MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"CÓMPUTO EN LA NUBE. PROPUESTA DE UN MODELO DE POLÍTICA PARA PROTECCIÓN DE DATOS PERSONALES PARA PROVEEDORES DE SERVICIOS DE CÓMPUTO EN LA NUBE"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de
MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:
Rodrigo Méndez Solís

Asesores:
Dra. Paulina Elisa Lagunes Navarro
Dr. Francisco Gomeztagle Sepúlveda

Ciudad de México, julio de 2020

CONACYT

INFOTEC POSGRADOS

Autorización de impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 16 de junio de 2021
INFOTEC-DAIC-GCH-SE-190/2021.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

CÓMPUTO EN LA NUBE. PROPUESTA DE UN MODELO DE POLÍTICA PARA PROTECCIÓN DE DATOS PERSONALES PARA PROVEEDORES DE SERVICIOS DE CÓMPUTO EN LA NUBE

Desarrollado por la alumno **Rodrigo Méndez Solís** y bajo la asesoría de la **Dra. Paulina Elisa Lagunes Navarro** y el **Dr. Francisco Gomeztagle Sepúlveda**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Lic. Juan Ramón Abarca Damián
Coordinador de Biblioteca

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

Para Goltzio La’Pilli.

Tabla de contenido

Introducción

Pareciera que las nuevas tecnologías y la ciencia del Derecho son polos opuestos, ya que de alguna forma las humanidades y la técnica comúnmente son contrapuestas y consideradas incompatibles. Seguir pensando así es un grave error, ya que el Derecho es una ciencia dialógica; lo cual significa que se encuentra en un constante diálogo con la realidad y que, por tanto, tiene capacidad de ayudar a regular todo lo que se encuentra a su paso tal y como es el caso de las Tecnologías de la Información y la Comunicación (TIC).

Actualmente, la mayoría de nosotros tiene acceso a dispositivos móviles o fijos con acceso a Internet y con ellos a diversas plataformas electrónicas en las que, de manera consciente o inconsciente, uno crea y comparte contenido con terceros al contratar servicios que se ofrecen dentro de Internet.

Hoy en día existen dentro de Internet diversos productos que ayudan a que nuestra vida diaria sea más práctica y entretenida, tales servicios pueden ser correos electrónicos públicos, redes sociales, aplicaciones para trabajar, videojuegos para entretenerse, entre otros y es a través de estas aplicaciones que accedemos a una serie de servicios dentro de la plataforma del prestador de servicios, que no sólo es el de tener una cuenta de e-mail para comunicarnos, sino acceder a otras aplicaciones como lo son: contar con un disco duro virtual en el que podemos almacenar nuestra información y archivos y así liberar nuestro disco duro físico; utilizar el *software* de un procesador de textos, creador de hojas de cálculo y de presentaciones para trabajar en línea con nuestros colegas o amigos; acceder a un procesador de imágenes y crear álbumes fotográficos en él y editarlos; tener un registro de nuestros contactos, localizaciones, calendario; organizar chats o video conferencias con nuestros contactos e incluso terceros a través de compartir un link. Lo interesante de estos servicios es que, en su gran mayoría, requieren almacenar información de nuestra persona, pero para ello es indispensable que nos sujetemos a sus términos y condiciones.

Lo anterior representa diversas ventajas en el sentido que, a través de aplicaciones fácilmente accesibles (y en algunos casos gratuitas) podemos obtener servicios proporcionados por terceros, pero con la puesta a disposición de nuestra información que queda almacenada en servidores de terceros. Esto tiene el inconveniente de que como usuarios tenemos que sujetarnos a diversos términos y condiciones y muchas veces no sabemos si en verdad nuestra información se encuentra debidamente protegida en términos de lo que establece nuestra legislación. El problema de ello es que, de alguna manera, estamos confiando a ciegas en que el proveedor de servicios considere lo más adecuado para proteger nuestra información, cuestión que dejaría de preocuparnos si tuviéramos conocimiento de cuáles son las responsabilidades que este tercero se compromete a asumir, así como aquellas políticas de resguardo de información que implementará para proteger nuestros datos de terceros.

El presente trabajo tiene como objetivo proponer un modelo de política interna de protección de datos personales para empresas privadas de *cloud computing*, a través del análisis realizado sobre algunos aspectos técnico-jurídicos de lo que significa e implica prestar un servicio a través de un modelo de cómputo en la nube tales como: el rol que tienen los prestadores de este servicio, así como sus revendedores, en la prestación del servicio; las implicaciones que surgen en temas de propiedad intelectual y de seguridad de la información, y finalmente las obligaciones en materia de protección de datos personales que las empresas prestadoras de este servicio deben asumir a fin de cumplir con la normativa aplicable en México, haciendo especial hincapié en los beneficios y desventajas que se tienen como prestador de servicios y como usuario final en un servicio como lo es éste.

Asimismo, dado que éste es un servicio de TIC a disposición de la llamada *sociedad de la información*[1] reglamentado por normativa no sólo técnica sino que

[1] La definición que, a mi consideración es la más completa es la que realiza el Ministerio de Tecnologías de la Información y las Comunicaciones quién lo define como "*aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas debe estar centrada en la persona,*

también legal, en este trabajo de titulación me enfocaré en el análisis de la regulación e implicaciones jurídicas que se encuentran implícitas en su prestación y su contratación que existen hoy en México.

El modelo de política interna que propondré tiene como objetivo que puedan utilizarlo aquellos proveedores de servicios de *cloud computing* que requieran llevar a cabo el correcto tratamiento de la información que reciben por parte de sus clientes, pero, sobre todo, de aquellos datos personales que almacenen a fin de cumplir con aquellas medidas requeridas por la normativa de privacidad y protección de datos personales aplicable en México.

La conveniencia del modelo que propondré, es que éste se basará en los principios rectores de la normativa en materia de protección de datos personales, mismos que han tenido la característica de ser atemporales y mundialmente reconocidos[2]; por ello, en caso de haber una reforma legislativa sustancial o un avance importante en materia tecnológica que modifique radicalmente el modelo actual de *cloud computing*, el formato de política interna que propondré podrá ser válido de tiempo en tiempo y aquella empresa que lo implemente podrá hacer actualizaciones a medida que cambie la normativa o avance la tecnología.

---

integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida." disponible en *https://mintic.gov.co/portal/inicio/5305:Sociedad-de-la-Informaci-n*, última fecha de consulta 13 de enero de 2020.

[2] Privacy International, A Guide for Policy Engagement on Data Protection, Part 3: Data Protection Principles: disponible en: *https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf*, última fecha de consulta 13 de febrero de 2020.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010, artículo 6º "*Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley."*

Capítulo 1
Definiciones y conceptos básicos del cómputo en la nube

Capítulo 1. El cómputo en la nube

El *cloud computing* es una tecnología que facilita que los usuarios aprovechen la capacidad de procesamiento y almacenamiento proveniente de servidores de terceros. Los servicios que se prestan a través del cómputo en la nube, desde su surgimiento a la actualidad, han ido revolucionando y facilitando la manera en que tanto las organizaciones y como los particulares acceden y comparten información.

La evolución del cómputo en la nube ha ido demostrando que para un usuario promedio, lo único que necesita, es un dispositivo electrónico con acceso a Internet y acceder a sus archivos o el *software* que necesita para trabajar, divertirse u organizarse. Si bien es cierto, el término *nube* no es del todo correcto ya que, en estricto sentido, se necesita que la información quede almacenada en una unidad de almacenamiento físico (en este caso los discos duros y servidores que proporcionan los prestadores de servicios) y es por tanto que este servicio no es algo intangible como pudiera presuponerse cuando decimos que los archivos se encuentran *en la nube.*

A lo largo de la evolución de los servicios de cómputo en la nube han surgido dos corrientes claramente diferenciadas entre sí: (a) aquellos que siguen apostando por esta tecnología y ven a las inversiones que se realizan en ella como el principal motor para que ésta sea una herramienta cada vez más accesible a todo el público, y (b) aquellos que ven en esta tecnología como el triunfo de un producto de monopolización por parte de las grandes compañías (e incluso gobiernos) a efectos tener a la información de sus usuarios (ciudadanos) encadenada en servidores fuera de su control.

Uno de los mayores detractores de los servicios de cómputo en la nube es el fundador del sistema operativo con licencia GNU y la Fundación de *Software* Libre, Richard Stallman[3], quien defiende que la información que cada uno conciba debe

[3] Entrevista a Richard Stallman en *The Guardian* el 29 de septiembre de 2008, disponible en *https://www.theguardian.com/technology/2008/sep/29/Cloud.computing.richard.stallman,* última fecha de consulta 13 de marzo de 2020.

permanecer en donde se generé y no en manos de un tercero; siendo el cómputo en la nube una *trampa* que han puesto las grandes corporaciones con el único fin de mantener a sus usuarios cautivos en sus propios sistemas de almacenamiento de información.

Los riesgos y las virtudes del cómputo en la nube han ido poco a poco evolucionando -como toda tecnología- y poco a poco ha llegado al uso, conocimiento y adopción de la generalidad. Muchas veces el usuario no especializado en la utilización de Internet, ha ido empezado a caer en el uso de estos sistemas sin ni siquiera darse cuenta; tal es el caso de cuando se envía un documento a través del correo electrónico, o cuando se sube un archivo a la red con el motivo de poder compartirlo con otros o acceder a este desde cualquier parte en donde nos encontremos. Esto pasa con las aplicaciones que provee de manera gratuita Google, como lo es Google Docs en donde podemos enviar y trabajar sobre documentos de manera colaborativa y en tiempo real u otras plataformas o redes sociales tal y como lo son: Microsoft One Drive; Google Drive; Google Photos, Facebook, Instagram, Tumblr, SoundCloud, entre otros, que son herramientas en las que los usuarios utilizan su infraestructura para almacenar información, crear álbumes digitales de audio o video online, los cuales podemos mantener de manera privada o compartir con terceros. Esta manera es una forma de hacer cómputo en la nube y ha sido adoptada por un número enorme de usuarios que ni siquiera saben que están utilizando un servicio de esta índole[4].

El presente capítulo tiene como finalidad darle al lector las herramientas principales para entender cómo se realiza la prestación de servicios de *cloud computing*, por lo que se revisan aquellas posturas que se encuentran a favor y en contra de este negocio, cuáles son los elementos técnicos que intervienen en la prestación del servicio, y cómo es que este servicio puede ser adoptado de manera moldeable tanto por particulares como por pequeñas y medianas empresas

[4] Schubert, L., Jeffery, K. y Neidecker-Lutz, B. *The Future of cloud computing* – Report from the first *cloud computing* Expert Working GMeeting. Cordis (*Online*), BE: European Commission ed., 2010, disponible en *http://cordis.europa.eu/fp7/ict/ssai/docs/Cloud-report-final.pdf*, última fecha de consulta 13 de abril de 2020.

(*PYMES*) para su realización y simplificación de sus tareas diarias sin que sea necesaria el desembolso de una cantidad de recursos económicos importantes para su adopción.

Actualmente, son varias las discusiones y opiniones acerca del origen de la palabra cómputo en la nube; a mi parecer, el origen más sensato y en el que la mayoría coincide es aquel que se la atribuye al científico John McCarthy[5], y a la materialización de la palabra al momento en que los ingenieros y diseñadores de redes hacen en sus diagramas de flujo al referirse al Internet, ya que lo representan como una "nube" rodeada de dispositivos que transfieren y obtienen información que se encuentra en la misma.

Sin ahondar más en este tema, y para los efectos del presente trabajo, definiremos la palabra de cómputo en la nube como aquella tecnología que permite que de manera virtual y escalable, una entidad denominada proveedor suministre a través de Internet, a una o varias personas denominadas clientes, recursos tales como datos y/o aplicaciones mediante servicios o tecnologías diversas tales como: Infraestructuras como servicio (*IaaS*), Plataformas como Servicio (*PaaS*) y/o el *Software* como Servicio (*SaaS*).

1.1. Elementos

En términos generales, se entiende al cómputo en la nube como una arquitectura de red mediante la cual, datos o aplicaciones se encuentran en servidores propiedad de un tercero (*prestador*), y a los cuales personas físicas o morales (*clientes*) que lo tienen contratado, pueden acceder a los mismos de manera remota a través de cualquier dispositivo con conexión a Internet.

[5] López Jiménez, David. *La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español*, Revista de Derecho de la Pontificia Universidad Católica de Valparaíso no. 40 Valparaíso ago. 2013, disponible en: *https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512013000100021*, última fecha de consulta 13 de mayo de 2020.

