GUÍA BREVE PARA SUJETOS OBLIGADOS PARA LA CONTRATACIÓN DE **SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES**

inai

GUÍA BREVE PARA SUJETOS OBLIGADOS PARA LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES

Directorio

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

Av. Insurgentes Sur 3211, Insurgentes Cuicuilco, Alcaldía Coyoacán, Ciudad de México, C.P 04530.
Edición Abril 2021.

Contenido

Contenido

A partir de las obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1] (en adelante "Ley General") y los Lineamientos Generales de Protección de Datos Personales para el sector Público[2] (en adelante los "Lineamientos"), se presenta la siguiente Guía con recomendaciones de buenas prácticas en la utilización y contratación de servicios de cómputo en la nube con proveedores externos de servicios de nube (PSN) que cuenten con sus propios Términos y Condiciones de Uso (TyC), cuando dichos servicios impliquen el tratamiento de datos personales.

1. Preguntas y Respuestas Rápidas

1.1 ¿Se pueden almacenar Datos Personales en la nube?

Sí. De conformidad con los artículos 63 de la Ley General, el responsable (Sujeto Obligado) puede contratar y adherirse a las condiciones o cláusulas generales de contratación de servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo tenga políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables en la materia.

1.2 ¿Qué medios son válidos para acreditar el cumplimiento de los requisitos necesarios para contratar servicios de nube?

El Responsable deberá verificar ciertos aspectos específicos de los TyC de los PSN, como: estándares de seguridad, herramientas para controlar el acceso a los datos, etc. Ver el punto 6.10 para más detalles.

1.3 ¿Quién puede usar esta Guía?

Cualquier Sujeto Obligado mencionado en el párrafo quinto del artículo 1, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que pretenda contratar servicios de cómputo en la nube con un PSN que cuente con sus propios TyC.

1.4 ¿En dónde se pueden alojar o tratar los Datos Personales que sean procesados como resultado de la prestación de los servicios de nube?

La Ley General no establece limitaciones respecto de la ubicación geográfica de la infraestructura de los prestadores de servicio en el que se traten o almacenen los datos personales que sean procesados como resultado de

1 Publicada en el D.O.F. el 26 de enero de 2017.
2 Publicados en el D.O.F. el 26 de enero de 2018.

la prestación de los servicios de cómputo en nube, por lo que dichos datos podrían ser tratados o almacenados dentro o fuera del país.

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 de su país, o en su caso cumplan con estándares internacionales que le permitan proteger los datos personales en su posesión.[3] De acuerdo con la Guía para el uso de cómputo en nube de la Oficina del Comisionado de Información en Reino Unido, un PSN puede tener varios centros de datos localizados en diversos países; la distribución de esta arquitectura permite mayor fiabilidad en los servicios de nube. Lo cual representa un número potencialmente mayor de ubicaciones en donde se pueden tratar los datos personales. Los responsables pueden solicitar a los PSN una lista de los países donde potencialmente se pueden tratar los datos.[4]

Por otra parte, de acuerdo con la Agencia Española de Protección de Datos, refiere por ejemplo que debe tenerse muy presente que Autoridades competentes de terceros países en los que se traten datos personales en el marco de los servicios de cómputo en nube podrían solicitar y acceder a la información de la que las Administraciones públicas son responsables, en algunos casos, sin que se les informe de esta circunstancia.

1.5 ¿Qué medidas de seguridad están previstas en la Ley?

La Ley General establece medidas de seguridad físicas, técnicas y administrativas. Ver el punto 6.2 para más detalles.

1.6 ¿La mención específica de tecnologías o estándares de seguridad de la información limita la adopción de tecnologías futuras?

