, al tratarse de un modelo que optimiza la prestación de servicios de tecnología, centrado en el uso de Internet, permite hacer más eficientes los procesos y procedimientos de una organización y es un detonante de la competitividad y apoya la especialización. El cómputo en la nube facilita el tratamiento de la información, indispensable para el desarrollo de un mundo globalizado y con grandes beneficios económicos y sociales.

No obstante, dicho tratamiento realizado por parte de un prestador de servicios de cómputo en la nube (inclusive, datos personales) podría implicar un riesgo para la confidencialidad, integridad y disponibilidad de la información, si no se adoptan medidas adecuadas. Es por ello que, para que una sociedad se beneficie de las ventajas del cómputo en la nube, surge la necesidad de establecer un marco regulatorio y de buenas prácticas que fomenten servicios seguros y que brinden confianza tanto a los usuarios de dichos servicios, como al titular de los datos personales.

En ese sentido, el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento) estableció requisitos mínimos a observar por parte de los responsables del tratamiento de datos personales, para la adhesión a cláusulas generales de contratación de servicios, aplicaciones e infraestructura del denominado cómputo en la nube. Al respecto, dicho artículo señala que los responsables del tratamiento de los datos personales sólo podrán utilizar servicios en los que el proveedor 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 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;

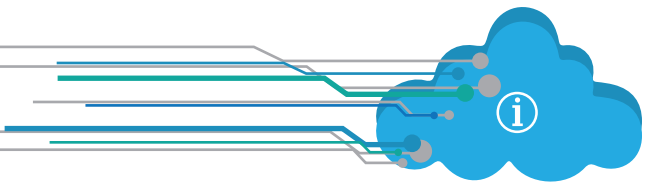
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y

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.

Asimismo, el artículo en mención, establece que el responsable no podrá adherirse a servicios de cómputo en la nube que no garanticen la debida protección de los datos personales.

De manera adicional, resulta importante que, en la contratación de servicios de cómputo en la nube, el responsable del tratamiento de datos personales tome en cuenta lo previsto en los artículos 50, 51, 54 y 55 del Reglamento, para establecer su relación con el proveedor del servicio, en su calidad de encargado del tratamiento.

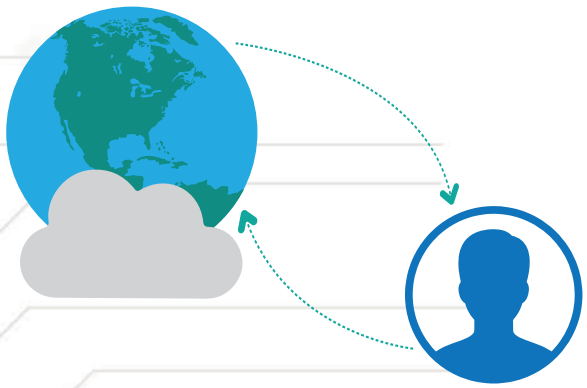
Siendo así, con el objeto de aportar mayores elementos y orientar sobre el debido tratamiento de datos personales en el denominado cómputo en la nube, el artículo 52 del Reglamento estableció la atribución de las dependencias reguladoras de la materia, en coadyuvancia con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), de emitir criterios sobre el particular.



En ese orden de ideas, la Secretaría de Economía, en calidad de autoridad reguladora, facultada para difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto, y el INAI, en su calidad de autoridad garante del derecho de protección de datos personales, emiten los presentes Criterios mínimos que buscan orientar a los responsables del tratamiento de datos personales en la selección de proveedores y servicios de cómputo en la nube, para garantizar una debida protección de los datos personales.

Si bien estos Criterios pretenden un nivel elevado de protección de los datos personales, se emiten con fines de orientación, por lo que no son vinculantes, ni su observancia es obligatoria, a fin de evitar sobrecargas regulatorias que pudieran afectar la competitividad e innovación de las empresas y organizaciones del país.

Así, en virtud de que el contenido de este documento tiene fines de orientación, y con independencia de la adopción de las prácticas aquí señaladas, los responsables están obligados a dar cumplimiento a la normatividad que regula el derecho de protección de datos personales en México.



Por último, resulta relevante reconocer que los servicios de cómputo en la nube tienen una naturaleza transnacional, por lo cual, cuando el responsable del tratamiento de datos personales elija contratar servicios de cómputo en la nube, será responsabilidad de éste seleccionar aquéllos que operen bajo normas equivalentes a las mexicanas, o en su caso cumplan con estándares internacionales que le permitan proteger los datos personales en su posesión.

Sección I. Generalidades

1. Objetivo y alcances

Los presentes criterios tienen por objeto establecer consideraciones mínimas que orienten a los responsables del tratamiento de datos personales en la selección y contratación de proveedores, para los servicios de infraestructura, plataforma y software del denominado cómputo en la nube, que ofrezcan garantías de un debido tratamiento de datos personales, a fin de cumplir con las obligaciones que establece la normatividad en la materia y evitar una vulneración en la protección de los datos personales en su posesión.

2. Fundamento jurídico

Los presentes Criterios se emiten con fundamento en lo dispuesto por el último párrafo del artículo 52 del Reglamento, que señala lo siguiente:

Tratamiento de datos personales en el denominado cómputo en la nube
Artículo 52.

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.

Lo anterior, considerando que la Secretaría de Economía, en su calidad de autoridad reguladora, tiene la facultad de difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano.

Por su parte, de conformidad con el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos y 38 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el INAI es la autoridad garante del derecho de protección de datos personales.

Para las definiciones de los términos utilizados en los presentes Criterios, se sugiere consultar los artículos 3° de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2° y 52 de su Reglamento.

3. Servicios de cómputo en la nube

Derivado del artículo 52 del Reglamento, se considerará al cómputo en la nube, como un modelo de abastecimiento y entrega externa de servicios de acceso a recursos informáticos y su tecnología (por ejemplo, redes, servidores, almacenamiento, aplicaciones), que cumpla con las siguientes características:

1. **Medidos y bajo demanda:** los que se ofrecen según las necesidades de consumo del Cliente.

2. De **distribución flexible**: los que permiten modificaciones de sus características, aun estando en marcha el servicio.

3. **Compartidos:** los que se utilizan de manera dinámica entre distintos consumidores, a través de mecanismos como la virtualización, que dan la apariencia de que los recursos proveídos son únicos para cada Cliente.

4. Con **acceso a través de múltiples plataformas** de hardware y/o software.

Las características mencionadas anteriormente pueden variar dependiendo de la configuración del servicio de cómputo en la nube, dicha composición considera los siguientes Criterios:

1. Si la infraestructura se encuentra **dentro o fuera del perímetro físico** del Cliente.

2. Si el servicio utiliza tecnología **propietaria o abierta**.

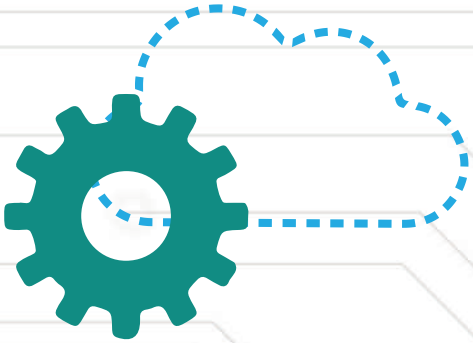
3. Si el servicio opera **con las políticas aplicadas a la infraestructura del Cliente, o sin ellas.**

4. Si el servicio es proporcionado **por un tercero o por el propio personal del Cliente.**

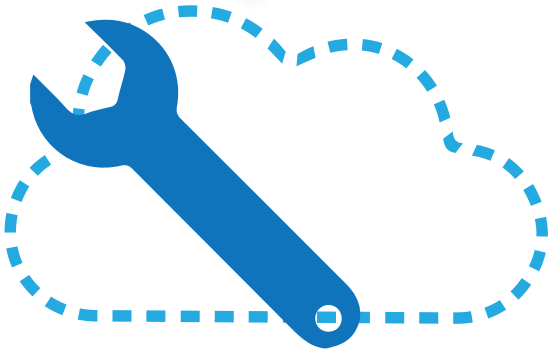
En este sentido, los presentes Criterios se enfocan a todo servicio de cómputo en la nube proporcionado por un proveedor externo, quien se identifica bajo la figura del encargado, sin importar la ubicación geográfica de la infraestructura, el tipo de tecnología utilizada, o si actúa dentro de las premisas de operación del Cliente.

Asimismo, de manera enunciativa más no limitativa, se contemplan tres modelos principales de aprovisionamiento de servicios de cómputo en la nube:

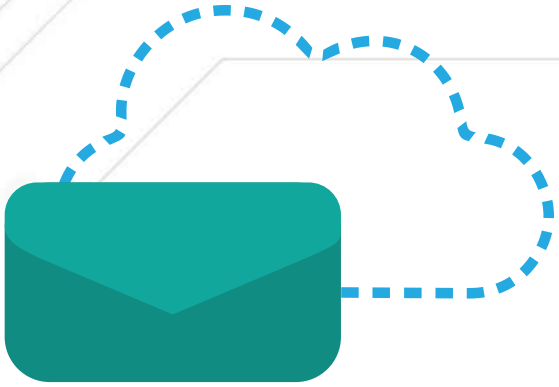
a. **Infraestructura como Servicio (*Infrastructure as a Service o IaaS*):** el Proveedor ofrece acceso directo a almacenamiento, unidades de procesamiento, redes y otros recursos computacionales, para que el Cliente utilice a modo el software y/o hardware que requiera. **El Cliente administra tanto la infraestructura como el software.** Por ejemplo: El Cliente puede utilizar, a través de Internet, servicios empresariales tales como: servidores, máquinas virtuales, administración de redes.