1.1.1 La virtualización

En palabras técnicas, “la virtualización es un término amplio que se refiere a la abstracción de los recursos de una computadora; este término es bastante antiguo y viene siendo utilizado desde antes de 1960, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos hasta capacidades o componentes individuales[6]”.

Microsoft define a la virtualización como una tecnología clave para la administración de ambientes de IT la cual permite acelerar los tiempos de entrega de aplicaciones, y su actualización centralizada, sin necesidad de replicar la instalación en cada computadora que utilice soluciones virtualizadas, permitiendo de igual forma, crear una infraestructura de servicios simple de administrar y de rápida instalación, lo cual ayuda a reducir los costos de los departamentos de IT de empresas y organizaciones, siendo las aplicaciones instaladas en un servidor central y entregadas en la computadora de los usuarios, en forma de imagen virtualizada, minimizando las alteraciones que produce en el sistema operativo y sin provocar cambios en otras aplicaciones[7].

Bob Muglia, vicepresidente en el 2006 de la división Servidores y herramientas de Microsoft, señaló al momento en que Microsoft hizo la compra de la empresa de virtualización de aplicaciones Softricity que “con las aplicaciones virtualizadas y *software* bajo modalidad *streaming*, Microsoft permite que los usuarios accedan a estas soluciones al nivel de la PC, en lugar de hacerlo solamente en los servidores. Esto es una parte importante de la estrategia de Microsoft, ya que ahora los clientes podrán correr aplicaciones virtualizadas y mantener sus sistemas dinámicos sin necesidad de actualizar sus equipos en forma

[6] Brodkin, Jon; With long history of virtualization behind it, IBM looks to the future. Networld World, disponible en *https://web.archive.org/web/20090504085115/http://www.networkworld.com/news/2009/043009-ibm-virtualization.html*, última fecha de consulta 13 de junio de 2020.

[7] Descripción disponible en *https://docs.microsoft.com/en-us/windows-server/virtualization/virtualization*, última fecha de consulta 13 de junio de 2020.

permanente, permitiendo a la vez contar con las últimas versiones de las aplicaciones provistas por los fabricantes[8]".

El tema que tienen en común aquellas tecnologías de virtualización es la de ocultar detalles técnicos a través de la encapsulación; en otras palabras, lo que realiza la virtualización es crear una interfaz externa de recursos en locaciones físicas diferentes.

La importancia que este término genera en el cómputo en la nube es que la tecnología permite ofrecer a sus usuarios el uso de manera remota de *hardware* físico y/o almacenamiento virtual en cuestión de segundos y, por lo tanto, ofrece la flexibilidad de añadir o disminuir recursos en tu infraestructura según las necesidades del cliente por el pago de una cuota mensual o anual sin necesidad de comprar los productos de manera física.

1.1.2 La escalabilidad

La escalabilidad puede definirse como la habilidad a través de la cuál un sistema se adapta a un crecimiento constante de ordenes sin afectar su calidad, fluidez y tiempos de respuesta, sin perjuicio de poder adoptar nuevos componentes técnicos o tecnológicos que le ayuden cumplir y soportar una mayor y creciente demanda en sus operaciones.

En el cómputo en la nube, la escalabilidad se diferencia dependiendo de la tecnología o servicio que se preste ya sea en el de Infraestructura, *Software* o Plataforma como servicio, tecnologías que abajo se describirán de manera general. Cabe destacar que la escalabilidad tiene la propiedad de atender a la demanda y necesidades de los usuarios ya que se tanto se pueden sumar recursos, como de disminuirlos cuando el usuario no necesite más de ellos.

En el nivel de la tecnología identificada como Infraestructura como Servicio (*IaaS*), la escalabilidad se materializa en la facilidad y rapidez que se tenga para poder multiplicar los sistemas en función de las necesidades de los usuarios. Por

[8] Stuart J. Johnston; Microsoft Completes Softricity Buyout, disponible en *https://redmondmag.com/articles/2006/07/20/microsoft-completes-softricity-buyout.aspx,* última fecha de consulta 13 de enero de 2020.

poner un ejemplo: toda empresa tecnológica , a medida que va creciendo, necesitará de ampliar la capacidad de su sistema informático para poder satisfacer la demanda de sus usuarios actuales como a los usuarios futuros.

En el nivel del Plataforma como Servicio (*PaaS*) y *Software* como Servicio (*SaaS*), la escalabilidad se encontrará a cargo del proveedor del servicio de *Cloud*, formando parte en éstos, el conjunto de servicios y soluciones ofrecidas por la empresa, sin que el usuario final tenga una intervención directa en los mismos.

Por último, como en la tecnología IaaS, en la SaaS la escalabilidad también se representa con la posibilidad que existe para de aumentar el número de usuarios que pueden acceder a la aplicación (aumentar el número de licencias de *software*) que a diferencia con el *software* físico es una gestión que se puede realizar de manera remota con gran facilidad y rapidez.

Como conclusión, la importancia de la escalabilidad es que brinda a los usuarios una capacidad, casi ilimitada, de los recursos contratados por los usuarios del servicio, pudiendo así adaptarse a las necesidades actuales, futuras y si fuera el caso, de cancelar servicios o aplicaciones que deje de necesitar.

Finalmente y para ilustrar lo anteriormente mencionado, daré el ejemplo teórico de cómo es que funciona el servicio de cómputo en la nube en el comercio electrónico de las PYMES: cuando uno de estos tipos de negocio tienen una demanda mayor de productos (tal y como lo son las empresas de venta de juguetes el 30 de abril (día del niño) y meses de diciembre y enero por Navidad y Reyes Magos) necesitan de una capacidad mayor de servidores, así como de espacio de almacenamiento y velocidad de procesadores mayor para gestionar y procesar pedidos, que aquella tecnología que necesitan el resto del año.

Por lo anterior sería ilógico que una PYME de juguetes (como la mencionada en mi ejemplo anterior) contrate un servicio de amplias dimensiones para los doce meses, siendo que ésta solamente lo necesitará en determinadas épocas del año. Por lo tanto, la empresa solamente contratará (dependiendo de las necesidades que le fueran demandadas) un tipo de servicio distinto para las necesidades que tuviere.

1.1.3 Tecnologías y/o servicios

En el cómputo en la nube como lo mencionamos anteriormente, se emplean tres tipologías de tecnologías y/o servicios distintos denominados: *Software* como Servicio (*SaaS*), Infraestructura como servicio (*IaaS*) y Plataforma como Servicio (*PaaS*), los cuales se describen de la siguiente manera:

1.1.3.1 Software como servicio

Software as a Service, que en castellano traducido literalmente como *Software* como Servicio, es el modelo de servicio que lleva a cabo el despliegue de un programa de *software* y a través del cual, un proveedor licencia una aplicación para que los clientes puedan usarla como si fuera un servicio bajo demanda, denominación también dada al SaaS (*software* bajo demanda).

En el cómputo en la nube, los proveedores de *software* alojan la aplicación en sus servidores y el usuario accede a ella vía remota a través de un dispositivo con acceso a Internet. Cabe destacar que el beneficio del SaaS es que no se necesita instalar una aplicación en un solo equipo, por lo que cuando necesita acceder a la misma podrá hacerlo desde cualquier otro dispositivo.

Ejemplos de proveedores de este servicio son: Microsoft, Google Apps, Salesforce, Zoho, Basecamp y en España Litebi, AparasW, CETEL, MetoCUBE y ASPGems.

1.1.3.2 Infraestructura como servicio

La Infraestructura como Servicio es el modelo de distribución de infraestructura o *hardware*, a través de la virtualización mediante el cual, un cliente solicita el alquiler de la infraestructura de equipos de cómputo que se encuentran en los servidores del proveedor, a través de una plataforma de virtualización que ofrece máquinas virtuales con un diseño específico y a solicitud del cliente, por lo que en vez de adquirir completamente el *hardware*, los clientes compran todos estos recursos a un proveedor de servicios externo.

La diferencia que existe entre el *hosting* o alojamiento virtual es que el suministro de estos recursos y servicios se hace de manera integral a través de Internet.

El ejemplo más destacado actualmente es: Amazon Web Services denominado Elastic Compute *Cloud* o *EC2*, Microsoft Azure, GoGrid, Nimbus, RackSpace y Arsys.

1.1.3.3 Plataforma como servicio

Este servicio de PaaS es considerado el conjunto de plataformas compuestas por uno o varios servidores de aplicaciones y una base de datos que ofrece la posibilidad de desarrollar aplicaciones en distintos lenguajes de programación. Por lo tanto, el servicio PaaS suele identificarse como una evolución del SaaS debido a que es un modelo en el que se ofrece todo lo necesario para realizar la construcción y puesta en marcha de aplicaciones y servicios web.

Otra característica importante es que no hay descarga de *software* que instalar en los equipos de los desarrolladores ya que a pesar de que el PasS ofrece múltiples servicios, todos se encuentran a través de la web.

Los ejemplos más representativos de estos servicios son: Google App Engine, Amazon Web Services, Salesforce, SimpleDB y SQS.

1.1.4 Brechas de seguridad

Como todo servicio electrónico, dentro de los servicios de cómputo en la nube existen riesgos que pueden generarse en caso de ocurrir una brecha de seguridad de la información de los contenidos creados o almacenados a través de servicios de *cloud computing*.

Para ejemplificar lo anterior, a continuación, daré tres breves ejemplos de cómo es que una brecha de seguridad puede ocurrir en cada una de las tipologías que se describieron en este capítulo y cómo es que los usuarios quedamos regulados frente a ellas:

1.1.4.1 Google Drive – software como servicio

Tomando el caso que indiqué en la introducción de este trabajo, imaginemos que contamos ya con nuestra cuenta en Google y necesitamos almacenar nuestros archivos de trabajo y personales en su aplicación de Google Drive. Para ello, seleccionaremos todos aquellos archivos que se encuentren en nuestro disco duro físico y los subiremos a la nube de este proveedor de, entre otros servicios, cómputo en la nube a fin de almacenarlos ahí y poder contar con ellos en el momento que así lo requiramos.

Pues bien, lo anterior es una solución práctica y conveniente ya que dejamos a manos de un tercero el resguardo de nuestra información, pero ¿qué implicaciones se ocasionarían en caso de ocurrir una brecha de seguridad que deje expuestos nuestros archivos a cualquier tercero? Según las Condiciones de Servicio de Google[9], las únicas garantías que ofrece son: (a) ofrecer sus servicios con un nivel de competencia y diligencia razonable; (b) no revisar, ni compartir los archivos o datos personales almacenados con nadie[10], excepto lo establecido en la Política de Privacidad de Google[11], y (c) aquellas establecidas en la legislación aplicable. Además de estos compromisos, no obligaciones, Google no ofrece ninguna otra garantía en relación con los servicios que presta.

Ahora bien, en la Política de Privacidad de Google se establece que trabajará de manera constante para la protección de la información y responder ante casos de fraude y abuso, riesgos de seguridad y problemas técnicos que puedan dañar a Google, sus usuarios o el público en general; como tal, Google no indica qué es lo que realizará de manera legal en caso de haber una vulneración de seguridad, sin embargo, ¿esto quiere decir que estaremos desprotegidos en caso de existir una brecha de seguridad?, la respuesta es no. A pesar de que las Condiciones de

[9] Condiciones del Servicio de Google, disponibles en *https://policies.google.com/terms?hl=es-419* (vigente a partir del 31 de marzo de 2020), última fecha de consulta 13 de febrero de 2020.
[10] Condiciones del Servicio Adicionales de Google Drive, disponibles en: *https://www.google.com/drive/terms-of-service/?hl=es_419* (vigente a partir del 31 de marzo de 2020), última fecha de consulta 13 de abril de 2020.
[11] Política de Privacidad de Google, disponible en *https://policies.google.com/privacy?hl=es-419* (vigente a partir del 31 de marzo de 2020), última fecha de consulta 13 de abril de 2020.

Servicio de Google parecen ser muy amplias, estas establecen que la responsabilidad de la plataforma se obligará conforme a lo establecido en la legislación aplicable, lo cual quiere decir que, Google tendrá que responder exclusivamente en los tribunales federales o estatales del Condado de Santa Clara, California, EE.UU., y en la medida en que la ley local aplicable impida que ciertas disputas se resuelvan en un tribunal de California, el usuario podrá presentar esas disputas en los tribunales locales. Del mismo modo, si la ley local aplicable impide que el tribunal local aplique la ley de California para resolver estas disputas, estas disputas se regirán por las leyes locales aplicables en el país, estado u otro lugar de residencia del usuario.