No. De acuerdo con el artículo 32, fracción III de la Ley General, en la implementación de medidas de seguridad de la información, los Sujetos Obligados deberán tomar en consideración el desarrollo tecnológico. La presente guía brinda orientación a los Sujetos Obligados para que conozcan las tecnologías y estándares específicos con las que se protege

3 Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales, INAI. http://inicio.ifai.org.mx/nuevo/ComputoEnLaNube.pdf

4 https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

adecuadamente la información, como son los mencionados en los puntos 6.3 al 6.9. Dichas especificaciones serán actualizadas cada 2 años calendario con la finalidad de mantener actualizada la guía y no limitar la adopción de tecnologías futuras. La inclusión de tecnologías y estándares específicos afianzan la certeza que los Sujetos Obligados buscan tener en la elección de los mismos, minimizando la confusión que podría generar la existencia de distintas soluciones en el mercado.

2. Objetivo y Alcance

El objeto de la presente guía es brindar orientación a los Sujetos Obligados (en adelante e indistintamente Sujetos Obligados, Responsables o Clientes), que pretendan contratar la provisión externa de servicios de cómputo bajo demanda con PSN que cuenten con sus propios TyC, que implique el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente (en adelante los "servicios de cómputo en la nube"). El presente documento les permitirá contar con una metodología concreta que les ayude a evaluar el servicio ofrecido por los potenciales PSN, con la finalidad de cumplir con las obligaciones en materia de privacidad y protección de datos personales que establece la Ley General y los Lineamientos.

Esta guía puede ser utilizada por todo Sujeto Obligado; término que se define en el artículo 1, párrafo cuarto de la Ley General:

> ***"Artículo 1. (...)***
>
> *Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos."*

Los términos utilizados en este documento y no definidos aquí, tendrán el significado otorgado a ellos en la Ley General o en los Lineamientos.

3. Fundamento jurídico

Ley General

Artículo 3, fracción VI, XV.

Título Cuarto, Relación responsable y encargado, Artículos, 58 al 64.

Lineamientos

Relación Responsable y encargado

Artículos 108 a 112.

4. Servicios de cómputo en la nube

Los servicios de cómputo en la nube suplen necesidades de cara a la infraestructura, plataformas informáticas y software, convirtiéndose en una solución que día tras día ha ganado mayor relevancia para el tratamiento de información. El usuario de estos servicios no tiene necesidad de realizar inversiones en infraestructura, sino que utiliza la que pone a su disposición el PSN, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecosto asociado a dichas situaciones. Los Datos Personales y la información que sean tratados en la nube se encuentra disponibles para los Sujetos Obligados, de modo que éstos puedan cumplir con los deberes y obligaciones relacionados con dichos Datos Personales (por ejemplo, respuesta a solicitudes relacionadas con los Derechos ARCO).

Existen varias definiciones formales y ampliamente aceptadas para CN. Como referencia, utilizaremos la definición elaborada por el Instituto Nacional de Estándares y Tecnología (NIST),[5] ampliamente aceptada en la industria tecnológica:

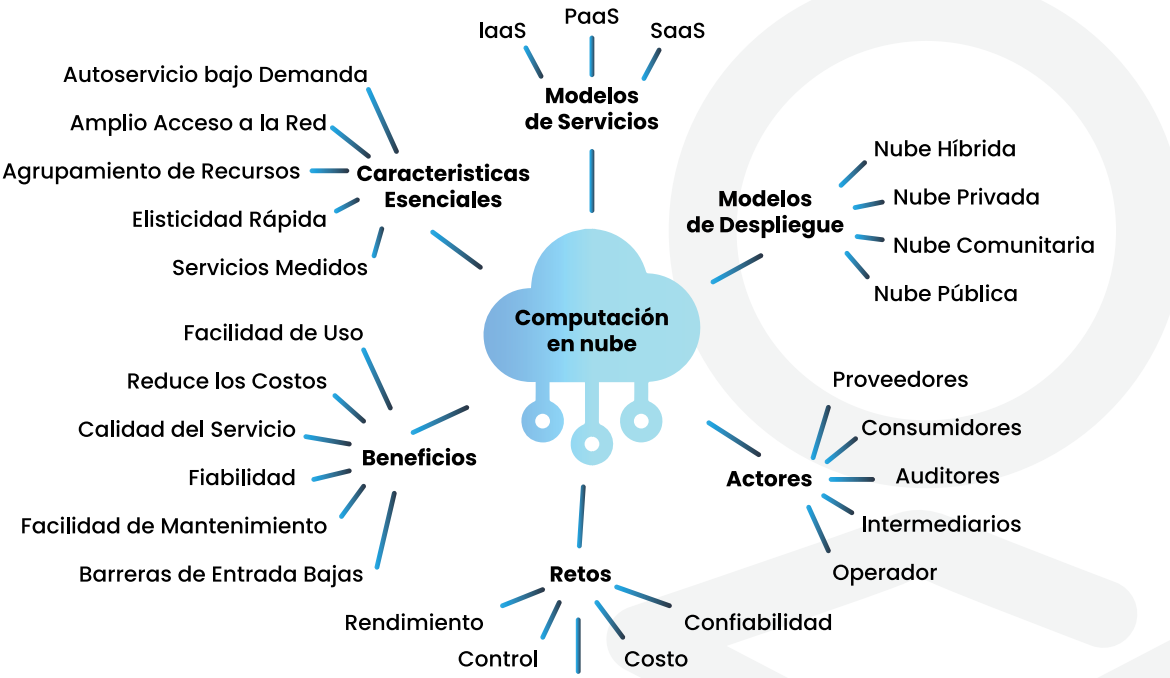
> *"Computación en nube es un modelo para facilitar el acceso ubicuo a través de red, conveniente y bajo demanda, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que pueden ser rápidamente asignados y liberados con mínimo esfuerzo de gestión o interacción con el proveedor de servicios."*

Por otra parte, derivado del artículo 3 de la Ley General, se considera al cómputo en la nube como un modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático (por ejemplo, redes, servidores, almacenamiento, aplicaciones), distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

A continuación, se ilustran los principales aspectos que conforman un sistema de cómputo en nube, los cuales se incluyen en el documento elaborado por el NIST:

5 Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

GUIA BREVE PARA SUJETOS OBLIGADOS PARA LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES



A continuación, se mencionan algunas de las características principales de los servicios de cómputo en nube:

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.

Los servicios de cómputo en la nube revisten un particular interés cuando su prestación implica el tratamiento de datos personales, lo que hace necesario

prestar especial atención en las condiciones ofrecidas por los distintos PSN y las garantías que representen para la seguridad y la protección de los datos.

En este sentido, la presente guía se enfoca a todo servicio de cómputo en la nube proporcionado por un PSN que cuente con sus propios TyC, quien se identifica bajo la figura de encargado de datos personales, sin importar la ubicación geográfica de la infraestructura, el tipo de tecnología utilizada, o si actúa dentro del perímetro o las instalaciones 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:

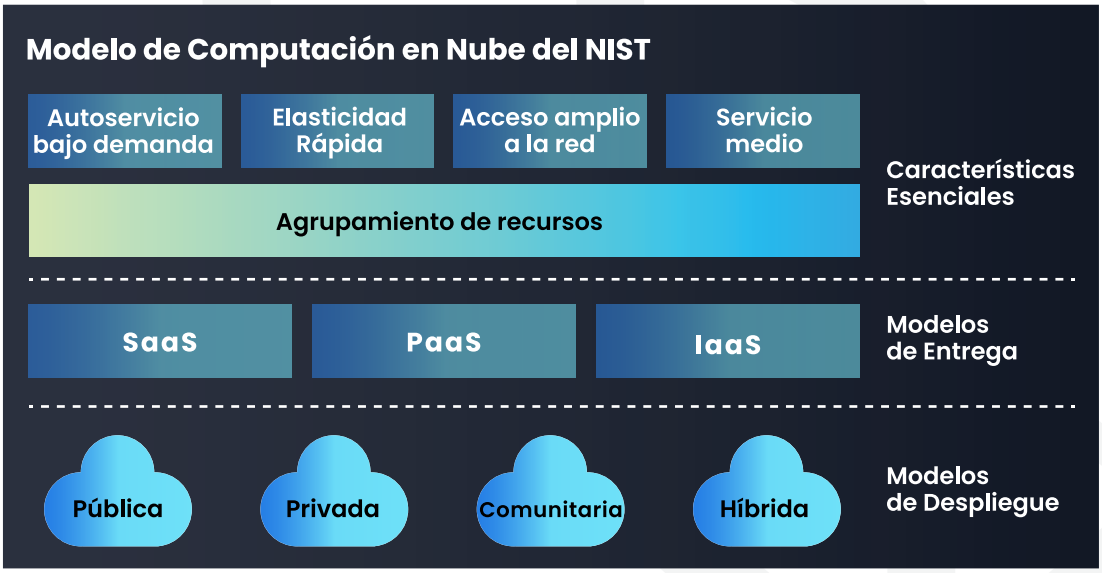
a. **Infraestructura como Servicio** *(Infrastructure as a Service o IaaS)*: La infraestructura como servicio, contiene los bloques de creación fundamentales para la Tecnología de la Información (TI) en la nube. Por lo general, permite acceder a las características de conexión en red, a los equipos (virtuales o en software dedicado) y al espacio de almacenamiento de datos. La infraestructura como servicio le ofrece el mayor nivel de flexibilidad y control de la administración en torno a sus recursos de TI y guarda el mayor parecido con los recursos de TI existentes con los que muchos departamentos de TI y desarrolladores están familiarizados.
b. **Plataforma como Servicio** *(Platform as a Service o PaaS)*: Las plataformas como servicio eliminan la necesidad de las organizaciones de administrar la infraestructura subyacente (normalmente hardware y sistemas operativos) y le permiten centrarse en la implementación y la administración de sus aplicaciones. Esto contribuye a mejorar su eficacia, pues no tienen que preocuparse del aprovisionamiento de recursos, la planificación de la capacidad, el mantenimiento de software, los parches ni ninguna de las demás arduas tareas que conlleva la ejecución de su aplicación.
c. **Software como Servicio** *(Software as a Service o SaaS)*: El software como servicio les proporciona a los clientes un producto completo que el PSN ejecuta y administra. En la mayoría de los casos, quienes hablan de software como servicio en realidad se refieren a aplicaciones de usuario final. Con una oferta de SaaS, el cliente no tiene que pensar en cómo se mantiene el servicio ni en cómo se administra la infraestructura subyacente. Solo debe preocuparse por cómo utilizar ese sistema de software concreto. Un ejemplo común de una aplicación SaaS es un programa de correo electrónico basado en la web que le

permite enviar y recibir mensajes sin tener que administrar la incorporación de características ni mantener los servidores y los sistemas operativos en los que se ejecuta, por ejemplo, el programa de correo electrónico.

Con el tiempo se han agregado distintas denominaciones que usualmente vemos identificadas como XaaS (X como Servicio), que se refieren a casos de servicios especializados que en realidad utilizan uno de los tres modelos fundamentales, en su mayor parte SaaS. Independiente del modelo de que se trate, el PSN puede implementar protocolos de encriptación para proteger la diseminación de información en la red, como se explica en los puntos 6.2 y 6.3.

Por otro lado, para el despliegue de la plataforma de nube se pueden adoptar varios modelos, a saber: Nube Pública, Nube Privada, Nube Comunitaria y Nube Híbrida, aunado a que se recomienda utilizar el concepto completo al que se refiere: Modelos de implementación. Y detallar un poco sobre los cuatro tipos de modelos de implementación o de despliegue y mejorar la calidad de la imagen y utilizar una que ejemplifique todos los modelos de computación en la nube contemplados en el documento Special Publication 800-146 de NIST, como la siguiente:

A continuación, se ilustran los modelos de servicio y despliegue básicos de CN[6].



6 Elaboración de imágenes a partir de la definición de sistema computación en nube del NIST.

GUIA BREVE PARA SUJETOS OBLIGADOS PARA LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES

5. Responsabilidad Compartida

5.1 Responsables y Encargados

La contratación de servicios de cómputo en nube implica la existencia de una relación jurídica entre un encargado (el PSN) y un responsable (el Sujeto Obligado).