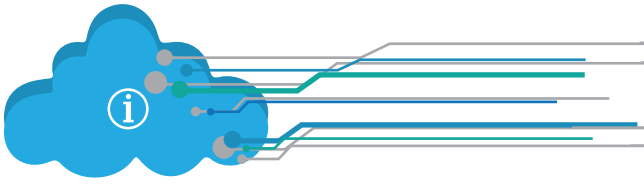


b. **Plataforma como Servicio (*Platform as a Service o PaaS*):** el Proveedor facilita herramientas a sus Clientes para que desarrollen sus propias aplicaciones en la plataforma ofrecida. **El Cliente administra el software, pero no la infraestructura.** Por ejemplo: El Cliente puede acceder a través de Internet, a plataformas de desarrollo de aplicaciones en línea, para distintos lenguajes de programación, colaborativas y de bases de datos.

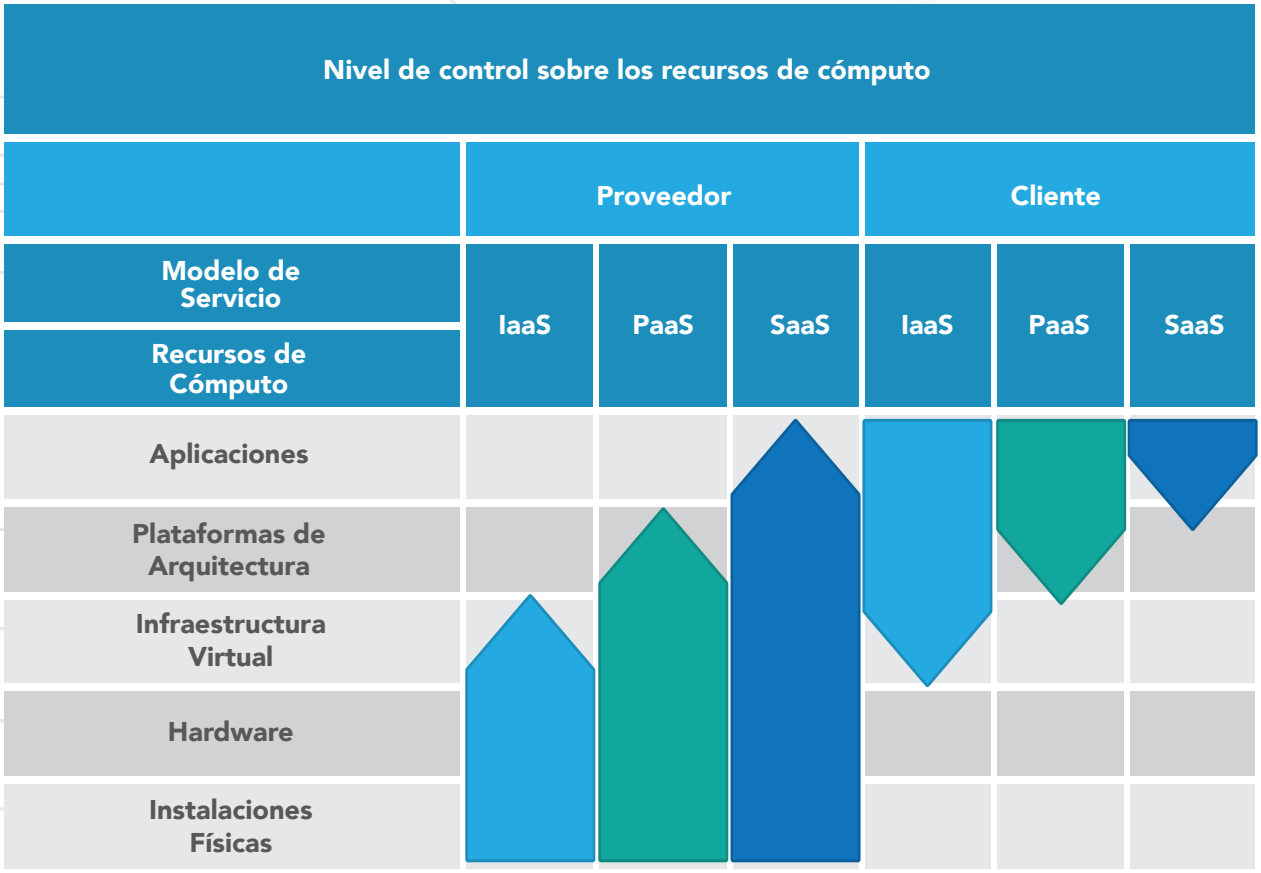


c. **Software como Servicio (*Software as a Service o SaaS*):** el Proveedor suministra programas o aplicaciones que corren completamente en su infraestructura para uso de sus Clientes. **El Cliente no tiene control de la infraestructura y sólo tiene control sobre ciertas características del software.** Por ejemplo: El Cliente puede gestionar correo electrónico, almacenamiento de contenido o mensajería instantánea, a través de software o aplicaciones ofrecidas por el Proveedor.





El **nivel de control que tienen el Proveedor y el Cliente sobre los recursos de cómputo y la información** depende de los modelos de servicio de aprovisionamiento, como se muestra en la figura siguiente:



Como puede observarse en el gráfico, **el nivel de control sobre la administración de los recursos de cómputo** por parte del proveedor aumenta, conforme el modelo de aprovisionamiento pasa de *IaaS a SaaS*, lo que a su vez implica que el Proveedor aumente su intervención en el tratamiento de la información.

En esta línea de ideas, no se debe perder de vista, que al permitir que un Proveedor intervenga en cualquier fase del tratamiento de datos personales, **existe un riesgo proporcional al nivel de control sobre los recursos de cómputo.**

Por lo que respecta a las características de los servicios de cómputo en la nube, así como los modelos de aprovisionamiento expuestos anteriormente, tienen por objeto apoyar a los responsables y encargados en el entendimiento del nivel de control que pueden tener sobre los datos personales a través de estos servicios.

Es importante aclarar que los conceptos expuestos no son absolutos, debido a la condición evolutiva de las tecnologías de la información y las comunicaciones y el dinamismo que las caracteriza.

4. Responsables y encargados

Cuando la prestación de servicios de cómputo en la nube implica la contratación de dichos servicios por parte de un Cliente a un Proveedor, este último lleva a cabo el tratamiento de datos personales a nombre y por cuenta del primero, en el marco del servicio de cómputo en la nube que brinde.

El artículo 3° de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define las figuras de **responsable** y **encargado** de la siguiente forma:

> **IX. Encargado:** La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.
>
> **XIV. Responsable:** Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Por su parte, el artículo 49 del Reglamento precisa la naturaleza y alcance de la figura del encargado, de la siguiente forma:

> **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.

En congruencia con lo anterior, se entenderá que el **Proveedor** de un servicio de cómputo en la nube tiene la figura de "**encargado**", en términos de lo dispuesto por la LFPDPPP y su Reglamento, por lo que en adelante será mencionado de manera indistinta como encargado o Proveedor.

En consecuencia, el **Cliente** es el **"responsable"** del tratamiento de datos personales, al ser quien decide sobre dicho tratamiento, por lo que en adelante será mencionado de manera indistinta como responsable o Cliente.

Asimismo, es relevante señalar que la comunicación de datos personales entre el responsable y el encargado es definida como remisión, por el Reglamento.

Lo anterior implica que la protección de los datos personales que se coloquen en la nube sigue siendo responsabilidad de quien contrata un servicio de cómputo en la nube, quien ha sido definido como el Cliente en su carácter de responsable, con independencia de que el Proveedor de dicho servicio tenga también obligaciones con relación al manejo de la información personal que le sea comunicada, en su carácter de encargado.

Es por ello, que resulta importante la contratación de servicios de cómputo en la nube seguros.

Con independencia de lo anterior, es importante tener en cuenta que cuando el Proveedor destine o utilice los datos personales con una finalidad distinta a la autorizada por el Cliente, o bien efectúe una transferencia incumpliendo con las instrucciones del Cliente, el encargado del tratamiento de datos personales puede tomar la figura de responsable conforme lo señala el artículo 53 del Reglamento, con las obligaciones que ello implica.

5. Cumplimiento de principios y deberes

El tratamiento de datos personales en el denominado cómputo en la nube deberá observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, así como los deberes de confidencialidad y seguridad, establecidos en la LFPDPPP y su Reglamento, y deberá prever condiciones para que los titulares de los datos personales puedan ejercer sus derechos ARCO.

El cumplimiento de estos principios y deberes está a cargo del Cliente, quien es el responsable del tratamiento de los datos personales y quien deberá responder frente al titular de los mismos. Para conocer más de estos principios y deberes en materia de protección de datos personales, se recomienda ver el **Anexo 1.**

Adicionalmente, en la *Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube* disponible en la página de PROSOFT de la Secretaría de Economía, se puede consultar el *Checklist para la revisión del cumplimiento*[1], el cual permite a las empresas evaluar por sí mismas su nivel de conocimiento y aplicación de la normatividad en materia de Protección de Datos Personales en el uso de Cómputo en la Nube. Un extracto de este *checklist* también se puede consultar en el **Anexo 2** de los presentes criterios.