Desde una perspectiva legal, ¿es esto válido?, la respuesta es sí, la autonomía de la voluntad es la principal fuerza rectora de los contratos y, a pesar de que un usuario pueda argumentar de que Google no permitió negociar el contrato de la prestación de sus servicios con él, Google válida y legalmente podría indicar que el usuario voluntariamente accedió someterse a la jurisdicción y leyes de California al momento de escoger a Google y no a otro prestador de servicios.

Conforme lo anterior, ¿estamos como usuarios desprotegidos al someternos a una jurisdicción y leyes extranjeras?, a mi parecer, no del todo ya que la legislación de California, en específico la Ley de California de Privacidad del Consumidor (*California Consumer Privacy Act* o *CCPA*) es de las más estrictas a nivel mundial en materia de protección de datos personales, ahora bien, en aquellas cuestiones que por ley no le fuesen aplicables a un usuario mexicano, éste podría la aplicabilidad de la ley mexicana e intervención de la autoridad reguladora en materia de protección de datos para México, es decir, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (*INAI*), desafortunadamente, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares solamente exige que ante una vulneración de seguridad que afecte de forma *significativa* los derechos morales o patrimoniales de la persona, el responsable[12] del tratamiento de datos deberá informarlo de manera

[12] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010, Artículo *3o. "Para los efectos de esta Ley, se entenderá por:*

inmediata al titular; por tanto no exige que haya una notificación de ello a la autoridad[13].

1.1.4.2 Microsoft Azure – infraestructura como servicio

Siguiendo los mismos pasos que en el ejemplo principal de este trabajo para crear una cuenta en un servicio electrónico, hacemos lo pertinente para obtener el servicio de *hardware* como servicio de Microsoft Azure. Para ello, llevamos a cabo la contratación de *hardware* personalizado para nuestra PYME y escogemos de manera virtual una CPU, memoria, almacenamiento y velocidad de red ajustado a nuestras necesidades y a partir de ahí ejecutar las aplicaciones empresariales necesarias para nuestro negocio que demanden ciertas características de *hardware*, sin contar con él físicamente.

El ejemplo que puede ocurrir en materia de brechas de seguridad es que un tercero no autorizado, tenga acceso a la infraestructura contratada por nosotros y a partir de ahí, monitorear la información que fluye a través del *hardware* contratado. En caso de ocurrir una vulneración que tenga injerencia en materia de protección de datos, los Términos y Condiciones para este servicio datan de junio de 2015[14], y refieren a la Declaración Privacidad de Microsoft[15]. En ninguno de estos dos documentos se indica algún aspecto relativo a la jurisdicción o competencia de los tribunales en caso de haber un conflicto entre las partes, sin embargo, al momento de crear una cuenta, los usuarios deben aceptar el Contrato de Prestación de

---

XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales."

[13] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010, Artículo *20o "Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos."*

[14] *Microsoft Terms of Use,* disponibles en: *https://www.microsoft.com/en-us/legal/intellectualproperty/copyright/default.aspx* (última actualización el 24 de junio de 2015), última fecha de consulta 13 de abril de 2020.

[15] Declaración de privacidad de Microsoft. Disponible en *https://privacy.microsoft.com/es-mx/privacystatement* (última actualización en mayo de 2020), última fecha de consulta 13 de abril de 2020.

Servicios de Microsoft[16] en el que se establece que ante cualquier conflicto las partes se someten a la jurisdicción y competencia de los tribunales estatales o federales de Kings County, Washington.

De la misma manera que como sucedería con Google, en caso de haber un conflicto entre el prestador de servicios y el usuario, tendrían que resolverlo en los tribunales de Estados Unidos y, dado que nuestra legislación en materia de protección de datos no exige que la autoridad sea notificada en caso de acontecer una brecha de seguridad, un usuario mexicano, tendría que pelear ante tribunales mexicanos atraer el juicio a México argumentando que el servicio es prestado en este país, que Microsoft cuenta con oficinas en México y con una identidad fiscal que lo hacen contribuyente en este país, a fin de tratar de convencer a las cortes en el estado de Washington que son las autoridades o tribunales mexicanos los competentes de resolver una controversia entre ellas, cuestión que en lo personal veo complicado dado que, como lo comenté en el ejemplo del caso de Google, los usuarios se sometieron voluntariamente a resolver conflictos de acuerdo a lo establecido en los términos de uso del prestador de servicio y en caso de que no hubieran querido que esto rigiera así, pudieron haber buscado un prestador de servicios locales y no a Microsoft.

1.1.4.3 Salesforce – plataforma como servicio

Salesforce se define como una solución de gestión de relaciones con clientes que une empresas y clientes a través de una plataforma de gestión de relaciones (comúnmente conocida como *CRM*) que brinda a todos los departamentos de una compañía soluciones de marketing, ventas, comercio y otros servicios. Salesforce aloja la información de sus bases de datos en Internet (nube), lo que representa una practicidad para sus clientes pues éstos pueden acceder y actualizar su información en cualquier momento y en cualquier lugar en el que se encuentren.

[16] *Microsoft Services Agreement*, disponibles en: *https://www.microsoft.com/en-us/servicesagreement/default.aspx* (publicados el 1 de julio de 2019 y vigentes a partir del 30 de agosto de 2019), última fecha de consulta 13 de abril de 2020.

En una plataforma PaaS, como lo es Salesforce el principal problema reside en que, al basarse en el uso de recursos compartidos, terceros no autorizados durante una violación de datos podrían obtener accesos y aprovechar esta información para hacer modificaciones en la configuración del sistema de gestión de clientes y, además de obtener los datos e información confidencial de cada uno de ellos, acceder al manejo de cuentas de gestión que se utilizan a través de esta plataforma.

Los términos y condiciones de Salesforce[17] de igual manera establecen la jurisdicción y competencia de los tribunales localizados en San Francisco, California. De igual manera que en los casos de Google y Microsoft, nos encontramos frente al sometimiento voluntario de los usuarios a una jurisdicción extranjera y al problema que he mencionado en cuanto a que nuestra legislación no exige que exista una notificación en caso de existir una vulneración de seguridad de datos.

1.1.5 Conclusiones

Al haber conocido cómo se realiza la prestación de servicios de cómputo en la nube a través de sus diferentes tipologías (*i.e.*, *SaaS*, *IaaS* y *PaaS*) y haber dado un panorama general de las principales posturas que se encuentran a favor y en contra de este negocio, considero que, el cómputo en la nube es un servicio que facilita la gestión, administración y vida diaria de las personas y empresas que recurren a sus servicios y que, si bien es cierto que existe una dependencia y confianza hacia un tercero para que almacene nuestra información, también es cierto que este tercero, a pesar de someter a sus usuarios a sus términos y condiciones, también existen leyes estrictas que tienen, de alguna manera, la forma de establecer un límite a lo que éstas empresas realicen con nuestra información y a responder en caso de ocurrir una vulneración de seguridad de datos.

Parecería que los usuarios mexicanos nos encontramos desprotegidos al contratar un servicio con un proveedor extranjero al someternos a las leyes del país

[17] *Salesforce – Terms of Service*, disponibles en: *https://www.salesforce.com/company/legal/sfdc-website-terms-of-service/,* última fecha de consulta 13 de abril de 2020.

que más le convenga a éste, sin embargo, las leyes que regulan estos servicios en el extranjero son estrictas y tienen como fin proteger la información que confían los usuarios a estas plataformas de vulneraciones de seguridad. Efectivamente, lo más conveniente sería que nuestra propia ley fuera quien nos protegiera en caso de sufrir una vulneración en materia de seguridad de la información, pero también habría que considerar que, las empresas que prestan servicios a través de la nube, lo hacen a través de Internet y se encuentran en un lugar establecido y no les sería escalable que, por cada usuario que contratase sus servicios tuvieran que negociar un contrato en específico con cada uno de ellos y menos aún, someterse a la jurisdicción de cada uno de ellos.

Capítulo 2
Regulación

Capítulo 2. Regulación

En el presente capítulo se revisarán cuáles son las partes que conforman la relación en la prestación del servicio de cómputo en la nube; cómo la prestación del servicio varía en plataformas afines pero distintas como lo es el *grid computing*, así como revisar cuál es el rol que juegan dentro de la relación que se establece entre los prestadores de servicios y los usuarios, con el objeto de determinar responsabilidades y obligaciones de conformidad con la normativa aplicable.

De igual forma se analizarán las principales implicaciones en materia de propiedad intelectual y seguridad de la información para finalizar con un amplio análisis en materia de protección de datos personales que de la pauta para que, con base en él, se proponga el formato de modelo de política interna que podrán adoptar los prestadores de servicios de cómputo en la nube y cumplir con él, sus obligaciones de seguridad de la información y protección de datos personales de conformidad con la normativa aplicable.

2.1. Prestador de servicios

El prestador del servicio de cómputo en la nube es aquella persona física o moral que proporciona un servicio de la sociedad de la información. Relativo a lo anterior, tal prestador del servicio podrá serlo cualquier persona física o entidad que, en teoría, cuente con la infraestructura necesaria para brindar el servicio de cómputo en la nube a terceros, y que posea los recursos y experiencia necesaria para poder brindar del servicio.

En conjunto con lo anterior, deberá entenderse que el servicio de cómputo en la nube es un servicio de intermediación a través del cual se facilita la prestación o utilización de otros servicios de las TIC, entendiéndose por servicio de intermediación el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros.

Desde un punto de vista académico considero que los prestadores de servicios de cómputo en la nube pueden ser clasificados atendiendo al lugar en donde tengan su sede o establecimiento de servidores de la siguiente manera:

a) Prestadores de servicios establecidos dentro del país en el que prestan sus servicios;
b) Prestadores de servicios establecidos en el extranjero, pero con presencia en el país en el que prestan sus servicios y,
c) Prestadores de servicios establecidos en el extranjero sin presencia en el país en el que prestan sus servicios.

En la práctica algunas empresas trasnacionales que necesitan de una gran capacidad y seguridad para sus datos han llegado incluso a hacer una división de su entidad de manera que establecen una sociedad de manera interna siendo ellos mismos sus propios prestadores de servicios, teniendo por tanto una empresa de cómputo en la nube interna que provee de los mismos servicios que una externa con la única particularidad de que los servidores y red, son de la misma empresa.

Esto obviamente es impensable de realizarse por las PYMES, pues hay una barrera y un abismo económico muy grande que hace que el establecimiento y mantenimiento de los servidores sea significativamente alto en comparación con lo que implicaría un costo de contratación mensual con una empresa ya establecida, tal como lo es Amazon, (quién fue uno de los primeros proveedores de servicios de cómputo en la nube) y que empezó dando servicio con el 10% de su *data centers* e infraestructura en red para el público en general. Lo anterior casó una difusión a cada día mayor entre pequeños grupos, quienes fueron demandando más rapidez y servicios, abriéndose definitivamente en 2002 lo que hoy se conoce como Amazon *Web Services.*

2.1.1 Usuario final

Para efectos de este trabajo definiremos al usuario o consumidor final de la siguiente manera cualquier persona física e incluso jurídica, que contrata con un proveedor

de servicios de cómputo en la nube un servicio IaaS, SaaS o PaaS, a cambio de un precio que variará según las condiciones tecnológicas que necesarias que sean solicitadas por el usuario.

En principio, al parecer esta es la parte que menor obligación podría tener más que la de pagar un precio por recibir el servicio, sin embargo, en materia de protección de datos no es así ya que, como se analizará posteriormente, el contratante de un servicio de cómputo en la nube deberá de cerciorarse que el proveedor del servicio cuenta con las medidas técnicas, físicas y administrativas que la normativa en materia de privacidad y protección de datos exige. Asimismo, el usuario o cliente, deberá de implementar políticas internas y procesos de protección de datos personales con el fin de que en caso de presentarse una eventualidad en que la información puesta en encargo del prestador de servicios se vea vulnerada. En el apartado relativo a protección de datos personales, describiré estas obligaciones y como propósito final de este trabajo de titulación, propondré el formato de una política interna que podrán adoptar las empresas de cloud computing para cumplir con sus obligaciones legales.

2.1.2 Revendedor

Tal y como en los servicios de telefonía y otros servicios de tecnologías de la información, cabe la posibilidad que empresas presten el servicio de cómputo en la nube a través de la reventa del servicio que originalmente provee un tercero o empresa que en su origen es la principal proveedora del servicio.