Los Sujetos Obligados tienen el carácter de **responsables,** los cuales se definen como aquellos que deciden sobre el tratamiento de los Datos Personales.

Por otra parte, de acuerdo con el artículo 3, fracción XV de la Ley General, un **encargado** se define como la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del responsable.

En los servicios de cómputo en la nube, los datos personales que se traten serán procesados por parte del PSN a nombre y por cuenta del Sujeto Obligado correspondiente. En consecuencia, el PSN tendrá el carácter de encargado, como lo establece el artículo 111 de los Lineamientos.

Para que el tratamiento de datos personales en los servicios de cómputo en nube tenga lugar, los datos personales deben ser comunicados por parte del responsable al encargado. Lo anterior, no implica la existencia de obligaciones en materia de transferencia de datos personales puesto que, como será explicado a continuación, el envío de datos realizado entre un responsable y un encargado no es considerado una transferencia de datos personales.

La comunicación de datos personales realizada exclusivamente entre el responsable y el encargado, ya sea dentro o fuera del territorio nacional, es considerada una remisión y, como tal, no requiere ser informada al Titular de Datos, ni contar con su consentimiento, de conformidad con los artículos 3, fracción XXVII y 71 de la Ley General.

Aunque el PSN tiene ciertos deberes y obligaciones (como se detalla más abajo), el Sujeto Obligado es responsable ante el Titular de Datos respecto de los datos personales que sean tratados como resultado de la provisión de los servicios de cómputo en nube.

5.2 Responsabilidades de los Sujetos Obligados

Los Sujetos Obligados son responsables de la seguridad del contenido que almacenan o procesan utilizando los servicios de cómputo en la nube

que elijan. Lo anterior, teniendo en cuenta que los Sujetos Obligados son quienes determinan qué contenido almacenan o procesan utilizando estos servicios y el nivel de seguridad que dicho contenido requiere, conforme al análisis de riesgos que lleven a cabo. Corresponde a los Sujetos Obligados administrar de manera segura el servicio, de acuerdo con los controles que implementen y las herramientas que les suministre el PSN.

Dentro de los controles que los Sujetos Obligados pueden implementar para dar seguridad a su contenido, se encuentran los siguientes:

- Políticas de contraseña fuertes, asignando permisos apropiados a los usuarios y tomando medidas sólidas para proteger sus claves de acceso;
- Cortafuegos apropiados y segmentación de red;
- Encriptación de contenido, y
- Diseñar sistemas de arquitectura resilientes.

Independientemente de lo anterior, y con base al Artículo 42 de la Ley, el Responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

En el capítulo 6 se describen algunos criterios mínimos de seguridad recomendados.

De acuerdo con el artículo 64 de la Ley General, los sujetos obligados se deben cerciorar del cumplimiento de las siguientes condiciones al momento de contratar a un PSN:

Artículo 64. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrán utilizar aquellos 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 presente Ley y demás normativa aplicable;*
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 preste el servicio, y*
d) *Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;*

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 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, conforme a la presente Ley y demás disposiciones que resulten aplicables en la materia.

5.3 Responsabilidades de los PSN

Los PSN son responsables de proteger la infraestructura que ejecuta todos los servicios provistos en la nube. En términos generales, corresponde a los PSN tener procesos y procedimientos establecidos para garantizar la seguridad operativa del servicio, gestionar el sistema operativo central (host) y proporcionar a los usuarios las herramientas necesarias para que administren de manera segura el servicio.

Los PSN también asumen responsabilidad por los servicios de nube que prestan, esto en calidad de encargados.

De acuerdo con el artículo 59 de la Ley General, las obligaciones mínimas del encargado consisten en:

1. Tratar los datos personales únicamente conforme a las instrucciones del responsable.
2. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
3. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
4. Guardar confidencialidad respecto de los datos personales tratados.
5. Suprimir o devolver los datos personales objeto del tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
6. Abstenerse de transferir los datos personales salvo en el caso de que

el responsable así lo determine, o la comunicación derive de una subcontratación, por mandato expreso de una autoridad competente.