[1] Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (Cloud Computing), 4. Checklist para la revisión del cumplimiento, Pp. 375-387. Estudio apoyado por el Programa para el Desarrollo de la Industria de Software (PROSOFT) y el Banco Mundial. Consultable en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_33.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

Previo a la contratación o adhesión[2] a un servicio de cómputo en la nube, resulta conveniente que el Cliente:

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.

[2] Para efectos de un servicio de cómputo en la nube, de acuerdo con la Procuraduría Federal de Consumidor y la Ley Federal de Protección al Consumidor, un contrato de adhesión es el documento elaborado unilateralmente por el Proveedor, para establecer en formatos uniformes los términos y condiciones aplicables a la adquisición de un producto o la prestación de un servicio, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato. Más información sobre contratos de adhesión puede ser consultada en: https://rcal.profeco.gob.mx/rcal.jsp

Bajo ese contexto, se recomienda considerar los siguientes **Criterios**:

A.1. Reputación del Proveedor

- El 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, y la opinión pública que existe entorno a sus servicios.

- Si el Proveedor o sus subcontrataciones **han sufrido incidentes importantes**, y si después de un incidente, el Proveedor es diligente con sus clientes, al tomar acciones que mitiguen su impacto.

- Si se han **denunciado de manera pública medidas de seguridad deficientes** por parte del Proveedor o sus subcontrataciones, y si dichas medidas se han mejorado.

- Si el Proveedor o sus subcontrataciones han sido s**ujetos de denuncias o investigaciones por autoridades de protección de datos personales** alrededor del mundo, así como la respuesta que dio el Proveedor a las autoridades.

- Si el Proveedor es claro y transparente respecto a su modelo de negocio, sus prácticas en el tratamiento de datos personales y su política de privacidad, esta última además debe ser diferenciada para cada uno de sus productos y servicios en la nube.

A.2. Identidad del Proveedor

Es importante que el Cliente cuente con información de la **identidad y medios para contactar al Proveedor**, entre ella la siguiente:

- Nombre o razón social del Proveedor.

- Medios de contacto para la atención al cliente y solicitudes sobre el servicio, tales como teléfonos, correos electrónicos o sistemas automatizados.

- En su caso, medios de contacto para zonas geográficas específicas, por ejemplo, de oficinas regionales.

A.3. Jurisdicción aplicable y ubicación geográfica de los datos personales

Es conveniente que, para poder tomar una decisión informada para contratar servicios de cómputo en la nube, el Cliente conozca la siguiente información, pues estos factores tienen una injerencia directa en las obligaciones que tendrá el Proveedor con relación al tratamiento de los datos personales:

- **La jurisdicción o normatividad que rige al Proveedor y al contrato**, sea por adhesión voluntaria, por domicilio, acuerdo contractual, o alguna otra.

- La **ubicación geográfica de los centros de tratamiento de información** y en su caso la oficina de atención regional que le corresponde. Al respecto, se recomienda tener 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, o bien optar por proveedores que, con independencia de la jurisdicción, habiliten el cumplimiento de los requerimientos de la normativa mexicana a sus clientes.

- Conocer el **ámbito geográfico en el cual se respalda la prestación del servicio**, considerando la ocurrencia de fenómenos naturales o la ubicación en zonas de riesgo, por ejemplo, zonas sísmicas.

- Si el Proveedor tiene operaciones en México, se recomienda identificar si cumple con la normativa mexicana en materia de protección de datos, y mucho mejor si cuenta con un esquema de autorregulación, como una certificación en materia de protección de datos personales.

Se reitera que con independencia de las responsabilidades contractuales que adquiera el Proveedor, el Cliente mantendrá su carácter de responsable del tratamiento de datos personales. En ese sentido, se recomienda optar por Proveedores que reflejen, a través de cláusulas para la contratación o adhesión a sus servicios, prácticas alineadas a la normatividad mexicana, en materia de protección de datos personales.

Adicionalmente, se sugiere consultar las normas *ISO/IEC 27018:2014 e ISO/IEC 19086-1:2016*, como referencia para la contratación previa de servicios de computo en la nube.

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, ni de la información que se genere directamente relacionada con el servicio.

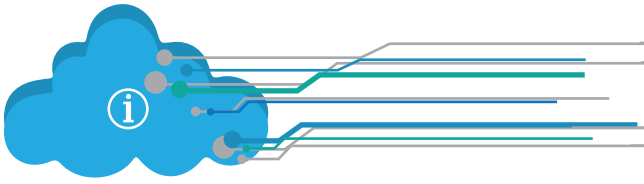
II. Se recomienda al Cliente que elija Proveedores que cuenten con cláusulas, políticas, mecanismos o sistemas automatizados:

a. Para que el Proveedor y sus subcontrataciones utilicen la información del Cliente **únicamente para las finalidades establecidas en los términos del servicio**.

b. Para 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.

c. Para mantener al Cliente **informado sobre quiénes acceden a su información y para qué propósito**, evitando los accesos no autorizados.

d. Para que el Cliente pueda **acceder, modificar o borrar información** en cualquier momento durante la vigencia del servicio.



e. Para eliminar o destruir la información del Cliente **con métodos de borrado seguro**, dentro de un periodo definido, durante y después de la prestación del servicio.

f. Para notificar al Cliente de cualquier **cambio o actualización en la prestación del servicio**, en particular en lo que se refiere a la protección de los datos personales.

g. 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:

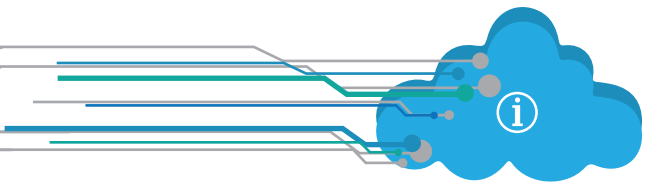
a. Notificar al Cliente cualquier **falla o interrupción del servicio**.

b. Notificar al Cliente el **acceso o solicitud de acceso de terceros a la información**, por ejemplo, las que realicen las autoridades competentes, nacionales o extranjeras. Lo anterior, a menos que exista alguna causal de clasificación, por la cual la notificación al cliente no sea posible, tal como una investigación policial en curso.

c. **Apoyar** al Cliente para **la identificación y la mitigación o remediación de una vulneración a la seguridad de los datos personales**, relacionada con el servicio. En su caso, el Proveedor debe proporcionar acceso a herramientas, bitácoras, registros, o elementos de prueba para apoyar al Cliente con la investigación del incidente, o bien para procedimientos ante las autoridades en materia de protección de datos.

d. **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.**

e. Ofrecer al Cliente **instrumentar acciones proactivas** para proteger los datos personales.



En ese sentido, se sugiere considerar los siguientes **Criterios**:

B.1. Transparencia en el servicio

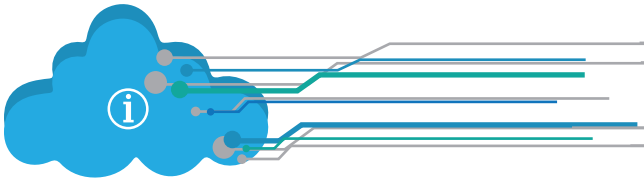
Con la finalidad de garantizar el cumplimiento de las obligaciones en materia de protección de datos personales, y de conformidad con lo establecido en los artículos 52, inciso b, fracción I, 54 y 55 del Reglamento, el Cliente debe conocer la existencia de las subcontrataciones que, en su caso, realice el Proveedor, con excepción de aquellos detalles o información que se encuentre protegida por algún secreto, cuya publicidad se encuentre protegida conforme la normatividad aplicable.

En ese sentido, se sugiere al responsable optar por Proveedores que garanticen transparencia en la cadena de subcontrataciones, así como los siguientes elementos:

- El control sobre las personas o empresas que subcontraten;
- Los mecanismos implementados por los terceros subcontratados para garantizar la confidencialidad de los datos personales;
- La posibilidad de atender solicitudes de ejercicio de derechos ARCO, en aquellos datos que estén siendo tratados por encargados subcontratados, y
- La supresión de los datos personales a través de métodos de borrado seguro u otro mecanismo, que evite la recuperación de los datos personales por un tercero no autorizado.

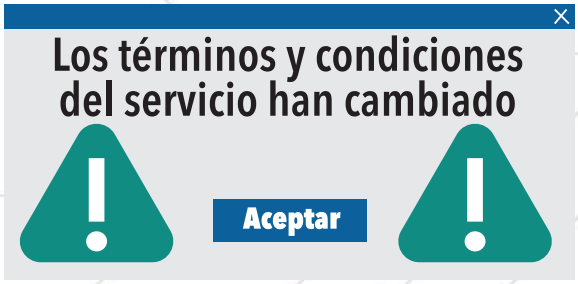
Con independencia de lo anterior, se recomienda que el Cliente o responsable elija proveedores que **tomen responsabilidad completa** por los servicios subcontratados, sin que lo anterior implique que el Cliente pueda perder su calidad de responsable de los datos personales.