Estas entidades contratan servidores para ofrecer servicios IaaS, SaaS o PaaS a otras empresas, al objeto de ofrecer dichos servicios a sus clientes, teniendo la responsabilidad de responder directamente frente a ellos. Conforme a lo anterior, la reventa de los servicios de comunicaciones electrónicas implica la actuación del revendedor como cliente mayorista respecto a un prestador de servicios principal y como suministrador minorista respecto a un tercero, siendo responsable de la

prestación del servicio ante el mismo y de aspectos conexos como facturación, entre otros[18].

El revendedor de servicios de cómputo en la nube contrataría en su propio nombre y presentaría a sus potenciales clientes el servicio como propio, ofreciendo sus propias condiciones y precios[19]. En el caso del cómputo en la nube debe destacarse que los servicios de transmisión de datos, tales como el IaaS, SaaS y PaaS, no exigen al prestador del servicio requisito alguno o título habilitante en materia de telecomunicaciones dado que este servicio no es considerado por la Ley Federal de Telecomunicaciones y Radiodifusión como servicio público de telecomunicaciones[20].

2.2 Cómputo en la nube y grid computing

Como lo mencioné al principio de este trabajo, el cómputo en la nube se deriva de dos tipos de servicio que fueron el *Utility Computing* y el *Grid Computing*, que es la figura más afín a lo que hoy se conoce como cómputo en la nube.

Debido a su similitud e importancia es que he decidido dedicar un capítulo de esta tesis a analizar algunas de las similitudes y diferencias entre los dos servicios,

---

[18] Resolución del Consejo del Mercado de las Telecomunicaciones (ahora Comisión Nacional de los Mercados y la Competencia), Resolución RO 2007/1208*: Consulta planteada por la entidad TELEMO COMUNICACIONES, S.L. relativa a la realización de determinadas actividades*, disponible en https://www.cnmc.es/expedientes/ro-20071208, última fecha de consulta 13 de junio de 2020.

[19] *Idem*

[20] Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación,* 14 de julio de 2014. Última reforma publicada el 24 de enero de 2020.

Artículo 2º Las telecomunicaciones y la radiodifusión son servicios públicos de interés general.

(…)

Artículo 3º Para los efectos de esta Ley se entenderá por:

(…)

LXV. Servicios públicos de telecomunicaciones y radiodifusión: Servicios de interés general que prestan los concesionarios al público en general con fines comerciales, públicos o sociales de conformidad con lo dispuesto en la presente Ley y la Ley Federal de Competencia Económica;

(…)

LXVIII. Telecomunicaciones: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión;

a efecto de no confundir los mismos y saber las implicaciones que podría atraer el contratar uno u otro.

2.2.1 Cómputo en la nube

Con el servicio de cómputo en la nube las empresas podrán tener capacidades (de *software*, datos, plataformas, entre otros) de manera masiva y escalable, así como una contratación de servicios de forma instantánea sin tener que invertir en infraestructuras, formación de personal o en licencias de *software*.

El cómputo en la nube se centra en satisfacer las necesidades tanto de la PYME como de la gran empresa. Por un lado, en las PYMES ayudan a que estas puedan gozar de tener la infraestructura de un data-center complejo fuera de la compañía y que todos los costos que esto implica sean de alguna manera, asumidos por el prestador del servicio a través del pago de su cuota mensual.

Por otra parte, beneficia a las grandes empresas que tienen un flujo altísimo de datos, para que estas cuenten con un servicio e infraestructura de grandes capacidades, así como de data centres de gran nivel y calidad. En ambos casos, los usuarios siempre tendrán un servicio a la medida de sus necesidades.

2.2.2 Grid computing

En resumidas cuentas, la historia del *Grid Computing*[21] comenzó el día en que surgió la idea de que al igual que cuando los primeros ordenadores comienzan a tener acceso a Internet, estos pudieran unir fuerzas para poder realizar las tareas en conjunto que eran imposible de realizarse con un sólo ordenador convencional.

[21] Javier Palazón, Grid, *Computing: potencia compartida, Emplear ciclos de procesamiento no utilizados por los ordenadores para realizar tareas similares a las de las supercomputadoras. Ésta es la base de 'Grid Computing*, *https://www.microsoft.com/spain/enterprise/perspectivas/numero_9/research.mspx*, última fecha de consulta 13 de marzo de 2020.

La manera de lograrlo era unir la potencia inutilizada de cada uno de todos los ordenadores que se encontraran conectados para que de alguna manera se creará una supercomputadora (mediante el conjunto de varias) como aquellas que poseen organizaciones gubernamentales, universidades o grandes multinacionales.

> *Esta tecnología fue denominada como Grid Computing (computación distribuida) y se basa en el aprovechamiento de los ciclos de procesamiento no utilizados por los millones de ordenadores conectados a la Red. De esta forma se consigue que puedan resolver tareas que son demasiado intensivas para ser resueltas por una única máquina.*

Para contribuir a este esfuerzo global, una aplicación cliente detecta cuando un PC está inactivo y en ese instante activa los procesos de cálculo que permiten poner en marcha las unidades de trabajo (working units). El sistema emplea una arquitectura cliente/servidor, de tal forma que el servidor administra las unidades de trabajo y gestiona el control de las tareas que dichas unidades tienen asignadas en cada momento[22]*.*

2.2.3 Afinidad y distinción entre los términos

La primera similitud que encontramos entre el cómputo en la nube y el Grid Computing es la escalabilidad, de la cual hablé al principio de este trabajo. En éstas dos tecnologías, la escalabilidad se logra a través del equilibrio del tiempo en que carga una aplicación, la cual se separa en varios sistemas operativos que se encuentran unidos a través de la Web. Los ordenadores y la capacidad de la banda ancha se asignan y se revocan según lo exija la demanda. Asimismo, la capacidad de almacenamiento del sistema sube y baja dependiendo del número de usuarios, casos, y la cantidad de datos que son transferidos en un tiempo determinado.

[22] *Ídem.*

Por otra parte, en ambas tecnologías computacionales tienen como característica que pueden desempeñar múltiples tareas, lo cual habilita a que sus usuarios realicen diferentes trabajos, accediendo a una o varias aplicaciones; de esta manera, ambas herramientas informáticas pueden compartir recursos reduciendo costos y sin encontrarse limitadas una determinada capacidad.

La diferencia entre el cómputo en la nube y el Grid Computing es que ésta última distribuye la tecnología informática de varios ordenadores conectados entre sí para una realizar una tarea específica, y el cómputo en la nube se utiliza para realizar un rango completo de actividades.

2.3 Propiedad Intelectual

Los asuntos relacionados con la propiedad intelectual y el cómputo en la nube se encuentran extremadamente vinculados con la jurisdicción correspondiente y la dificultad que representa determinar esta, así como los tribunales competentes y regulación aplicable, así como cuál será la ley (ya sea local, federal, tratado internacional, entre otros) que regirá el acuerdo entre las partes[23].

Esto es complicado debido a que toda la información que se transmita haciendo uso de los servicios de cómputo en la nube podrá estar en servidores localizados en cualquier otra parte del mundo (de la misma forma, la transmisión de estos datos dependerá del lugar en donde se encuentre el/los usuarios). Por ejemplo: la información de una empresa multinacional podrá estar al mismo tiempo siendo transmitida de un servidor localizado en las islas Fiji, a las sedes de la empresa pudiendo estar localizadas en Dubái, Hong Kong, Nueva York, Sao Paolo, Madrid y en la Ciudad de México al mismo tiempo.

Cuestiones que pueden llegar a surgir con este tipo de ejemplos (que no distan en nada de lo que sucede día a día en la realidad), puede ser como aquella

[23] “Capitol Records, Inc. v. llc, Exp. No. 07-9931 (S.D.N.Y. Agos 13, 2009)”, Casetext, disponible en: https://casetext.com/case/capitol-records-inc-v-mp3tunes-3 última fecha de consulta 13 de julio de 2020.

en que el usuario final de los servicios se encuentre frente a conflictos con las leyes relacionadas a la privacidad y sobre todo con los derechos de propiedad intelectual al momento de ser transmitida información y archivos que no cuenten con los permisos o las licencias requeridas por los creadores de las obras. A mi parecer estos asuntos y posibles conflictos deberán ser previstos y regulados por los proveedores de servicios y el usuario, en los contratos de prestación de servicios que se al momento de contratarse los mismos para dar una solución, sin embargo, esto suele no ser así. Ejemplo de ello es la resolución del Tribunal de Justicia de la Unión Europea (*UE*) de 24 de noviembre de 2011, en el asunto C-70/10, Scarlet Extended SA (*Scarlet*) contra la *Société belge des auteurs, compositeurs et éditeurs* (*SABAM*) al imponérsele a Scarlet (un proveedor de servicios de Internet) a instalar un sistema de filtrado de comunicaciones electrónicas generadas por el uso de *software* de intercambio de archivos (”*peer to peer*”).

2.3.1 El intercambio de archivos en el cómputo en la nube

Un tema interesante de tratar y que actualmente no se encuentra totalmente regulado de pies a cabeza, es la cuestión de compartir archivos a través de la nube, los cuales podrán o no tener los permisos o licencias correspondientes del autor que capacite a los usuarios o propietarios usarlos o compartirlos de una u otra manera.

En el siguiente artículo publicado por Andy Ramos[24] en el que a su vez se refiere a la publicación del libro del Profesor Sánchez Aristi titulado “*El Intercambio de obras protegidas a través de las Plataformas Peer-to-Peer*” se hace mención a lo que implica el compartir obras protegidas, y aunque el tema aquí no son las plataformas Peer-to-Peer (en adelante, *P2P*), el cómputo en la nube y sus servicios se ven íntimamente relacionados con el tema al momento en que el usuario hace

[24] Ramos Gil De La Haza, Andy, *Hacia la Abogacía 2.0 y Digitalización del Derecho*, disponible en *http://www.andyramos.com,* última fecha de consulta 13 de enero de 2020.

de una pequeña porción de su nube privada para que ésta se convierta en una nube pública y genere enlaces para compartir o enviar un archivo o cúmulo de archivos que se encuentren dentro de ésta, a un número determinado o indeterminado de usuarios. Como lo indica el abogado especializado en propiedad intelectual, Andy Ramos en comento a lo descrito por el profesor Sanchez Aristi, los usuarios que comparten estos enlaces a obras protegidas por derechos de autor se encuentran ante un ilícito civil dado que no existe un ánimo de lucro, siendo esta una actividad que infringe los derechos de titulares de obras y prestaciones protegidas, tanto por la acción de la puesta a disposición como por aquella que existe en la descarga de obras ofrecidas por terceros sin la autorización de aquellos que son legítimos propietarios.

Aquí habrá que advertir, pero sobre todo, se deberá hacer consientes a los usuarios que hagan uso de plataformas en el cómputo en la nube para compartir archivos, que se estaría cometiendo un ilícito penado conforme a lo establecido en la Ley Federal de Derecho de Autor si se estuvieran compartiendo archivos protegidos por derechos de autor y pudiendo (según el caso) llegar a infringir una norma de derecho penal siempre que el intercambio de los mismos se hiciera con ánimo de lucro, por ser ésta conducta, una infracción de los derechos de los titulares de obras al actualizarse el supuesto exigido por mencionada ley que es la puesta a disposición de una obra, sin la autorización de los legítimos propietarios de ésta.

2.3.2 Posibles soluciones planteadas

Como lo he comentado, el cómputo en la nube nos provee de un sin número de herramientas que dan la posibilidad a los usuarios de acceder a sus archivos de manera fácil y en cualquier lugar donde se encuentren. Asimismo, dentro de la nube uno puede compartir archivos de carpetas a un sinnúmero de personas a través de la red. Tales archivos pueden o no estar sometidos a una licencia o a derechos de autor y la forma de detectarlos suele ser muy complicada entre los millones de archivos que se comparten a través de Internet.

El sector audiovisual, sobre todo, es la industria más afectada por el intercambio de archivos en la red y actualmente han sido planteadas algunas soluciones por expertos en el tema, en específico el autor del libro "*El Intercambio de obras protegidas a través de las Plataformas Peer-to-Peer*", del profesor Rafael Sánchez Aristi propone que[25]:

"1. Establecer un nuevo límite (similar al de copia privada, cita, entre otros), lo cual descarta rotundamente porque ello supondría estar fuera de la Directiva e incluso de los tratados internacionales. Citó el caso de Italia, que recientemente ha aprobado un nuevo límite para la publicación de obras protegidas en Internet, aunque de forma "degradada" y para fines didácticos, lo cual dista mucho de la legalización de la puesta a disposición masiva y gratuita de obras protegidas.