Respecto de la supresión de los datos, en caso de que el Sujeto Obligado no elimine la información contenida en el servicio una vez concluida la relación jurídica con el PSN, dichos datos podrán ser bloqueados y posteriormente eliminados por el PSN de acuerdo con lo estipulado en los TyC correspondientes.

Respecto de las medidas de seguridad, el PSN debe de ofrecer la funcionalidad para cifrar la información en tránsito y en reposo (ver puntos 6.2 y 6.3). Únicamente el Sujeto Obligado puede activar o desactivar dicha funcionalidad u otorgar privilegios de acceso e impedir el acceso a su información.

Con relación a las transferencias por mandato expreso de una autoridad competente, en caso de que el PSN reciba una solicitud de acceso, debidamente fundada y motivada, por parte de la autoridad competente, el PSN informará al Sujeto Obligado de dicha solicitud siempre y cuando no se encuentre legalmente impedido para ello.

6. Cumplimiento de obligaciones para la contratación de servicios de cómputo en la nube

6.1 Medidas de seguridad previstas por la Ley General

De acuerdo con el artículo 64, fracción II, inciso c) de la Ley General, los encargados deben establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio de cómputo en nube. Las medidas de seguridad descritas en el presente numeral buscan proteger los datos personales contra daño, pérdida, alteración, destrucción, o uso, acceso o tratamiento no autorizado.

La Ley General establece las siguientes medidas de seguridad:

a) Administrativas.
b) Físicas.
c) Técnicas.

De acuerdo con el artículo 3, fracción XXI de la Ley General, las medidas de seguridad administrativas se refieren al establecimiento de políticas y procedimientos para:

a) La gestión, soporte y revisión de la seguridad de la información a nivel organizacional.
b) La identificación, clasificación y borrado de la información.
c) La sensibilización y capacitación del personal, en materia de protección de datos personales.

De acuerdo con el artículo 3, fracción XXII de la Ley General, por medidas de seguridad físicas se entiende el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Las medidas de seguridad ***físicas*** se refieren al establecimiento de políticas y procedimientos para:

a) Prevenir el acceso no autorizado al perímetro de la organización, instalaciones físicas, áreas críticas, recursos e información.
b) Prevenir daño o interferencia a instalaciones físicas, áreas críticas de la organización, recursos e información.
c) Proteger recursos móviles, portátiles, soportes físicos o electrónicos que salgan de la organización.
d) Proveer equipos que almacenan datos personales de mantenimiento eficaz.

De acuerdo con el artículo 3, fracción XXIII de la Ley General, por medidas de seguridad técnicas se entiende como conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Las medidas de seguridad ***técnicas*** se refieren al establecimiento de políticas y procedimientos para:

a) Asegurar que el acceso a las bases de datos sea por usuarios identificados y autorizados.
b) Generar privilegios o perfiles de acceso a los datos personales en función de las atribuciones y funciones de cada usuario.
c) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.
d) Revisar la configuración de seguridad del software y hardware.
e) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

En caso que los servicios contratados impliquen un tratamiento intensivo de datos personales, el Sujeto Obligado deberá realizar una Evaluación de Impacto en la Privacidad.

Por otra parte, en la valoración de los servicios ofrecidos por el PSN, el responsable deberá en todo momento observar los principios y deberes de protección de

datos personales, que son: legalidad, consentimiento, información, calidad, propósito, lealtad, proporcionalidad y responsabilidad.

A continuación, se expone una serie de recomendaciones que puede ser utilizada por los responsables, y que es relativa a mejores prácticas para almacenar o procesar datos personales en la nube.