Asimismo, se recomienda seleccionar proveedores que tengan políticas y rindan 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

Resulta indispensable que el responsable se informe y esté al tanto de cualquier cambio en el servicio de cómputo en la nube, que pudiera tener alguna implicación relevante para la protección de los datos personales.



En ese sentido, de conformidad con lo dispuesto en el inciso a, fracción II del artículo 52 del Reglamento, 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:

a. Para la protección de la **confidencialidad de la información almacenada** en los sistemas del Proveedor y de sus subcontrataciones. Por ejemplo, el uso de cifrado en sus sistemas de almacenamiento y de mecanismos de autenticación para el acceso del Cliente a los servicios.

b. Para la protección de la **confidencialidad de la información en tránsito**, entre los diferentes sistemas del Proveedor o de sus subcontrataciones, y entre los sistemas del Cliente y el Proveedor o de sus subcontrataciones. Por ejemplo, el cifrado del canal de comunicaciones.

c. Para la protección de la **disponibilidad e integridad de la información** del Cliente. Por ejemplo, a través de copias de seguridad o almacenamiento redundante.

d. Para 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.

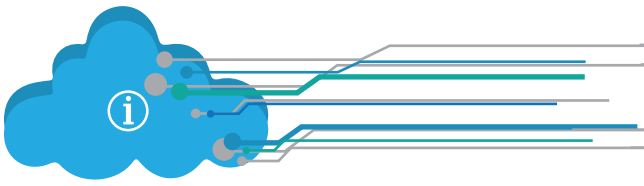
e. Para que el Cliente tenga **control sobre el acceso y gestión de los datos, procesos o servicios.** Por ejemplo, con contraseñas, gestión de identidades o certificados digitales.

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

a. Mostrar 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.

b. Mostrar evidencia de que sus servicios consideran **la protección de datos personales desde el diseño o rediseño**, como una característica intrínseca en sus operaciones, a fin de llevar la seguridad de la información más allá de la normativa.

c. 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.



Por lo anterior, se sugiere considerar los siguientes Criterios:

C.1. Evaluación de riesgos para los datos personales

De conformidad con lo establecido en los artículos 60 y 61, fracción III del Reglamento, 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[3], a fin de identificar los controles de seguridad que resultan necesarios para la protección de los datos personales.

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, como pudiera ser:
    - **Falta de confidencialidad**: los datos personales tratados en la nube no son de uso exclusivo del Cliente y pueden ser accedidos por el Proveedor para finalidades adicionales a las del servicio contratado, o bien por terceros.
    - **Falta de transparencia en las subcontrataciones que dificulta el cumplimiento**: el Proveedor de cómputo en la nube puede valerse de subcontrataciones que se añaden o eliminan de manera dinámica para la prestación de sus servicios, y que podrían no resultar seguras. Las subcontrataciones deben estar debidamente controladas por el Proveedor y ser claras para el Cliente, a fin de que éste no pierda el control de su información.

[3] Para realizar el análisis de riesgos se recomienda consultar la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales, disponible en el portal de Internet del INAI en la sección "Protección de Datos Personales", subsección "Documentos de interés".

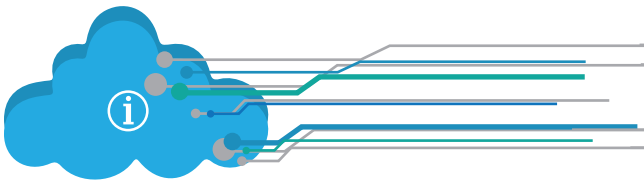
- **Falta de sistemas automatizados o mecanismos de ayuda**: el servicio de cómputo en la nube carece de las herramientas necesarias para que el Cliente cumpla con sus obligaciones normativas, como podría ser la atención de solicitudes de ejercicio de los derechos ARCO.

- **Uso inadecuado de recursos compartidos y falta de aislamiento**: puede ser que existan conflictos entre los distintos clientes de un Proveedor, ya que el servicio de cómputo en la nube puede disponer de sistemas comunes. También el Proveedor podría ejercer control sobre los datos almacenados por distintos clientes y realizar tratamientos adicionales, por ejemplo, combinar o cruzar la información.

- **Falta de portabilidad**: en caso de que el Proveedor almacene la información en un formato cerrado, de manera que, en un futuro, se dificulte al Cliente trasladar su información a otros servicios de cómputo en la nube, o bien, recuperarla una vez que se concluya la relación con el Proveedor.

- **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, en particular cuando ocurre lo siguiente:

  - **Tratamiento adicional, no autorizado de datos personales**: el servicio de cómputo en la nube puede incluir tratamientos de los datos personales que no son conocidos o deseados por el Cliente, lo que además podría dar lugar a comunicaciones ilícitas de dichos datos.



- **Tratamiento de datos personales por múltiples actores**: los servicios de cómputo en la nube están compuestos por una cadena compleja de proveedores y subcontrataciones y, por tanto, el Cliente puede exponer los datos personales sin saberlo o estar consciente de ello.

- **Tratamiento de datos personales para modelos de negocio basados en publicidad sin autorización**: el Cliente podría estar exponiendo la información si el Proveedor utiliza y explota las bases de datos para fines publicitarios propios, sin que exista autorización para ello o conocimiento por parte del Cliente.

- **Tratamiento de datos personales en distintas jurisdicciones o zonas geográficas que no cumplen con un nivel adecuado de protección**: el Cliente podría estar exponiendo la información a un régimen jurídico que no satisface sus requerimientos en materia de protección de datos personales. Esto podría ocasionar a los responsables quedar sin la protección de la legislación mexicana ante un Proveedor extranjero.

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, y en un formato tal que el Cliente tenga la capacidad de utilizar esa información, o bien migrarla a un servicio diferente.

Además de la recuperación de la información, para cumplir con el inciso d de la fracción II del artículo 52 del Reglamento, es **indispensable que el Cliente opte por Proveedores que establezcan cláusulas, políticas, mecanismos o sistemas para el borrado seguro de la información**, una vez finalizado el servicio. Para conocer los métodos de borrado seguro, se sugiere consultar la Guía para Borrado Seguro de los Datos Personales,[5] emitida por el INAI y publicada en su portal de Internet.

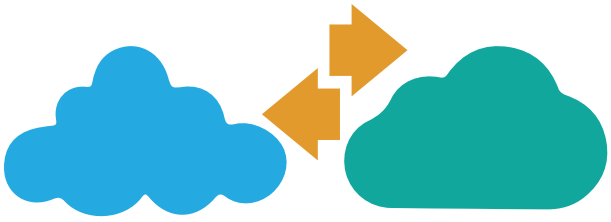
[4] Para consulta en: http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

[5] Consultable en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

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.

Para ello, se recomienda que el Cliente conozca si el Proveedor le permite obtener copias, en cualquier momento, de la información almacenada y tratada en la nube; si le proporciona orientación y ayuda para descargar la información, así como si al finalizar el contrato, le permite exportar la información en un formato tal que pueda utilizarse en otros servicios de cómputo en la nube, o directamente por el Cliente.



C.4. Adhesión o contratación del servicio

De manera general, 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.

En todo caso, el responsable deberá tomar en cuenta las obligaciones que existen respecto de la relación entre el responsable y encargado, según lo establecido en los artículos 50, 51, 53, 54 y 55 del Reglamento.

Sección III. Acciones a evitar en la contratación o adhesión a servicios de cómputo en la nube

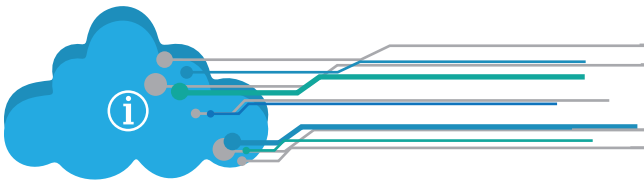
Además de los criterios mínimos establecidos en este documento, se sugiere evitar las siguientes acciones:

I. **Considerar que los servicios de cómputo en la nube son una cuestión "de informáticos"**. Los servicios de cómputo en la nube requieren de un análisis integral de diversos elementos aplicables a la organización, como cumplimientos legales, valoraciones económicas (costo-beneficio), buenas prácticas, gestión de calidad, entre otros, además del factor tecnológico.

II. **Asumir que los servicios de cómputo en la nube populares o en tendencia son la mejor opción**. Dependiendo del Cliente, un servicio de cómputo en la nube podría no ser una opción, o sólo ser funcional para ciertos tipos de datos, procesos o servicios.

III. **Asumir que los servicios de cómputo en la nube son convenientes por ser gratuitos.** Es importante que los clientes que opten por adherirse a servicios de cómputo en la nube de carácter general o gratuito, evalúen las condiciones de servicio y políticas de privacidad que ofrecen, si es que las tienen, para evaluar los riesgos mencionados en los presentes Criterios mínimos, pues en la mayoría de los casos, el uso y aprovechamiento de la información personal es en lo que se basa el modelo de negocio que permite la gratuidad del servicio.

IV. **Asumir que el tratamiento de información y operaciones del Cliente deben estar por completo en la nube.** El Cliente debe ponderar cuáles son las operaciones o procesos que conviene optimizar a través del servicio de cómputo en la nube, y cuáles no.