2. Establecer un canon/compensación, también rechazada por su imposibilidad de llevarla a la práctica; sería muy complicado establecer un mecanismo de recaudación, y sobre todo determinar a qué dispositivos, mecanismos, entre otros se debería imponer dicho canon.

3. Respetar los derechos exclusivos de los titulares de las obras, licenciando la utilización de sus obras y prestaciones, articulando un mecanismo de recaudación a través del operador de la red P2P o a través del propio usuario."

De acuerdo con lo anterior, estas soluciones vendrían rencausar al lado legal una actividad que comúnmente es realizada sin mesura por los usuarios de este tipo de plataformas de compartición de archivos y que, de alguna manera, ayudaría a que este intercambio de información sea debidamente controlado a fin de respetar los derechos de autor.

[25] Extracto tomado del blog de interiuris en el que se resume la opinión de Sánchez Aristi cuando se habló de las redes P2P y la descarga de archivos que contengan obras protegidas por la propiedad intelectual, disponible en *http://www.interiuris.com/blog/?p=424*, última fecha de consulta 13 de junio de 2020.

2.4 Seguridad

Como toda idea de externalización (dejar en manos de terceros sistemas, aplicaciones o servicios que son vitales para el funcionamiento del negocio), los ahorros de costes se perfilan quizás como la ventaja más evidente[26]. Pero, al mismo tiempo, la seguridad se asoma como el mayor riesgo que hay que encarar. Algo que no es ajeno al modelo de cómputo en la nube.

> Palabras como las anteriores no solamente vienen de expertos en el tema, como es el caso anterior, sino que la mayoría de los usuarios y personas que se encuentran relacionados con este tema se plantean y se encuentran de alguna manera preocupados y desconfiados al dejar en manos de terceros los datos todos aquellos contenidos que puedan ser objeto de almacenamiento y uso a través de un servicio de cómputo en la nube.

Entre los potenciales riesgos de seguridad, actualmente se plantean supuestos y conflictos que aparecerían cuando se vulneran los sistemas de seguridad de la *nube* dejando *desprotegidos* a sus usuarios al ofrecer *oportunidades* inminentes a cibercriminales tales como aquellos que son podrían utilizar este servicio para evadir impuestos, para tener un canal espía secretos industriales, para acceder y robar datos de otros y posiblemente con ellos poder extorsionar a alguien.

Dentro del primer (posible caso), se encuentra que dado a la flexibilidad de ubicación geográfica de servidores con la que se cuenta al poder contratar un servicio de cómputo en la nube, genera que muchos bancos en paraísos fiscales y casinos prefieran escoger un prestador de servicios se encuentre en alguna jurisdicción que los “proteja” o no los regule tanto, agregando a esto que pudiese darse la situación en la que proveedores de servicios tengan sus servidores en

---

[26] IDG Communications, *Cloud Computing, que hay en la nube,* disponible en *http://www.idg.es/pcworldtech/Cloud-computing:-__que-hay-en-la-nube__-/art194631-comunicaciones.htm,* última fecha de consulta 13 de mayo de 2020.

ciudades en la que no se tenga una Ley lo suficientemente protectora de consumidores y usuarios o que en la misma no se tengan suficientes requisitos de privacidad exigidos al proveedor y finalmente que ofrezcan impuestos por debajo de la media y con un alto secreto bancario.

Es menester que los proveedores de servicios de cómputo en la nube se exijan implantar las medidas tecnológicas necesarias para que el usuario final (consumidor) tenga resguardada su información de aquellos terceros que puedan representárseles como potenciales rivales o terceros ajenos a conocer la información, así como de implantar todos aquellos recursos que para poder evitar errores de sistema que puedan producir fuga de información entre usuarios.

2.5 Protección de datos personales

El 5 de julio de 2010 fue publicada en el Diario Oficial de la Federación (*DOF*) la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (*LFPDPPP*); posteriormente, el 21 de diciembre de 2011 fue publicado en el DOF el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (*Reglamento*). Ambos ordenamientos contienen los principales requisitos y obligaciones a los que se encuentran sujetos todos aquellos particulares que llevan a cabo el "tratamiento" de datos personales. Dentro de las innovaciones que tuvo la LFPDPPP, es que fue pionera -en su tiempo- en regular el tratamiento de los datos personales a través del cómputo en la nube.

Antes de profundizar en la regulación del cómputo en la nube y las implicaciones jurídicas que conllevan en el ámbito privado, hablaré un poco de cuáles son los pilares del tratamiento y protección de la información personal que se encuentran regulados en México comenzando con algunas definiciones importantes contenidas tanto en la LFPDPPP como en su Reglamento.

Las definiciones que a continuación menciono se encuentran en los artículos 3 de la LFPDPPP y 2 de su Reglamento, sin embargo, el orden que siguen las mismas no es alfabético ni conforme se establece en la normativa, sino que es un

orden que hago de manera discrecional conforme a lo que en lo personal considero que es aquel con el que el lector de este trabajo de titulación podrá comprender mejor la regulación, sin ser necesario que sea abogado.

2.6 Definiciones

Dato Personal. Es cualquier información concerniente a una persona física, identificada o identificable, tales como nombre, teléfono, domicilio e incluso fotografía. Al respecto, es importante hacer hincapié en que el término “identificable” (según el Reglamento) conlleva a considerar a toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información, no pudiendo considerarse como “persona física identificable” cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas.

Datos Personales Sensibles. Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Responsable. Es aquella persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. En otras palabras, cualquier profesionista o empresa que realice el tratamiento de datos personales se considera por nuestra LFPDPPP como “responsable”.

Encargado. Es la persona física o moral que lleve a cabo datos personales por cuenta del responsable; de conformidad con el Reglamento de la LFPDPPP, el encargado es la persona física o moral, pública o

privada, ajena a la organización del responsable, que sola o 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.

Esta definición es muy importante para el tema objeto de este trabajo de titulación ya que, por regla general, las empresas que prestan el servicio de cómputo en la nube, a pesar de tener bajo su resguardo la información que suben los que contratan sus servicios (*i.e.*, bases de datos que contienen información personal), deben de ser considerados como encargados ya que actúan delimitados por la prestación del servicio y no pueden apropiarse de la información ni de los datos personales que le son proporcionados o subidos a la nube.

Dentro de las obligaciones con las que cuenta el encargado, el Reglamento de la LFPDPPP establece las siguientes:

a) tratar únicamente los datos personales conforme a las instrucciones del responsable;
b) abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
c) implementar las medidas de seguridad conforme a la LFPDPPP, el Reglamento y las demás disposiciones aplicables;
d) guardar confidencialidad respecto de los datos personales tratados;
e) suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no

exista una previsión legal que exija la conservación de los datos personales, y

f) abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia. La comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado.

Remisión. La compartición de datos personales entre un responsable y sus encargados es considerada una remisión de datos. A diferencia de una transferencia, las remisiones son hechas a prestadores de servicios del responsable y éstas tienen como objeto que el responsable pueda cumplir con el fin del tratamiento que realiza de la información personal. Las remisiones nacionales e internacionales de datos personales no se tienen que informarse al titular, ni es necesario contar con consentimiento expreso para dicha remisión, sin embargo, será necesario que estas se describan en el aviso de privacidad.

Ahora bien, el responsable del tratamiento de datos personales tiene como primer paso dentro de sus obligaciones legales, informar a los titulares cómo es que llevará a cabo el tratamiento de estos a través de un aviso de privacidad.

Al respecto, la LFPDPPP define en la fracción I de su artículo 3 al “aviso de privacidad” como el “documento físico, electrónico o en cualquier otro formato

generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales". Conforme al artículo 15 y demás relacionados de la LFPDP, las personas físicas o morales responsables del tratamiento de datos personales están obligados a informar a los titulares los fines para los que se llevará a cabo el tratamiento (obtención, uso, divulgación o almacenamiento) de sus datos personales, a través de un aviso de privacidad.

Respecto al aviso de privacidad, el 17 de enero de 2013, la Secretaría de Economía publicó en el DOF los Lineamientos del Aviso de Privacidad[27] (Lineamientos) que delimitan el contenido y alcance del aviso de privacidad.

Los Lineamientos delimitan el contenido y alcance del aviso de privacidad a efecto de dar a conocer las condiciones en las que se llevará a cabo el tratamiento de datos personales.

Algunos aspectos de los Lineamientos que se deben tomar en cuenta al momento de crear un aviso de privacidad son:

Formato y Lenguaje. El aviso de privacidad deberá ser eficiente, práctico, sencillo, claro, redactado en idioma español y con una estructura que facilite su entendimiento. No deberá incluir (i) frases inexactas o ambiguas o vagas; (ii) textos que induzcan a elegir una opción en específico; y (iii) en caso de contener casillas, éstas no deberán de estar previamente marcadas. De igual forma, la redacción del aviso de privacidad deberá tomar en cuenta el perfil de los titulares de los datos personales a quienes va dirigido.

Difusión. El aviso de privacidad puede darse a conocer a través de formato físico, electrónico, óptico, sonoro, visual o mediante cualquier otra tecnología que permita su comunicación y conocimiento eficaz, por parte del titular de los datos.

[27] Lineamientos del Aviso de Privacidad, *Diario Oficial de la Federación,* 17 de enero de 2013.

Personas Físicas con actividad Empresarial. No se considerarán datos personales y, por ende, no será necesario dar a conocer aviso de privacidad a personas físicas cuando actúen como comerciantes o profesionistas, a personas físicas con actividades empresariales o a personas físicas que estén prestando sus servicios para una persona moral y la estén representando. Estos datos personales son: (i) nombre y apellidos; (ii) funciones o puestos desempeñados; (iii) datos laborales como domicilio físico, correo electrónico, y teléfono de contacto.

Modalidades. El aviso de privacidad puede ser integral, simplificado o corto; el uso de las distintas modalidades dependerá de si la obtención de datos personales se lleva a cabo personalmente del titular, de manera directa, o si el espacio para obtener los datos es limitado, de conformidad con los siguientes requisitos:

Integral. A utilizarse cuando el titular da conocer los datos personales personalmente y debe incluir, como mínimo:

a) nombre y domicilio del responsable. Este requisito es el mínimo indispensable por incluir en los avisos de privacidad para aquellos casos en que los datos no se recaban personalmente; el resto del aviso de privacidad se puede dará conocer a los titulares a través de otros mecanismos, como publicaciones en Internet, entre otros;
b) datos personales específicos que se tratarán;
c) listado exhaustivo de los datos personales sensibles que se tratarán;
d) finalidades del tratamiento de datos de forma determinada, especificando aquellas finalidades que no son estrictamente necesarias para la existencia y cumplimiento de la relación entre el responsable y el titular, así como las relacionadas

con fines de mercadotecnia o publicidad. Al redactar esta sección, se deberán evitar frases como “entre otras”, “fines análogos” o “por ejemplo”;

e) mecanismos para que el titular pueda manifestar su negativa para las finalidades no necesarias;

f) transferencias de datos, incluyendo el receptor y finalidades que la justifiquen. No es necesario especificar transmisiones de datos a agentes o encargados, es decir, terceros que llevan a cabo el tratamiento a nombre del responsable, pues éstas se consideran “remisiones” de datos.

   Al respecto, es importante destacar que los responsables podrán transferir datos a terceros en México o en el Extranjero, siempre y cuando dicha transferencia haya sido notificada y consentida en el aviso de privacidad (y por tanto exista consentimiento por parte del titular) y la persona que los recibe los utilice únicamente para los fines señalados en el aviso.

   Excepcionalmente, no será necesario obtener el consentimiento del titular para transferir datos personales en los siguientes casos: (i) transmisiones a encargados que actúan por cuenta del responsable, a filiales o subsidiarias; (ii) transferencias previstas en ley; (iii) transferencias necesarias para cumplir un contrato; (iv) transferencias con motivo de interés público:

   i. cláusula específica para que el titular exprese si acepta o no las transferencias de datos;
   ii. medios y procedimientos para ejercer derechos de acceso, rectificación, cancelación u oposición;
   iii. procedimientos y mecanismos para revocar consentimiento;

iv. opciones y medios para limitar el uso o divulgación de datos;
v. información, en su caso, sobre uso de medios tecnológicos que permitan recabar datos de forma automática, y
vi. procedimientos para que el responsable comunique a los titulares cambios en el aviso de privacidad. En caso de que se modifique la identidad del responsable, recabar datos adicionales, modificar las finalidades de tratamiento o las condiciones de transferencias de datos, será necesario poner a disposición de los titulares un nuevo aviso de privacidad.