6.2 Seguridad de la Información almacenada o en reposo

Debido a la especial sensibilidad de los datos tratados por los Sujetos Obligados, la aplicación de técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados, constituye una medida necesaria para garantizar su confidencialidad, es por eso que, se recomienda el uso de cifrado en sus sistemas de almacenamiento[7], utilizando por lo menos la encriptación AES de 256 bits. Por otro lado, se recomienda utilizar mecanismos de autenticación de múltiples factores (AMF) para el acceso a los servicios y datos personales.

La autenticación de múltiples factores (AMF) es un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser. Estas pruebas pueden ser diversas, como una contraseña, que posea una clave secundaria rotativa, o un certificado digital instalado en el equipo, entre otras.

6.3 Seguridad de la Información en tránsito

Para la protección de la seguridad de la información en tránsito, entre los diferentes sistemas del PSN y/o, en su caso, de sus subcontratistas, y entre los sistemas del responsable y el PSN y/o, en su caso, de sus subcontratistas, se recomienda cifrar el canal de comunicaciones (información en tránsito) utilizando Transport Layer Security 1.2 (TLS, anteriormente denominado Secure Sockets Layer [SSL]). Transport Layer Security 1.2 es un protocolo de encriptación utilizado para proteger la diseminación de información en la red.[8]

6.4 Disponibilidad e integridad

Para la protección de la disponibilidad e integridad de la información del Sujeto Obligado, se recomienda realizar copias de respaldo de los datos personales para permitir su recuperación en caso de pérdida o destrucción. Se deben realizar pruebas de recuperación de los datos personales respaldados; para comprobar que las copias de respaldo pueden ser utilizadas en caso de ser requerido.

7 Guía para clientes que contraten servicios de Cloud Computing [sep 2018]: https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf

8 NIST Special Publication 800-52. Revision 2.

6.5 Privacidad desde el Diseño

Adicionalmente, se sugiere a los Sujetos Obligados que incorporen buenas prácticas de protección de datos, ética y seguridad de la información desde el diseño (Privacy by Design, PbD), a través del ciclo de vida de los datos en las soluciones desarrolladas.

	Principios Fundacionales de la Privacidad desde el Diseño
1	Proactivo, no reactivo
2	Preventivo, no correctivo
3	La privacidad como configuración predeterminada
4	Privacidad incorporada en la fase de diseño
5	Funcionalidad total: pensamiento "todos ganan"
6	Aseguramiento de la privacidad en todo el ciclo de vida
7	Visibilidad y transparencia

Tabla 1 –Principios de la "Privacidad desde el diseño"

Para más información ver la "Guía de Privacidad desde el Diseño", documento desarrollado por la Agencia Española de Protección de Datos[9].

6.6 Borrado Seguro

Para la protección de los datos personales a lo largo de su ciclo de vida, así como en general de cualquier información que represente un activo para una organización, es importante, contar con una medida de seguridad que permita minimizar el efecto de cualquier tipo de recuperación de información no autorizada, sobre los medios de almacenamiento físicos y electrónicos, relacionados con el tratamiento de datos personales que desecha una organización. Por lo tanto, el borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

Se considera indispensable que el Sujeto Obligado cuente con mecanismos o sistemas para el borrado seguro de la información, una vez finalizado el servicio. El Encargado no podrá quedarse con una copia de la información una vez que el Responsable ejecute la acción de borrado.

9 Guía de Privacidad desde el Diseño – Agencia Española de Protección de Datos (https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf)

Para conocer los métodos de borrado seguro, se sugiere consultar la Guía para Borrado Seguro de los Datos Personales, emitida por el INAI[10] y publicada en su página web, la cual permite conocer métodos y técnicas basadas en las mejores prácticas y estándares, para la eliminación segura de los datos personales en los sistemas de tratamiento.

6.7 Control sobre el Acceso y Gestión

Para que el Sujeto Obligado tenga control sobre el acceso y gestión de los datos, procesos o servicios, se recomienda controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales; mediante la adopción de las siguientes medidas:

a) Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.
b) Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.
c) Obligar al usuario a cambiar la contraseña asignada de manera periódica.
d) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
e) Cancelar el acceso a los usuarios cuando dejen de trabajar con el Sujeto Obligado o en las funciones que requieran el acceso a los datos personales.