Anexo 1. Los principios y deberes de protección de datos personales en los servicios de cómputo en la nube

1. Principios de licitud y lealtad[6]

De acuerdo con el principio de licitud, los datos personales deberán recabarse y tratarse de manera lícita, conforme a las disposiciones establecidas en la LFPDPPP y demás normatividad aplicable. En ese sentido, el responsable sólo podrá hacer con los datos personales aquello que esté legalmente permitido.

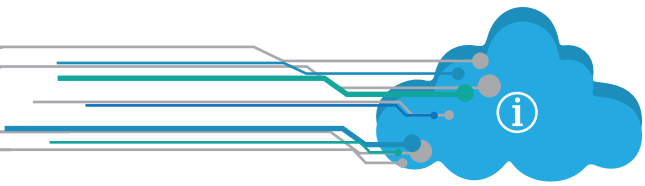
Por su parte, el principio de lealtad establece que en todo tratamiento de datos personales se presume que existe la expectativa razonable de privacidad de los titulares, es decir, la confianza de éstos de que sus datos personales serán tratados conforme a lo acordado con el responsable y en términos de la ley.

Para el tema de cómputo en la nube, resulta relevante lo siguiente:

1. En general, está permitido y es lícito el tratamiento de datos personales en el denominado cómputo en la nube, salvo que para ciertas actividades o sectores en lo particular exista alguna disposición que prohíba colocar cierta información en la nube. En ese sentido, es importante que el responsable conozca la normatividad que regula la actividad en la cual se están tratado los datos personales, por ejemplo, salud, bancaria, educación, telecomunicaciones, entre otras.

2. Es importante que el responsable contrate servicios seguros de cómputo en la nube, que garanticen el respeto a los derechos de privacidad y protección de datos personales, a fin de no vulnerar la expectativa razonable de privacidad de los titulares.

[6] Ver artículos 7 de la LFPDPPP y 10 y 44 de su Reglamento.



2. Principio de consentimiento[7]

Como regla general, el responsable deberá contar con el consentimiento del titular para el tratamiento de sus datos personales, salvo las excepciones previstas en la LFPDPPP.

En el caso que nos ocupa, en virtud de que el uso del servicio de cómputo en la nube no es una finalidad del tratamiento por sí misma, sino que es parte del procedimiento que se utiliza para el tratamiento de datos personales en el marco de una finalidad en lo específico, y debido a que la comunicación de datos personales para este servicio se trata, en lo general, de una remisión a un encargado (Proveedor); el responsable **no requiere el consentimiento del titular de los datos personales para tratar su información en la nube**.

3. Principio de información[8]

Por virtud de este principio, los responsables se encuentran obligados a informar a los titulares de los datos personales, las características principales del tratamiento al que será sometida su información personal, con toda la información que exige la norma, a través del aviso de privacidad.

En el caso del cómputo en la nube, dado que se actualizan los siguientes dos supuestos:

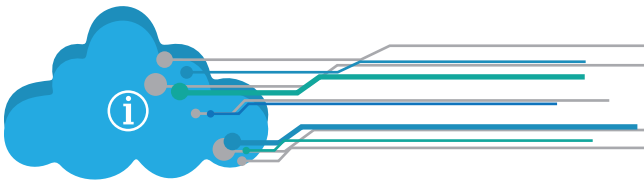
1. No es una finalidad específica de tratamiento de datos personales, como se señaló anteriormente, y

2. No se trata de una transferencia de datos personales, sino de una remisión, cuando el Proveedor tiene el carácter de encargado.

No es necesario informar en el aviso de privacidad que los datos personales serán colocados o tratados en la nube.

[7] Ver artículos 8 al 10 de la LFPDPPP y 11 al 22 de su Reglamento.

[8] Ver artículos 15 al 18 de la LFPDPPP y 23 al 35 de su Reglamento, así como los Lineamientos del Aviso de Privacidad.



4. Principio de calidad[9]

El principio de calidad establece que, conforme a la finalidad o finalidades para las que se vayan a tratar los datos personales, éstos deben ser pertinentes, correctos y actualizados. Asimismo, este principio señala que cuando los datos personales hayan dejado de ser necesarios para las finalidades para la cuales se obtuvieron, el responsable debe eliminarlos, tomando en cuenta las disposiciones legales aplicables para los plazos de conservación, y con independencia de que el titular ejerza o no su derecho de cancelación.

En suma, el principio de calidad implica dos obligaciones para el responsable:

1. Tomar las medidas pertinentes para que los datos personales tratados sean pertinentes, correctos y actualizados, y

2. Suprimir o eliminar los datos personales de las bases de datos, cuando éstos ya no sean necesarios para la finalidad para la cual se obtuvieron, y cuando hayan concluido los plazos de conservación correspondientes.

Con relación a la primera obligación, en el caso del cómputo en la nube, así como en cualquier otro caso, por ejemplo, una base de datos, los datos que se coloquen o traten en la nube deben ser pertinentes, correctos y actualizados. **En ese sentido, el responsable deberá optar por servicios de cómputo en la nube que permitan actualizar o modificar la información cuando ello sea necesario, y que garanticen la integridad de los datos personales.**

En cuanto a la segunda obligación, toma especial relevancia que el contrato que el responsable celebre con el Proveedor del servicio de cómputo en la nube, o al cual se adhiera, establezca con claridad las **obligaciones del Proveedor respecto de la eliminación de los datos personales cuando así lo solicite el Cliente o cuando concluya la prestación del servicio y no haya ninguna otra obligación legal de conservarlos.**

[9] Ver artículos 11 de la LFPDPPP y 36 al 39 de su Reglamento.

5. Principio de finalidad[10]

De acuerdo con este principio, el responsable sólo puede tratar los datos personales para cumplir con la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Al respecto, se reitera que el tratamiento de datos personales en el cómputo en la nube no es una finalidad en sí misma, sino parte del procedimiento que se utiliza para el tratamiento de datos personales en el marco de una finalidad en lo específico.

Con independencia de lo anterior, el cómputo en la nube debe ser utilizado **en el marco de las finalidades que fueron informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste, y se debe evitar cualquier desvío de estas finalidades, tant o por parte del responsable, como del Proveedor del servicio.**

[10] Ver artículos 12 de la LFPDPPP y 40 al 43 de su Reglamento.

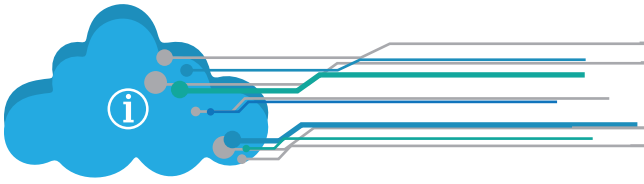
6. Principio de proporcionalidad[11]

Este principio establece la obligación del responsable de tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes para las finalidades para las cuales se obtuvieron.

En ese sentido, el responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron.

En el caso del cómputo en la nube, dado que éste no es un fin en sí mismo, sino parte del procedimiento para el tratamiento, **no aplica de manera directa el principio de proporcionalidad.** En cambio, este principio se debe observar desde el momento en que el responsable recaba los datos personales para la finalidad en cuestión, con independencia de que los mismos los vaya a tratar o no en la nube.

[11] Ver artículos 13 de la LFPDPPP y 45 y 46 de su Reglamento.



7. Principio de responsabilidad[12]

Este principio toma especial relevancia para la adopción de los presentes Criterios mínimos, pues señala que el responsable velará por el cumplimiento de los principios de protección de datos personales, para lo cual adoptará las medidas que resulten necesarias, aún y cuando los datos personales fueren tratados por un tercero a solicitud del responsable.

De conformidad con el artículo 48 del Reglamento, existen diversas acciones o medidas que puede tomar el responsable para garantizar el debido tratamiento de los datos personales, y privilegiar la expectativa razonable de privacidad de los titulares de los datos personales. Estas medidas complementan, en gran medida, las obligaciones previstas en el marco regulatorio, y se consideran buenas prácticas.

Para el caso que nos ocupa, destaca la medida señalada en la fracción V del artículo 48 del Reglamento, que establece que entre las acciones que podrán tomar los responsables para garantizar el debido tratamiento de datos personales, se encuentra la de "instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos".

En atención a lo anterior, es necesario que el responsable **contrate servicios de cómputo en la nube que garanticen el debido tratamiento de los datos personales, según lo establece la normatividad en la materia en México, con independencia de que el Proveedor del servicio se encuentre o no en territorio nacional.** Al respecto, es importante recordar que la obligación de la protección de los datos personales es del responsable del tratamiento, con independencia de que los datos se encuentren en su servidor, equipo de cómputo, archivos o en la nube.

[12] Ver artículo 14 de la LFPDPPP y 47 y 48 de su Reglamento.

8. Deber de confidencialidad[13]

Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Es por ello que el responsable tiene que adoptar medidas para evitar que quienes tengan acceso a los datos personales los divulguen de manera indebida o no autorizada.

En ese sentido, el responsable debe adoptar las medidas necesarias para que el **Proveedor del servicio de cómputo en la nube, que tiene acceso y trata los datos personales a su nombre y cuenta, cumpla con el deber de confidencialidad**, aun terminada la relación jurídica entre ambos, en cuyo caso, si no es necesario que el Proveedor conserve los datos personales por alguna cuestión legal, una vez terminada la relación con el Cliente, tendría que eliminarlos bajo métodos seguros de borrado.