Simplificado. Puede utilizarse cuando los datos personales se obtienen directa o indirectamente del titular –pero no personalmente-, por medios electrónicos, ópticos, sonoros, visual o a través de cualquier otra tecnología. En este caso, el aviso de privacidad deberá incluir el nombre y domicilio completo del responsable, al igual que las finalidades para las que serán tratados los datos personales, en los mismos términos que el aviso integral.

Adicionalmente, el aviso simplificado deberá especificar los mecanismos por los que el titular puede conocer el aviso de privacidad integral (por ejemplo, internet).

Corto. Puede utilizarse cuando los datos personales se obtengan por medios impresos, si el espacio para la obtención de los datos sea mínimo y limitado. En ese caso será necesario que se incluya la misma información que en los avisos simplificados:

a) nombre y domicilio completo del responsable;

b) las finalidades para las que serán tratados los datos personales, en los mismos términos que el aviso integral, y
c) los mecanismos por los que el titular puede conocer el aviso de privacidad integral.

Una de las finalidades del aviso de privacidad es que el titular pueda otorgar el consentimiento para el tratamiento de sus datos personales. La formalidad del consentimiento dependerá la naturaleza de dato personal.

En general, el consentimiento puede ser tácito, es decir por el simple hecho de que el titular no rechace el aviso de privacidad se entenderá consentido; sin embargo, en el caso de que los datos sean financieros o patrimoniales se requerirá un consentimiento expreso, mientras que para los datos sensibles, es decir, aquellos que afecta la esfera más íntima de su titular, se requiere consentimiento expreso y por escrito del titular (mediante firma autógrafa o a través de un medio de autenticación tecnológico que pueda asegurar la identidad del titular).

Una obligación derivada de la LFPDPPP que vale la pena recordar al momento de diseñar los avisos de privacidad, es la que tienen todos los responsables de para establecer medidas de seguridad que permitan proteger los datos personales contra daños, pérdidas, acceso o tratamiento no autorizado.

Aun cuando parecería que el cumplimiento de esta obligación requiere una inversión considerable por parte de los responsables, en muchas ocasiones puede que sólo sea necesario implementar políticas de confidencialidad con empleados y aquellos usuarios que tengan acceso a los datos personales, para evitar divulgación no autorizado. Las medidas específicas requeridas en cada caso dependerán del tipo de tratamiento que se lleve a cabo y la cantidad o naturaleza de datos que se recaben.

En cualquier caso, se requiere que el responsable tenga los medios necesarios para detectar una violación a las medidas de seguridad y poder avisar a los titulares de los datos involucrados.

Dado que ningún sistema de seguridad o de protección es completamente seguro, en caso de que ocurra alguna vulneración a los datos personales, el artículo 58 de la LFPDPPP establece que, al momento de llevar a cabo la evaluación e imposición de la multa correspondiente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (*INAI*) podrá tomar en consideración el cumplimiento de las recomendaciones que el mismo haya propuesto.

Para tal efecto, el INAI cuenta con las Recomendaciones en materia de seguridad de datos personales, a efecto de que los responsables y encargados del tratamiento de datos personales tengan un marco de referencia respecto a las acciones que se consideran las mínimas necesarias para la seguridad de los datos personales.

Es debido destacar que la adopción de las recomendaciones que aquí se describen es de carácter voluntario y el seguimiento de estas no exime a los responsables y encargados del tratamiento de datos personales de su responsabilidad en caso de alguna vulneración a sus bases de datos.

2.7 Sistema de gestión de seguridad de datos personales

El INAI ha pronunciado como recomendación general, adoptar un Sistema de Gestión de Seguridad de Datos Personales (*SGSDP*), el cual el mismo Instituto ha definido como un "*sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia*"[28].

[28] Recomendaciones en materia de seguridad de datos personales. Diario Oficial de la Federación, 30 de octubre de 2013.

Ahora bien, dicho SGSDP se integra por cuatro ciclos con distintas fases y actividades denominados como Planificar-Hacer-Verificar-Actuar (*PHVA*); con base en mi experiencia profesional, he notado que el común denominador es que las empresas realicen de manera ordinaria estas actividades por lo menos una vez al año, sin embargo, esto podrá variar dependiendo la cantidad y tipo de datos personales que cada empresa maneje; por ejemplo, no es lo mismo una empresa que trate datos de proveedores de servicios de infraestructura que aquella que maneje una base de datos de la nómina de empleados o aquella otra que cuente con la gestión de información de pacientes de un laboratorio. Por lo anterior, creo que el escenario más adecuado, para encontrarse en constante cumplimiento y revisión es realizar una auditoría interna cada seis meses, ya que considero que este plazo es suficiente para detectar fallos, implementarlos y evaluar su debido cumplimiento de acuerdo con las mejoras planteadas.

Para referencia y entendimiento del lector, a continuación, describo cuáles son cada una de las etapas que integran un correcto Sistema de Gestión de Seguridad de Datos Personales de conformidad con las Recomendaciones en materia de seguridad de datos personales publicadas por el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos (hoy INAI) en el DOF el 30 de octubre de 2013 (Recomendaciones):

2.7.1 Planificar

El presente ciclo tendrá como actividades las de identificar políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener la implantación de medidas de seguridad efectivas para el tratamiento de datos personales, y para que los mismos se encuentren protegidos ante daño, perdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los mismos.

Dentro de este ciclo, dentro de las Recomendaciones, el INAI propone seguir los siguientes pasos para su implantación:

1) Determinar el alcance y objetivos del tratamiento de datos personales conforme al modelo de negocio de la organización o empresa.
2) Crear una política de gestión de datos personales, a manera de compromiso formal y documentado para el tratamiento adecuado de los datos personales.
3) Determinar y asignar funciones y obligaciones de quienes traten datos personales dentro de la empresa u organización.
4) Levantar un inventario de los datos personales que se recaben y efectivamente se traten, así como el flujo que tienen los mismos.
5) Realizar un análisis de riesgo de los datos personales con los que se cuenten.
6) Identificar y evaluar las medidas de seguridad con las que actualmente se cuente en la empresa, contra aquellas que sería conveniente tener; así como realizar el análisis de brecha que existe para su adopción.

Los 6 pasos anteriores deberán tener el fin de cumplir con la legislación de protección de datos y obtener resultados acordes con las políticas y objetivos generales de la organización.

2.7.2 Hacer

Implementar dentro de la empresa u organización el plan de acción mencionado en el punto 1) del apartado anterior.

Dentro de este ciclo el INAI propone:

1. Implementar las medidas de seguridad aplicables a los datos personales y contar con indicadores de medición para tal efecto.

2.7.3 Verificar

Evaluar y medir los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada (el correcto tratamiento de los datos personales).

Dentro de este ciclo el INAI propone lo siguiente:

2. Llevar a cabo labores de revisión y auditoria, conforme a lo establecido en la legislación de protección de datos personales, la revisión de los factores de riesgo, posibles vulneraciones, política, objetivos y experiencia práctica del SGSDP, e informar los resultados a la Alta Dirección[29] de la empresa para su revisión.

2.7.4 Actuar

Adoptar medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras fuentes de información relevantes, para lograr la mejora continua.

3. Lograr una mejora continua del SGSDP basada en adoptar medidas correctivas y preventivas en función de los resultados obtenidos por parte del personal de Alta Dirección de la empresa, así como llevar a cabo programas de capacitación y mejora para su implantación.

Dado que lo puntos anteriores son un ciclo, estos deben de tener una constante verificación, revisión y adaptación a efecto de combatir en todo momento las posibles vulnerabilidades a las que se encuentran expuestos los datos personales, así como cumplir con las novedades legislativas en materia de protección de datos que puedan surgir en el futuro.

2.8 Designación de un departamento de Protección de Datos

Los responsables deberán designar a una persona o departamento de datos personales para dar trámite a las solicitudes de los titulares, respecto del ejercicio

[29] La sección 2.1. de las Recomendaciones define *"Alta Dirección"* como toda persona con poder legal de toma de decisión en las políticas de la organización. Por ejemplo: la junta directiva, ejecutivos y trabajadores experimentados, la persona a cargo del departamento de datos personales, los socios de la organización, el dueño de una empresa unipersonal o quien encabeza la organización.

de sus derechos de acceso, rectificación, cancelación u oposición de datos personales.

La LFPDPPP no exige una formalidad específica para esto, sino que simplemente se requiere que exista una persona de contacto para atender las solicitudes de los titulares. Una vez más, será necesario analizar el tipo de datos personales que se trata junto con la cantidad de datos almacenados para tomar la decisión sobre la vía idónea para dar cumplimiento a esta decisión.

Para asegurar el cumplimiento de las obligaciones a cargo de todos aquellos responsables de datos personales, es conveniente que se haga un análisis particular sobre (i) el tipo y cantidad de datos que se recaban; (ii) las actividades de la empresa o responsable de datos, en relación con los mismos; (iii) si ya se cuenta con algún tipo de medida o protocolo de seguridad de la información.

2.9 El cómputo en la nube en la LFPDPPP

El artículo 52 del Reglamento de la LFPDPPP es el único artículo dentro de la normativa en materia de protección de datos que regula el tratamiento de datos personales a través del cómputo en la nube. Al respecto, el mencionado artículo establece que cuando la información personal se trate a través de servicios, aplicaciones e infraestructura en el denominado cómputo en la nube en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla con ciertas obligaciones específicas que garanticen los principios y deberes establecidos en la LFPDPPP; transparenten el tratamiento que realizarán terceros subcontratados por el prestador de servicios; y se guarde la propiedad y confidencialidad de la información personal que se trate a través de estos sistemas. De igual manera el artículo mencionado, establece los límites y mecanismos de seguridad que deberán observarse en la relación jurídica que se establezca con el prestador de servicios.

A manera de referencia, a continuación, transcribo el artículo mencionado para efecto de que, posteriormente, se realice un análisis práctico de sus elementos:

> Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:
>
> I. Cumpla, al menos, con lo siguiente:
>
> a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;
>
> b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
>
> c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y
>
> d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y
>
> II. Cuente con mecanismos, al menos, para:
>
> a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
>
> b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;

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

e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

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

Habiendo establecido cuáles son los requisitos mínimos que deberá cumplir el un proveedor de servicios de cómputo en la nube, para los efectos prácticos de este trabajo, conforme lo establece el artículo 52 del Reglamento de la LFPDPPP, el proveedor de servicios de cloud computing deberá tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y el Reglamento.

2.10 Conclusiones

Como pudimos ver en este capítulo, existen distintas partes que conforman la relación en la prestación del servicio de cómputo en la nube: el prestador de servicios en sí que cuenta con el mayor cúmulo de obligaciones conforme a la legislación y que, de acuerdo con la LFPDPPP, podrán existir casos en los que se considere como el principal responsable del tratamiento de la información y, por tanto, deba implementar políticas internas para asegurar la protección de la información que le es proporcionada por sus titulares; las personas contratantes que, como titulares, confían en los términos y condiciones que los prestadores de servicios y que cuentan con la protección de la normativa en cuanto a la protección de la información que conceden a los prestadores de servicios y, finalmente los revendedores de los servicios quienes, van a responder de manera individual frente a sus clientes pero repetir en contra del prestador de servicio principal en caso de ocurrir una contingencia o vulneración como puede ocurrir en materia de propiedad intelectual, seguridad de la información y protección de datos personales.

Con base en lo descrito en el presente capítulo y habiendo fijado las obligaciones con las cuales cuentan los responsables del tratamiento de información personal, a continuación propongo un Modelo de Política para la Protección de Datos Personales que podrá ser utilizado por una empresa que preste servicios de cómputo en la nube a efecto de cumplir el mínimo de sus obligaciones legales y actualizar de tiempo en tiempo en caso de haber modificaciones sustanciales a la regulación o cambios en la tecnología.

Capítulo 3
Propuesta de modelo de política interna de protección de datos personales para empresas de cloud computing

Capítulo 3. Propuesta de modelo de política interna

Como fue descrito en el capítulo anterior, de conformidad con la LFPDPPP y en aras de iniciar con el cumplimiento de la normativa en materia de protección de datos, como primer paso, es necesario a cabo la realización de diversos avisos de privacidad para cualquier compañía a fin regular todas y cada una de las relaciones jurídicas que sostiene con titulares de datos personales, como lo son sus empleados o aquellos candidatos a ocupar un puesto vacante dentro de la empresa, clientes y proveedores. En el caso de las empresas que presten servicios de cómputo en la nube, el aviso de privacidad sobre el cual se deberá tener más cuidado en su implementación, es aquel que regule la relación con sus clientes.