Se debe revisar periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado por el responsable. Esta revisión debe generar un registro que evidencie la realización de esta revisión.

6.8 Otras recomendaciones

Se recomienda que, el Sujeto Obligado opte por un PSN que además cuente con las medidas siguientes:

- Mostrar evidencia, de estar sujetos a revisiones, o auditorías por terceros de reconocido prestigio, o en cumplimiento con estándares internacionales, como son ISO/IEC 27017 e ISO/IEC 27018. Estas

10 http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

certificaciones, pueden ser un medio creíble para que los PSN demuestren que han establecido y mantienen medidas de seguridad para la protección de los datos personales, según lo especificado en la Ley General. Dichas certificaciones indicarían, como mínimo, que los controles de protección de datos han sido objeto de una auditoría o revisión con respecto a una norma reconocida por una organización tercera de reconocido prestigio.

- Contar con evidencia de cumplimiento del informe de Control de organizaciones y sistemas (SOC) 2: Seguridad, Disponibilidad y Confidencialidad, la cual que demuestra que el PSN ha cumplido los principios y criterios de seguridad, disponibilidad y confidencialidad de servicios de confianza de AICPA[11]

6.9 Medios para acreditar el cumplimiento

A continuación, se describen los medios para acreditar el cumplimiento del artículo 64 de la Ley General tomando como base servicios de nube en modelo de Infraestructura como Servicio (Infrastructure as a Service o IaaS):

Tabla A. Medios para acreditar el cumplimiento del artículo 64 de la Ley General.

No.	Obligación del Responsable	Medios para acreditar el cumplimiento	Cumple	
			SÍ	No
1	Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;	Solicitar al PSN sus Términos y Condiciones que rigen el tratamiento del contenido, para asegurarse que el Responsable tiene control completo del contenido; que le permita cumplir con los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable.		
2	Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio	Verificar que los PSN sean transparentes sobre los subcontratados que utilizan para procesar la información sobre la que se presta el servicio.		
3	Abstenerse de incluir condiciones en la prestación del servicio, que le autoricen o permitan al PSN asumir la titularidad o propiedad de la información sobre la que preste el servicio.	Verificar que los Términos y Condiciones del PSN, no incluyan condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.		

11 https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc-2report.html

No.	Obligación del Responsable	Medios para acreditar el cumplimiento	Cumple	
			SÍ	No
4	Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.	Verificar que el PSN implemente estándares de seguridad apropiadas en los servicios que los Responsables utilizan para los datos personales.		
5	Dar a conocer al responsable, los cambios en sus políticas de privacidad o condiciones del servicio que presta, para que, de resultar necesario, el responsable los haga del conocimiento de los titulares de datos.	Verificar en los Términos y Condiciones u otros mecanismos del PSN, la forma en la que el Responsable podrá conocer los cambios a los Términos y Condiciones.		
6	Que el PSN permita al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.	Verificar que los Términos y Condiciones del PSN permitan al Responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.		
7	Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.	Verificar que el PSN implemente estándares de seguridad apropiadas en los servicios que los Responsables utilizan para los datos personales.		
8	Que el PSN provea funcionalidades al Responsable, que le permitan la supresión de los datos personales; una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos	Verificar que, el PSN permita a los Responsables eliminar su contenido bajo demanda. Los Responsables tendrán que eliminar los datos una vez finalizado el servicio; ya que los PSN únicamente permiten al Responsable borrar su información.		
9	Que el PSN provea funcionalidades al Responsable, para 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	Verificar que el PSN proporcione al Responsable herramientas para controlar el acceso a su contenido en la nube, incluyendo los datos personales.		

GUIA BREVE PARA SUJETOS OBLIGADOS PARA LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE QUE IMPLIQUEN EL TRATAMIENTO DE DATOS PERSONALES

7. Anexo y Glosario

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Responsable: Sujeto obligado de la Ley General de Protección de Datos

Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

INAImx INAImexico inai_mx inaimexico