Lo anterior implica tomar medidas de carácter contractual, que obliguen al Proveedor a guardar secreto respecto de los datos personales a los que tiene acceso con motivo del servicio que presta. Asimismo, resulta fundamental establecer una condición que prohíba al Proveedor asumir la propiedad de la información que el Cliente deposite o que se genera en la nube.

9. Deber de seguridad[14]

Este deber se refiere a la obligación, tanto del responsable como del encargado, de establecer y mantener medidas de seguridad técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Las medidas adoptadas no podrán ser menores a aquéllas que tengan el responsable y el encargado para el manejo de su información en lo general.

[13] Ver artículo 21 de la LFPDPPP.

[14] Ver artículos 19 de la LFPDPPP y 57 al 66 de su Reglamento.

Así, el responsable deberá contratar servicios de cómputo en la nube que garanticen medidas de seguridad adecuadas para la protección de los datos personales. Por su parte, el deber de seguridad es una obligación para el encargado, cuando a éste le aplique la normatividad mexicana, de conformidad con la fracción III del artículo 50 del Reglamento.

En el apartado *C. Criterios mínimos a considerar por el cliente para asegurar que el proveedor cuente con medidas de seguridad*, de la Sección II del documento principal, se abordó con mayor detalle este deber.

10. Notificación de vulneraciones

El artículo 20 de la LFPDPPP establece que 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 que considere pertinentes para su defensa.

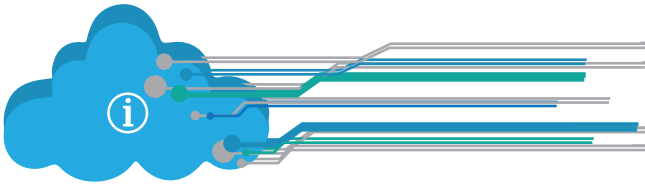
De acuerdo con lo anterior, el responsable del tratamiento está obligado a informar al titular sobre las vulneraciones que ocurran a los datos personales que están en su posesión. En ese sentido, en caso de que ocurriera una vulneración en el servicio de cómputo en la nube, que afecte a los datos personales, el responsable tendría que informar sobre la misma al titular.

Es por ello, que adquiere especial relevancia la contratación o adhesión de servicios que garanticen que el Proveedor hará del conocimiento del Cliente las vulneraciones ocurridas y la información relevante sobre las mismas.

11. Ejercicio de derechos ARCO

De conformidad con los Capítulos III y IV de la LFPDPPP y VII de su Reglamento, los responsable están obligados a atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los titulares, en un plazo máximo de veinte días hábiles, contados desde la fecha en que se recibió la solicitud (para informar sobre la determinación adoptada, es decir si procede o no el ejercicio del derecho solicitado), y de quince días hábiles más para hacer efectivo el derecho, en caso de que éste proceda, contados a partir de que se comunique la respuesta al titular.

En el caso que nos ocupa, resulta relevante que los servicios de cómputo en la nube que se contraten, permitan que el responsable o Cliente atienda en tiempo y forma las solicitudes de estos derechos.



Anexo 2. *Checklist* para la revisión del cumplimiento de la Guía para empresas en materia de Protección de Datos Personales en el uso de Cómputo en la Nube

En este Anexo se incluye un *checklist* general y un *checklist* específico extraídos de la *Guía para empresas en materia de Protección de Datos Personales en el uso de Cómputo en la Nube* apoyado por el Programa para el Desarrollo de la Industria del Software (PROSOFT)[15], para que las empresas puedan revisar, por sí mismas, su estado de cumplimento de la normatividad en materia de Protección de Datos, así como analizar los riesgos que asumen al contratar productos y servicios en la nube.

El primer *checklist* incluye preguntas, en diversas áreas, cuya finalidad es que los clientes o futuros clientes de cómputo en la nube conozcan si están alineados con la normatividad en la materia y, de esta manera, evaluar su situación actual. En concreto, esta lista de comprobación incluye preguntas relativas a:

- Riesgos legales y regulatorios;
- Protección de datos personales;
- Seguridad;
- Propiedad intelectual;
- Acuerdo de nivel de servicio (SLA) y otras cuestiones contractuales, y
- Ciberdelitos.

El segundo *checklist* pretende que las empresas conozcan y evalúen los principales aspectos a considerar, antes y durante la contratación de servicios de cómputo en la nube.

[15] Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (*Cloud Computing*), *4. Checklist para la revisión del cumplimiento,* Pp. 375-387. Estudio apoyado por el Programa para el Desarrollo de la Industria de Software (PROSOFT) y el Banco Mundial. Consultable en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_33.pdf

Ambas listas de comprobación son una herramienta de apoyo, de manera que no sustituyen en modo alguno la realización de una auditoría futura u otra forma de asegurar el cumplimiento, que corresponde al cliente o futuro cliente de servicios de cómputo en la nube en cada caso concreto, atendiendo a las circunstancias específicas de su caso.

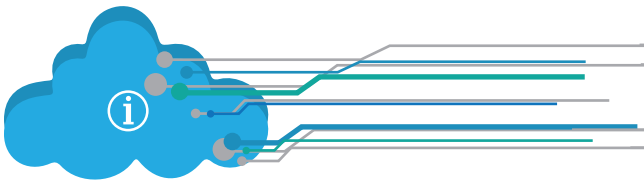
2.1 *Checklist* general sobre cómputo en la nube

RIESGOS LEGALES Y REGULATORIOS		
¿Ha adoptado medidas para identificar riesgos legales y regulatorios previamente a la contratación de servicios de cómputo en la nube?	Sí	No
Cuando contrata servicios de cómputo en la nube, ¿ha adoptado medidas de gestión para minimizar los riesgos legales y regulatorios que pudieran ocurrir?	Sí	No
¿Ha verificado que los servicios de cómputo en la nube y su tecnología cumplan con las NormasOficiales Mexicanas y las Normas Internacionales aplicables en la materia?	Sí	No
En caso de que se produzca algún incumplimiento, ¿tiene previsto un procedimiento para adoptar medidas correctivas que le permitan responder ante dicha situación?	Sí	No
En relación con los servicios que pudiera subcontratar el proveedor de servicios de cómputo en la nube, ¿le ha proporcionado información sobre si existen políticas específicas sobre el uso de subcontratistas?	Sí	No
Con respecto al proveedor de servicios de cómputo en la nube, ¿sabe si se somete esporádicamente a algún procedimiento de evaluación de su desempeño?	Sí	No
¿Tiene suficiente ancho de banda para hacer uso del servicio y se ha informado sobre las características del mismo en cuanto a necesidad de hardware y conexión?	Sí	No
PROTECCIÓN DE DATOS PERSONALES		
Al contratar servicios de cómputo en la nube, ¿ha visto si en el contrato correspondiente se considera al cliente de servicios de cómputo en la nube como responsable del tratamiento de los datos personales?	Sí	No
Al contratar servicios de cómputo en la nube, ¿ha visto si en el contrato se considera al prestador de servicios de cómputo en la nube como encargado del tratamiento de datos personales?	Sí	No
Al firmar el contrato u otro instrumento jurídico con el proveedor de servicios de cómputo en la nube, ¿se asegura de que el acuerdo esté acorde con el aviso de privacidad correspondiente?	Sí	No
¿Ha adoptado las medidas necesarias para identificar riesgos en materia de protección de datos personales y para minimizar dichos riesgos?	Sí	No
¿Los datos personales se recaban y se tratan conforme a las disposiciones legales establecidas?	Sí	No
¿Los datos personales que se tratan cumplen con los principios previstos en la normatividad?	Sí	No
¿Ha establecido políticas de protección de datos personales afines a los principios y deberes que establecen las normas en la materia?	Sí	No
¿Cuenta con políticas de protección de datos y privacidad que se refieran a todos los tratamientos de datos personales que lleva a cabo, incluido el uso de la nube?	Sí	No
¿Cuenta con alguna certificación en materia de protección de datos personales y si es así, dicha certificación se refiere también a tratamientos de datos por encargados y en la nube?	Sí	No
Antes de contratar los servicios de cómputo en la nube, ¿se ha asegurado de que el proveedor de servicios de cómputo en la nube se abstiene de incluir condiciones relativas a la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio?	Sí	No
¿En el aviso de privacidad se ha informado a los titulares de los datos personales que se tratan sobre las características principales del tratamiento al que será sometida dicha información?	Sí	No
¿Ha adoptado medidas para asegurarse de que los datos personales que recoge son exactos y están actualizados?	Sí	No