3.1 Contar con un aviso de privacidad

La obligación de que los responsables del tratamiento de los datos personales tengan un aviso de privacidad que deba ser informado a los titulares de los datos personales que trate, se encuentra contemplada en los artículos 15, 16 y 17 de la LFPDPPP, mismos que a continuación se citan por su relevancia:

> Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.
>
> Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:
>
> I. La identidad y domicilio del responsable que los recaba;
>
> II. Las finalidades del tratamiento de datos;
>
> III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;

IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

V. En su caso, las transferencias de datos que se efectúen, y

VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Como puede desprenderse del artículo 16 de la LFPDPPP antes citado, será necesario que el aviso de privacidad cuente con diversos elementos mínimos. Dichos elementos han sido descritos en a lo largo del Reglamento de la LFPDPPP y los Lineamientos al Aviso de Privacidad.

3.2 Departamento de datos personales

La LFPDPPP establece en su artículo 30, la obligación de los responsables del tratamiento de datos personales, la designación de una persona o departamento responsable que dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos y que fomentará la protección de datos personales al interior de la organización.

> "*Artículo 30.- Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo, fomentará la protección de datos personales al interior de la organización.*"

Conforme a lo anterior, la LFPDPPP es relativamente vaga por su amplitud dado que en la misma no se establecen criterios, métodos o mecanismos que deban seguir las empresas u organizaciones para la designación de esta persona o departamento (menos aun considerando cuando hablamos de empresas de cómputo en la nube al ser escasamente reguladas en el Reglamento de la LFPDPPP en un solo artículo); en este aspecto, la LFPDPPP permite actuar libremente al particular, lo cual muchas veces puede causar incertidumbre dentro de las organizaciones y dudas en diversas cuestiones en las cuales los responsables del tratamiento de datos personales tienen responsabilidades y funciones relacionadas al tratamiento de datos.

Por lo anterior, a efecto de que cualquier empresa, así como aquellas dedicadas a la prestación de servicios de cómputo en la nube, realicen una adecuada designación de la persona o integración el departamento encargado de la protección de datos personales, a continuación, se realizarán una serie de apreciaciones con base en las recomendaciones para la designación de la persona

o departamento de datos personales, emitidas por el INAI en agosto de 2016[30] y mi experiencia profesional.

3.2.1 Designación

En lo que se refiere a la designación de esta persona o departamento de datos personales, de conformidad con el artículo 30 de la LFPDPPP antes citado, se desprende que los particulares que se encuentren en posesión de datos personales podrán optar por la designación ya sea de: i) una persona o, ii) un departamento de datos personales.

Ahora bien, como se comentó en párrafos anteriores, la LFPDPPP al dejar actuar libremente al particular, no exige ninguna de las opciones mencionadas como tal; es por lo anterior que las empresas de manera interna deberán decidir qué es lo más conveniente conforme a su organización, sin que esto limite su cambio en un futuro. Es decir, una empresa de cómputo en la nube podrá designar a una persona que tenga las responsabilidades establecidas en el artículo 30 de la LFPDPPP y en un futuro, atendiendo al comportamiento que se tenga en la empresa respecto al tratamiento de datos personales, podrá integrar un departamento de datos personales como tal. Lo más conveniente para empresas de tecnología, como lo es una prestadora de servicios de cómputo en la nube, atendiendo a la cantidad de datos personales que puedan tratar, es designar a un Oficial de Protección de Datos (*Chief Privacy Officer*) que sea ayudado por un equipo de profesionales tanto técnicos como jurídicos a revisar el debido cumplimiento de la normativa técnico-jurídica en materia de protección de datos.

En mi opinión, sea cual fuere la decisión que tome una empresa para la designación de una persona o de un departamento de protección de datos personales, deberá evaluarse si es indispensable la contratación de personal adicional especializado o que integre un nuevo departamento de datos personales

[30] Recomendaciones para la Designación de la Persona o Departamento de Datos Personales disponibles en: *http://inicio.ifai.org.mx/DocumentosdeInteres/privacidadresponsable.pdf*, última fecha de consulta 13 de marzo de 2020.

dentro de la empresa. Al respecto, será necesario que, atendiendo a los retos que implica el tratamiento de información dentro de una empresa de cómputo en la nube, es recomendable, aunque casi obligatorio, someter a capacitación al personal en general y con base en ello, advertir lo que se refiere a la protección de datos personales dentro de una empresa de tecnología.

En este sentido, sugiero que diversos departamentos dentro de empresa colaboren a la par a fin de llevar a cabo diversas funciones relacionadas con el tratamiento de datos personales tales como que exista una coordinación entre ellos y, en caso de ocurrir una contingencia, puedan colaborar en dar seguimiento a las obligaciones naturales de un responsable del tratamiento de datos personales, tales y como lo es el trámite a solicitudes para el ejercicio de derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (*Derechos ARCO*) presentadas por parte de los clientes. No está por demás mencionar que dentro de la empresa deberá llevarse a cabo la difusión de la importancia de los datos y su adecuado tratamiento dentro de ella, para que en su conjunto y en general, pueda cumplir con las funciones que por sí exige la LFPDPPP.

Respecto a lo anterior y de conformidad con lo dispuesto por la LFPDPPP, a efecto de que empresas prestadoras de servicios de cómputo en la nube puedan tomar una decisión para la designación de una persona o departamento de datos personales, el INAI sugiere que el Oficial de Protección de Datos sea designado tomando en cuenta lo siguiente:

- El tipo y cantidad de datos personales que se tratan;
- La naturaleza e intensidad del tratamiento;
- Número potencial de solicitudes de titulares de datos personales que podrá recibir; y
- El valor que tengan los datos personales para la organización.

3.2.2 Manera de designación o nombramiento

Pasando a la manera en que habrá que realizarse la designación o nombramiento, en especial, el mismo debe realizarse de manera tal que pueda dejarse constancia su celebración, tal y como lo es a través de: actas notariales, consejos de administración u otros documentos o procesos similares. Con base en lo anterior, sugiero realizar el nombramiento por escrito ya sea a través de un documento formal o una asamblea ordinaria en la que se trate al mismo nombramiento como uno de los asuntos a tratar en el Orden del Día respectivo.

3.2.3 Obligaciones

En lo que se refiere a las obligaciones de la persona o departamento de datos personales, deben distinguirse los dos sujetos obligados que surgen de conformidad con lo dispuesto por el artículo 30 de la LFPDPPP, ya que por una parte y de conformidad con el artículo mencionado, surgen obligaciones tanto para: i) la empresa prestadora de servicios de cómputo en la nube, como para ii) el Oficial de Protección de Datos y el departamento que lo asista.

Por su parte, la empresa será responsable de designar a la persona o departamento quien, por otra parte, tendrá las siguientes funciones:

- Dar trámite a las solicitudes de los titulares que se realicen, para el ejercicio de los derechos ARCO, y
- Fomentar la protección de datos personales al interior.

En cuanto a la primera función de "*Dar trámite a las solicitudes de los titulares que se realicen, para el ejercicio de los derechos ARCO*", mi sugerencia es establecer métodos sencillos para que los titulares de datos personales puedan ponerse en contacto con la empresa y ejercer sus derechos ARCO.

Sobre este punto, considero adecuada la puesta a disposición de diversos medios de contacto tales como la creación de un correo electrónico especial a través

del cual la empresa prestadora de servicios de *cloud computing* reciba todas aquellas comunicaciones que se refieran al tratamiento de datos personales y el cual sea claramente identificable por los titulares.

Asimismo, y en un afán de dar mayores posibilidades de contacto a los titulares de datos personales, sugiero informar a los mismos (a través del Aviso de Privacidad) que pueden establecer contacto también a través de la dirección postal de la empresa, siendo conveniente mencionar que, las comunicaciones deberán ser dirigidas al Oficial de Protección de Datos o departamento de datos personales que le asista a efecto de llevar un control sobre las mismas.

Ahora bien, de manera interna, cualquier empresa (sin importar que ésta sea prestadora de servicios de cómputo en la nube) deberá crear los mecanismos para dar trámite y seguimiento de conformidad a los plazos establecidos en la LFPDPPP, de aquellos ejercicios de derechos ARCO solicitados por los titulares, así como establecer una coordinación y cooperación entre las personas y departamentos dentro de la empresa que tengan relación con el tratamiento de datos personales.

Respecto a lo anterior y de manera complementaria, el INAI sugiere ciertas funciones a efecto de dar un cumplimiento efectivo a la LFPDPPP, a saber:

- Establecer y administrar procedimientos para la recepción, tramitación, seguimiento y atención oportuna de las solicitudes para el ejercicio de los derechos ARCO, así como para la atención de quejas o solicitudes presentadas por los titulares relacionados con las políticas y/o prácticas de protección de datos personales desarrolladas por la organización, y
- Monitorear los avances o cambios legislativos en materia de privacidad y protección de datos personales que pudieran impactar en los ejes rectores y acciones desarrolladas en este tema al interior de la organización, haciendo las adecuaciones necesarias.

Pasando a la segunda función denominada por el artículo 30 de la LFPDPPP como "*Fomentar la protección de datos personales al interior de la organización*",

de manera general la persona o departamento designado, deberá realizar la implementación políticas de difusión dentro de la empresa relativas a la protección de datos, a fin de dar a conocer a todo el personal el cuidado que debe tenerse respecto al manejo y tratamiento de datos personales y los mecanismos que de manera interna se han implementado.

Al respecto y en seguimiento al objetivo último que tiene el presente trabajo de titulación que es proponer un formato de política interna de protección de datos personales para empresas de *cloud computing*, el INAI sugiere las siguientes 12 acciones complementarias:

1. Diseñar y ejecutar una política y/o prácticas de protección de datos personales al interior de la organización, o bien, adecuar y mejorar las prácticas ya existentes en el marco de la LFPDPPP;
2. Alinear esta política y/o prácticas -incluyendo sus objetivos, acciones estratégicas, líneas de acción, asignación de roles y responsabilidades generales y específicas y un procedimiento y plazos de implementación- a los procesos internos de la organización que demanden o aprovechen información personal;
3. Desarrollar un mecanismo para evaluar la eficacia y eficiencia de esta política y/o prácticas;
4. Monitorear y evaluar los procesos internos de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales, a fin de asegurar que la información sea protegida, tratada conforme a los principios de la LFPDPPP y respetada;
5. Colaborar y coordinar acciones con otras áreas de la organización como la legal, de tecnologías, sistemas, seguridad de la información, mercadotecnia, atención al cliente, recursos humanos, entre otras, a efecto de asegurar el debido cumplimiento de la política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo;

6. Asegurar que la política y/o prácticas de protección de datos personales cumplan con la LFPDPPP y demás normatividad aplicable;
7. Difundir y comunicar la política y/o prácticas de protección de datos personales implementadas al interior de la organización, así como capacitar a todo el personal sobre las mismas;
8. Fomentar una cultura de protección de datos personales orientada a elevar el nivel de concienciación del personal y terceros involucrados, como encargados, en el tratamiento de datos personales;
9. Monitorear el cumplimiento de la política y/o prácticas de protección de datos personales de las sociedades subsidiarias o afiliadas bajo el control de común de la organización o cualquier sociedad del mismo grupo del responsable que opere y le sean aplicables estas prácticas;
10. Identificar e implementar mejores prácticas relacionadas con la protección de datos personales;
11. Promover la adopción de esquemas de autorregulación; y
12. Ser el representante de la organización en materia de protección de datos personales ante otros actores.

Como propiamente lo dispone el INAI, la aplicación de las medidas complementarias antes mencionadas dependerá de las necesidades que tenga el particular y podrán ser aplicables a través de distintos departamentos dentro de la empresa, pudiéndose aplicar medidas adicionales que tengan como fin el fomento de la protección de datos personales dentro de la empresa.

3.2.4 Publicidad

Es debido que el titular de datos personales cuente con la mayor información posible en cuanto a la persona o departamento responsable de los datos personales dentro de una empresa, ya sea para efectos de contactar con éste para dudas, quejas o sugerencias o, en su caso, ejercer sus derechos ARCO.

Para tal efecto, en lo que respecta a empresas tecnológicas como lo son aquellos prestadores de servicios de *cloud computing*, es necesario que en su página de Internet (dentro de su aviso de privacidad) hagan referencia a la identidad de la persona o el nombre del departamento de protección de datos, así como de las distintas maneras disponibles para contactar con el mismo.