Ha adoptado medidas para asegurarse de que los datos personales que trata sean veraces mientras persiste su tratamiento?	Sí	No
¿El tratamiento de los datos personales se lleva a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del usuario del servicio?	Sí	No
¿Ha verificado que el tratamiento de datos personales sea únicamente el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad?	Sí	No
¿Ha verificado si el proveedor de servicios de cómputo en la nube ha adoptado medidas para guardar confidencialidad respecto de los datos personales sobre los que se presta el servicio?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para impedir el acceso a los datos a personas que no cuenten con privilegios de acceso?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube ha implementado medidas para informar al responsable de los datos personales cuando exista una solicitud fundada y motivada de autoridad competente?	Sí	No
¿Maneja datos sensibles que hagan referencia a salud, ideología, afiliación sindical, religión, etc.?	Sí	No
¿Verifica que las bases de datos que contengan datos personales sensibles únicamente se creen cuando exista una finalidad legítima, concreta y acorde con las actividades o fines explícitos que procura el sujeto regulado?	Sí	No
¿Ha considerado la posibilidad de hacer uso de una nube privada para el tratamiento de datos sensibles?	Sí	No
¿Cuenta con mecanismos para resguardar los datos personales de tal forma que los derechos de acceso, rectificación, cancelación y oposición puedan ser ejercidos sin dilación?	Sí	No
Antes de contratar los servicios de cómputo en la nube, ¿ha revisado si el proveedor de servicios transparenta las subcontrataciones que involucren la información sobre la que se presta el servicio?	Sí	No
Se ha asegurado de que, si el proveedor de servicios subcontrata el servicio de cómputo en la nube o servicios relacionados con el mismo, ¿cuenta con la autorización necesaria?	Sí	No
¿La subcontratación de servicios de cómputo se formaliza a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido?	Sí	No
¿Ha adoptado medidas, tales como supervisiones, auditorias o certificaciones, para velar porque el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumpla con sus obligaciones en materia de protección de datos personales?	Sí	No
¿Emplea mecanismos de autorregulación para verificar que el prestador de servicios de cómputo en la nube cumpla con sus obligaciones en materia de protección de datos?	Sí	No
¿Ha verificado si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta?	Sí	No
¿Se ha informado de que el proveedor de servicios de cómputo en la nube le permite recuperar sus datos una vez que haya concluido el servicio?	Sí	No
¿Los plazos para la eliminación de los datos al finalizar el servicio son razonables?	Sí	No
¿Se ha informado o le han informado de cómo garantiza el proveedor de servicios de cómputo en la nube la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable?	Sí	No
¿Puede asegurarse de que los datos se borrarán al final del servicio por el proveedor de servicios de cómputo en la nube?	Sí	No

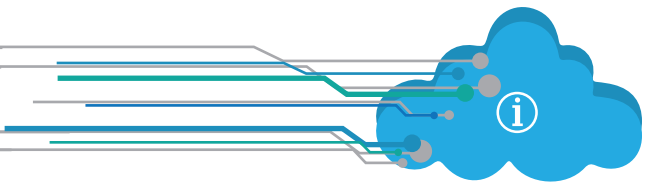
SEGURIDAD		
¿Conoce qué normatividad le aplica en materia de seguridad?	Sí	No
Antes de contratar servicios de cómputo en la nube, ¿el proveedor de servicios de cómputo en la nube le ha informado o usted ha solicitado información sobre qué medidas de seguridad ha adoptado para la protección de los datos personales sobre los que se presta el servicio?	Sí	No
¿Cuenta con medidas de seguridad para proteger los datos personales que trata?	Sí	No
¿Los datos sensibles están protegidos de tal forma que sólo las personas autorizadas pueden tener acceso a los mismos?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube ha adoptado medidas para evitar que terceros no autorizados accedan a los datos personales u otra información que trata para prestarle el servicio?	Sí	No
¿Existen mecanismos de protección de la identidad de los usuarios que acceden a datos personales para tratarlos en el desarrollo de sus funciones?	Sí	No
¿Existen reglas para el acceso de los empleados a los datos de los clientes?	Sí	No
¿Documenta el acceso de los empleados a los datos de los clientes?	Sí	No
¿Existen medidas disciplinarias para el caso de que los empleados vulneren las reglas de acceso a los datos de los clientes?	Sí	No
Aunque los datos personales, u otra información esté almacenada en la nube, ¿realiza con frecuencias copias de seguridad de los datos?	Sí	No
¿Las copias de seguridad están almacenadas en un lugar seguro?	Sí	No
Si sufre una pérdida de datos, ¿puede restaurarlos fácilmente a partir de una copia de seguridad?	Sí	No
¿Existen medidas de seguridad para prevenir la fuga de datos?	Sí	No
¿Existen procedimientos para el manejo de fugas de datos?	Sí	No
¿Se escanea con frecuencia en busca de vulnerabilidades de la red y las aplicaciones?	Sí	No
En caso de que exista un fallo en la seguridad, ¿cuenta con medidas para notificar a los titulares de los datos personales que trata en la nube?	Sí	No
¿Cuenta con procedimientos de reparación de vulnerabilidades?	Sí	No
¿Los plazos para reaccionar a una vulneración de la seguridad son razonables?	Sí	No
PROPIEDAD INTELECTUAL		
¿En los contratos SLA se estipula que todos los datos del usuario (incluyendo los que son objeto de copias duplicadas) son propiedad del mismo de manera que el proveedor de servicios de cómputo en la nube no adquiere ningún derecho de propiedad intelectual u otro título sobre los mismos?	Sí	No
¿Los contratos SLA o las condiciones de contratación que le ofrece el proveedor de servicios de cómputo en la nube, prevén de alguna manera la transferencia de derechos de propiedad intelectual?	Sí	No
¿Cuenta con contratos de licencias de software?	Sí	No
¿Cuando contrata servicios de cómputo en la nube se asegura de obtener las licencias necesarias?	Sí	No
¿Ha adoptado medidas para gestionar los activos de software, como por ejemplo cumplir con la norma ISO/IEC 19770 sobre gestión de activos de software (en inglés, Software Asset Management, SAM)?	Sí	No
¿Se ha asegurado de que el proveedor de servicios de cómputo en la nube garantice la confidencialidad respecto a la información sujeta a derechos de propiedad intelectual que transfiera a la nube?	Sí	No

ACUERDO DE NIVEL DE SERVICIO (SLA) Y OTRAS CUESTIONES CONTRACTUALES		
¿Los contratos incluyen cláusulas relativas a la interoperabilidad?	Sí	No
¿Se estipulan algunas medidas de compensación adecuadas para los usuarios en caso de que ocurra un incidente de seguridad o se incumpla con la prestación del servicio?	Sí	No
¿En el contrato de nivel de servicio se establecen cláusulas legales y contractuales que garanticen al cliente que el proveedor será sancionado en caso de incumplir con sus obligaciones o tenga fallos en la prestación de servicio?	Sí	No
¿El usuario tiene derecho a rescindir el contrato si el proveedor realiza modificaciones sustanciales a los términos estipulados en el contrato?	Sí	No
¿El usuario tiene derecho de rescindir el contrato si se incumple con las obligaciones de privacidad y seguridad estipuladas en el contrato?	Sí	No
¿Existen cláusulas de responsabilidad por pérdida de los datos o revelación indebida de los mismos por parte del proveedor o cualquier subcontratista?	Sí	No
¿Los contratos contienen previsiones sobre la finalización de los mismos?	Sí	No
¿El acuerdo de nivel de servicio contiene previsiones sobre la finalización del contrato, de manera que, si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube?	Sí	No
¿Al finalizar el contrato se entrega al cliente una copia completa de todos sus datos?	Sí	No
CIBERDELITOS		
¿Se ha asegurado de que el proveedor de servicios de cómputo en la nube tenga implementadas medidas para prevenir y, en su caso, reaccionar ante ataques informáticos?	Sí	No
¿Se ha informado antes de contratar servicios de cómputo en la nube si el proveedor cuenta con procedimientos para descubrir e investigar ataques informáticos a sus redes y servidores?	Sí	No
Con independencia de las medidas adoptadas por el proveedor de servicios de cómputo en la nube, ¿cuenta usted con medidas de seguridad para prevenir ataques informáticos?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube audita periódicamente que sus redes y sistemas de información sean seguros frente a ataques informáticos?	Sí	No
Ante una fuga de datos como consecuencia de un ataque informático, ¿el contrato o SLA con el proveedor de servicios de cómputo en la nube prevé un mecanismo de notificación al cliente y de respuesta ante la incidencia por el proveedor?	Sí	No
¿Se ha informado sobre si la arquitectura del proveedor de servicios ha sido desarrollada conforme a estándares y normas para evitar intrusiones o ataques informáticos?	Sí	No
¿Ha considerado si el proveedor de servicios de cómputo en la nube ha incluido en el contrato previsiones sobre responsabilidad en caso de que sea objeto de un ataque informático que produzca pérdida de datos o fuga de los mismos?	Sí	No
¿Ha analizado si el proveedor de servicios de cómputo en la nube cuenta con alguna póliza de seguro frente a ciberataques?	Sí	No



2.2 *Checklist* específico sobre cómputo en la nube

En el desarrollo de sus actividades, ¿utiliza o tiene planeado utilizar servicios de cómputo en la nube?	Sí	No
En el desarrollo de sus actividades, ¿tiene planeado prestar servicios de cómputo en la nube o relacionados con el cómputo en la nube? (Por ejemplo: desarrollo de aplicaciones, desarrollo de software, etc.)	Sí	No
¿Conoce las ventajas que le proporcionaría el uso de servicios de cómputo en la nube para el desarrollo de sus actividades? (Por ejemplo: ahorro de costos, la posibilidad de acceder a la información en cualquier momento y desde cualquier lugar, etc.).	Sí	No
¿Conoce las ventajas que le proporcionaría el uso de servicios de cómputo en la nube para el desarrollo de sus actividades? (Por ejemplo: ahorro de costos, la posibilidad de acceder a la información en cualquier momento y desde cualquier lugar, etc.).	Sí	No
Si usted es usuario de servicios de cómputo en la nube, ¿conoce sus obligaciones legales como responsable deltratamiento de datos personales?	Sí	No
Si usted presta servicios de cómputo en la nube, ¿conoce sus obligaciones legales como encargado del tratamiento de datos personales?	Sí	No
¿Ha analizado o identificado qué datos personales va a transferir a la nube?	Sí	No
¿Ha clasificado los datos personales en atención a su sensibilidad?	Sí	No
¿Ha analizado los diferentes tipos de nubes?	Sí	No
¿Ha analizado las modalidades de servicios de nube?	Sí	No
¿Cuenta con un contrato de prestación de servicios que reúna los requisitos establecido en el artículo 52 de la LPDP?	Sí	No
¿El proveedor tiene algún mecanismo que le permita conocer la ubicación exacta de los datos personales?	Sí	No
¿Sabe si existen subcontratos para la prestación de los servicios de cómputo en la nube?	Sí	No
¿Conoce qué servicios se prestan por los subcontratistas?	Sí	No
¿Conoce quiénes son los subcontratados?	Sí	No
¿El proveedor le ha pedido su consentimiento para realizar las subcontrataciones?	Sí	No
¿Sabe si los contratos celebrados con los subcontratistas contienen las mismas garantías judiciales que están establecidas en el contrato que usted ha celebrado con el proveedor?	Sí	No
¿Existe algún mecanismo para que usted pueda recuperar los datos personales que ha puesto a disposición del proveedor cuando se termine la relación con éste?	Sí	No
¿Ha pactado el formato en el que el proveedor deberá entregarle esta información?	Sí	No
¿En todo momento puede utilizar los datos personales que ha puesto a disposición del proveedor?	Sí	No
¿Conoce las medidas de seguridad que ha adoptado el proveedor de los servicios de cómputo en la nube?	Sí	No



¿Puede comprobar en todo momento las medidas de seguridad que ha adoptado el proveedor?	Sí	No
¿Conoce qué personas tienen acceso a los datos personales que trata el proveedor?	Sí	No
¿Puede conocer en todo momento los registros de las personas que han accedido a los datos?	Sí	No
¿El proveedor cuenta con una certificación de seguridad adecuada? (Por ejemplo: ISO 27001).	Sí	No
¿El proveedor realiza auditorías internas a sus medidas de seguridad?	Sí	No
¿Tiene la posibilidad de solicitar una auditoría a las medidas de seguridad del proveedor?	Sí	No
¿Puede acceder a los informes de las auditorías que se hayan realizado al proveedor?	Sí	No
En caso de que hayan existido incidencias en la seguridad, ¿el proveedor le ha informado sobre dichas incidencias y sobre las medidas que ha adoptado para resolverlas?	Sí	No
¿El proveedor tiene algún mecanismo para recuperar la información en caso de que exista alguna incidencia en la seguridad?	Sí	No
¿El proveedor cuenta con mecanismos reforzados de protección para los datos sensibles?	Sí	No
¿Los datos sensibles se encuentran en nubes privadas?	Sí	No
¿Existe una conexión encriptada con el servidor o la plataforma de acceso del proveedor?	Sí	No
¿Los datos almacenados o en tránsito se encuentran cifrados?	Sí	No
¿El proveedor cuenta con medidas para garantizar que, cuando termine la prestación del servicio, no conservará los datos personales que le han sido encomendados? (Por ejemplo: la emisión de una certificación)	Sí	No
¿El proveedor cuenta con mecanismos para facilitar la atención al ejercicio de los derechos ARCO de los titulares de los datos?	Sí	No

Anexo 3. Referencias

Para la elaboración de los presentes Criterios se tomaron las siguientes referencias nacionales e internacionales:

- BADGER, GRANCE, PATTCORNER,VOAS,SpecialPublication 800-146: Cloud Computing Synopsis and Recommendations, Estados Unidos, U.S Department of Commerce, National Institute of Standards and Technology, 2012. Consultable en: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

- BRADSHAW, MILLARD, WALDEN, Contracts for Clouds: Contracts and Analysis of the Terms and Condition of Cloud Computing Services, Londres, Queen Mary University of London, School of Law, 2010. Consultable en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

- CASASOLA, SOLANGE, MOLINA, MORENO, RECIO, La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo, México, Centro de Investigación y Docencia Económicas, 2014.

- Cloud Computing Security for Tenants, Australia, Department of Defence, 2015. Consultable en: http://www.asd.gov.au/publications/protect/cloud-security-tenants.htm

- Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration, The Open Group, Jericho Forum, 2009. Consultable en: https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

- Dictamen 05/2012 sobre la computación en nube, Grupo de Protección de Datos del Artículo 29, 2012. Consultable en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

- Directrices del GSR 12 sobre prácticas idóneas enfoques de reglamentación para fomentar el acceso a las oportunidades digitales mediante servicios en nube, ITU, 2012. Consultable en: https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/consultation/GSR12_BestPracticeGuidelines_SPANISH_v3.pdf

- Grupo de Trabajo – Privacy Level Agreement, Esquema de Privacy Level Agreement (PLA) para la Venta de Servicios en la Nube en la Unión Europea, Cloud Security Alliance, 2013. Consultable en: https://www.ismsforum.es/ficheros/descargas/acuerdo-de-nivel-de-privacidad1374159133.pdf

- Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (Cloud Computing), Piñar Mañas & Asociados, S.C. PROSOFT, 2013. Consultable en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_33.pdf

- ISO/IEC 19086-1:2016 Information technology -- Cloud computing -- Service level agreement (SLA) framework -- Part 1: Overview and concepts, Suiza, International Organization for Standardization and International Electrotechnical Commission, 2016.

- ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, Suiza, International Organization for Standardization and International Electrotechnical Commission, 2014.

- JANSEN, GRANCE, Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing, Estados Unidos, U.S Department of Commerce, National Institute of Standards and Technology, 2011. Consultable en: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

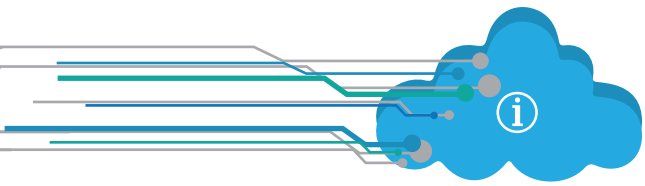
- MELL, GRANCE, Special Publication 800-145: The NIST Definition of Cloud Computing, Estados Unidos, U.S Department of Commerce, National Institute of Standards and Technology, 2011. Consultable en: http://csrc.nist.gov/publications/nist-pubs/800-145/SP800-145.pdf

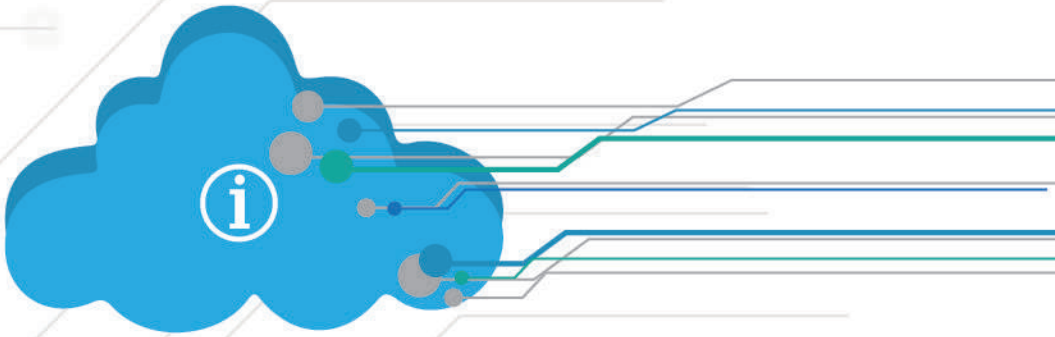
- Privacy & Cloud Computing Guideline Version 1.0, Australia, Privacy Committee of South Australia, 2013. Consultable en: http://archives.sa.gov.au/sites/default/files/20131029%20Privacy%20and%20Cloud%20Computing%20Guideline%20Final%20V1_Copy.pdf

- Privacy Level Agreement Working Group, Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union, Cloud Security Alliance, 2015. Consultable en: https://cloudsecurityalliance.org/group/privacy-level-agreement/

- SOLANGE, MORENO, RECIO, Lineamientos de Protección de Datos en el Cómputo en la Nube: Parámetros para su elaboración, México, Centro de Investigación y Docencia Económicas, 2014.

- STUDY: Cloud Service Agreements Omit Key Considerations, New ISO/IEC 19086-1 Standard Guides Organizations To Structured, Effective Agreements, Forrester Consulting, 2016. Consultable en: http://download.microsoft.com/download/7/7/E/77E57C7E-4458-47A7-8646-8AA6F2BC7EED/Cloud_Service_Agreements_Omit_Key_Considerations-Forrester_Paper.pdf





Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

SE
SECRETARÍA DE ECONOMÍA

ESTADOS UNIDOS MEXICANOS

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
Insurgentes Sur No. 3211
Col. Insurgentes Cuicuilco,
Delegación Coyoacán, Ciudad de México
C.P. 04530
www.inai.org.mx

Secretaría de Economía
Calle Pachuca No. 189
Col. Condesa, Delegación Cuauhtémoc,
Ciudad de México
C.P. 06140
http://www.gob.mx/se