3.2.5 Perfil

El INAI sugiere que la persona que se encuentre a cargo de las funciones de protección de datos personales dentro de una empresa cuente con: i) experiencia en materia de protección de datos personales; ii) tenga una jerarquía o posición indicada dentro de la organización; iii) cuente con los recursos materiales, técnicos y humanos suficientes para la implementación de sus funciones en lo que respecta a la protección de datos personales dentro de la empresa; iv) tenga conocimiento de la protección de datos personales; v) disponga de visión y liderazgo; y vi) cuente con habilidades de organización y comunicación[31].

Considero que lo anterior se enfoca a que efectivamente la persona que se encuentre en funciones, conforme al artículo 30 de la LFPDPPP, esté capacitada para el tratamiento de los datos personales en la empresa. En lo personal, considero que dentro de una empresa prestadora de servicios de cómputo en la nube, los principales pilares para integrar el departamento encargado de cumplir con la obligaciones en materia de seguridad, calidad o buenas prácticas, deberán ser las personas del departamento de sistemas en conjunto con el departamento jurídico, ya que ambas tienen los conocimientos técnico-legales necesarios y las bases para que son necesarias para determinar el correcto tratamiento y cumplimiento de las disposiciones de la LFPDPPP.

Es importante también, como lo menciona el INAI, que la persona tenga una jerarquía o poder de mando dentro de la organización a efecto de implementar

[31] Recomendaciones en materia de seguridad de datos personales. Diario Oficial de la Federación, 30 de octubre de 2013.

políticas de protección de datos que sean respetadas y acatadas a todos los niveles de la empresa, así como contar con los recursos que le permitan dar cumplimiento a su cargo y se genere una conciencia del buen tratamiento de datos personales dentro de la empresa.

Por otra parte, y dentro de las obligaciones que deberá de cumplir el responsable del tratamiento de los datos personales, se encuentra la obligación de establecer e implementar aquellas medidas técnicas, físicas y administrativas para salvaguardar los datos personales de daños, perdidas, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los mismos.

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

El artículo 19 de la LFPDPPP antes mencionado, ha sido complementado con las "*Recomendaciones en materia de seguridad de datos personales*", publicadas por el INAI en el Diario Oficial de la Federación el 30 de octubre de 2013, mismas que se describen en el siguiente apartado.

3.2.6 Medidas de seguridad

Como se describió en el Capítulo Segundo de este trabajo, el INAI ha propuesto las "*Recomendaciones en materia de seguridad de datos personales*", a efecto de que los responsables y encargados del tratamiento de datos personales tengan un

marco de referencia respecto a las acciones que se consideran las mínimas necesarias para la seguridad de los datos personales.

Es debido destacar que la adopción de estas recomendaciones, son de carácter voluntario y el seguimiento de estas no exime a los responsables y encargados del tratamiento de datos personales de su responsabilidad en caso de que suceda alguna vulneración a sus bases de datos.

Habiendo mencionado lo anterior, y con base en lo descrito en el presente trabajo, la propuesta de modelo de política interna de protección de datos personales para empresas de cloud computing que propongo a continuación tiene como propósito orientar a los responsables del tratamiento de datos personales en el cumplimiento de su obligación para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado dentro de un proveedor de servicios de cómputo en la nube persona o departamento de datos personales, que establece el artículo 52 del Reglamento de la LFPDPPP.

Al respecto, cabe destacar que este modelo de política interna, será complementaria y robustecedora de los términos y condiciones que posea una plataforma prestadora de servicios de cómputo en la nube, así como de los contratos que celebre con sus clientes, (ya sea personas físicas o morales); al respecto, su adopción influirá de manera benéfica en cuanto a que, como seguimiento a una política corporativa, podrá hacerse o no referencia a ella dentro de los mencionados términos y condiciones o contratos, sin embargo, en caso de existir una contingencia, como lo es una vulneración de seguridad, su correcta implementación, seguimiento y actualización , podrá servir para demostrar ante el INAI que la empresa, como prestador de un servicio de tecnología, sigue aquellas reglas dispuestas por el Instituto en materia de autorregulación y su correcta adopción servirá como evidencia para mitigar o atenuar las sanciones que, en su caso, la autoridad determine que son aplicables en caso de presentarse un evento de vulneración de datos personales.

Conclusiones

Conclusiones

Habiendo tratado este tema desde un aspecto técnico-jurídico cada uno puede estar a favor o en contra de esta nueva tecnología; en lo personal, considero que actualmente ésta es una herramienta más que se pone a disposición de la sociedad de la información para facilitar la vida diaria de las empresas y las personas, resolviendo inconvenientes tan simples como la falta de almacenamiento y la disponibilidad de recursos electrónicos que, sin ésta tecnología, sería muchas veces incosteable mantener.

Conforme a ello considero que el cómputo en la nube tiene grandes ventajas como la disponibilidad del servicio y/o aplicación web las 24/7, y que por tanto los usuarios no estarán obligados a solucionar problemas de mantenimiento, soporte e instalación ya que contarán con un prestador de servicios que se encargará de todo, ello, aparte la neutralidad tecnológica será potencializada debido a que se podrá tener acceso a la nube a través de diferentes tecnologías compatibles, tales como: pdas, teléfonos móviles, computadoras portátiles, netbooks, entre otros, con un uso de alguna manera ilimitado de recursos, los cuales podrán ser contratados a través de Internet y en cuestión de segundos.

Pero así como hay beneficios con esta tecnología, también hay desventajas que afectan a este nuevo desarrollo tales como que debido a una catástrofe natural o error humano, no se pueda tener un acceso completo al servicio e incluso aún que no se pueda acceder al servidor(es) en donde se encuentren los datos pudiendo tener inconvenientes graves e incluso perdidas que pueden repercutir de gran manera en el usuario final, así mismo, puede que muchos usuarios se encuentren aún muy desconcertados pues se le enviarán a un tercero datos de carácter personal e incluso documentos privados e íntimos tales como fotos, videos, secretos industriales, datos secretos, o información que ocupe una esfera mucho más privada del individuo, sumándose a esto que delincuentes informáticos ven como un nicho de acción vulnerar la seguridad de los servidores y hacerse con datos

privados para poder comerciar con ellos o pedir recompensas por su liberación, recuperación o no divulgación.

Ahora bien, en cuanto a la protección que actualmente tenemos los usuarios de estos servicios, encontramos términos y condiciones en la prestación que, a pesar de que en un principio pueden parecer no muy ventajosas para nosotros, lo cierto es que éstas se encuentran reguladas por normativa internacional que suele ser exigente y por órganos jurisdiccionales que buscan marcar precedentes en pro de la protección de los usuarios y de la información que éstos dejan en manos de terceros.

Como bien lo analicé y propuse en este trabajo, con el fin de cumplir la normativa en México y generar mayor confianza en el usuario, considero que una compañía de cloud computing puede valerse del formato de política interna a fin de regular dentro de su organización un correcto tratamiento de sus datos personales y a partir de ella ir complementando ésta con buenas prácticas internacionales que, en mi experiencia, empresas sujetas a la legislación mexicana, han comenzado a implementar tales como: (a) controles de acceso a la información; (b) escritorios limpios; (c) digitalización; (d) destrucción y digitalización de información y políticas paperless; (e) sellos de confianza; (f) creación de códigos de ética y de conducta; (g) capacitación de personal; y (h) realización de auditorías y actualizaciones periódicas.

En un mundo globalizado en donde la información se vuelve el activo más importante cualquier organización, es necesario que las empresas que presenten servicios en la nube creen e implementen mecanismos para la protección y correcto tratamiento de la información que procesan día con día. De igual manera, como usuarios de un servicio como lo es este, debemos de exigir que nuestra información se encuentre protegida y que una empresa cuente con los mecanismos necesarios para ello.

Si bien es cierto que será difícil que un usuario exija a los prestadores de servicio conocer las políticas que las empresas prestadores de servicios de cloud

computing demuestren que cuentan con políticas protectoras de su información, lo cierto es que al momento de crear una PYME o trabajar en una empresa, será necesario para efectos de auditorías contar con la certeza de que aquellos proveedores de servicios que se contratan actúan diligentemente en el procesamiento y protección de la información que se les encomienda y la mejor forma de comprobar que lo anterior es correctamente implementado, es contar con una política interna que así lo demuestre.

Bibliografía

ABERASTURI GORRIÑO, Unai, *El derecho a la indemnización en el artículo 19 de la Ley orgánica de Protección de datos de carácter personal*, Revista Aragonesa de Administración Pública, ISSN 1133- 4797, n. 41-42, 2013, p. 173-206. *http://w.aragon.es/estaticos/GobiernoAragon/Organismos/InstitutoAragonesAdministracionPublica/Areas/03_Revista_Aragonesa_Formacion/04%20Unai%20Aberasturi.pdf*

ALAMILLO DOMINGO, I., *El control de localización de los datos e informaciones en el Cloud*, en Martínez Martínez, R. ed., *Derecho y "cloud computing"*

ÁLVAREZ HERNANDO, Javier. *Guía práctica sobre protección de datos: cuestiones y formularios: Protección de datos personales en la sociedad de la información y la vigilancia*.

ÁLVAREZ CIVANTOS, Óscar J, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Albolote, Granada: Comares, 2008

APARICIO SALOM, Javier, *La computación en la nube cambia el paradigma de los negocios*. Dinero 26 de mayo de 2016. Acceso el 17 de enero de 2019. *https://www.dinero.com/edicion-impresa/tecnologia/articulo/la-computacion-en-la-nube-cambia-el-paradigma-de-los- negocios/224009*

APARICIO SALOM, Javier, *Estudio sobre la protección de datos*, Cizur Menor, Navarra, Aranzadi, 2013.

Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Grupo de Trabajo IV (Comercio Electrónico), 55° periodo de sesiones, *Aspectos contractuales de la computación en la nube*, Documento A/CN.9/ WG. IV/WP.142. Nueva York, 24 a 28 de abril de 2017.

Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Grupo de Trabajo IV (Comercio Electrónico), 56° periodo de sesiones, *Aspectos contractuales de la computación en la nube,* Documento A/CN.9/ WG. IV/WP.148. Nueva York, 16 a 20 de abril de 2018.

Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Grupo de Trabajo IV (Comercio Electrónico), 56° periodo de sesiones, *Aspectos contractuales de los servicios de computación en la nube,* Propuesta de los Estados Unidos de América, Documento A/CN.9/WG. IV/WP.151. Nueva York, 16 a 20 de abril de 2018.

BADGER, GRANCE, PATTCORNER, VOAS, *Special Publication* 800-146: *cloud computing Synopsis and Recommendations*, Estados Unidos, *U.S Department of*

Commerce, National Institute of Standards and Technology, 2012. Disponible 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.

CEBALLOS ATIENZA, Rafael, *Protección de datos de carácter personal: técnicas de adaptación y procedimientos*, 1ª ed. Alcalá la Real, Jaén: Formación Alcalá, 2012

DAVARA RODRÍGUEZ, Miguel Ángel. *Evaluación del impacto en la Protección de datos de carácter personal (EIPD),* Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal, ISSN 0210-2161, n. 9, 2014, p. 1041-1047

ENÉRIZ OLAECHEA, Francisco Javier, *La protección de los datos de carácter personal,* Pamplona, Defensor del Pueblo de Navarra, Nafarroako Arartekoa, 2012.

ENISA Agencia Europea de Seguridad, *Seguridad y resistencia en las nubes de la Administración Pública,* ENISA, Acceso el 17 de enero de 2019. *www.enisa.europa.eu/*

GALÁN MUÑOZ, Alfonso. *¿Nuevos riesgos, viejas respuestas?: estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación*, Revista General de Derecho Penal, ISSN-e 1698-1189, n. 19, 2013, *http://www.iustel.com/v2/revistas/default.asp*

GARCÍA DEL POYO, Rafael. *cloud computing: Aspectos jurídicos clave para la contratación de estos servicios*, Revista Española de Relaciones Internacionales, n.° 2, 2012. Acceso el 29 de abril de 2017. *http://reri.difusionjuridica.es/index.php/RERI/article/view/45/43*

GARCÍA SÁNCHEZ, M. *Retos de la computación en nube*. *En Derecho y cloud computing*, ed. por R. Martínez Martínez, Cizur Menor, Navarra: Thomson Reuters - Civitas, 2012.

GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria,* Madrid: Agencia Española de Protección de Datos: Agencia Estatal Boletín Oficial del Estado, 2014

JOYANES, Luis. *Computación en la nube. Notas para una estrategia española en cloud computing*. Revista del Instituto Español de Estudios Estratégicos, n.°0 2012, p.89-112.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Lineamientos del Aviso de Privacidad.

LÓPEZ JIMÉNEZ, David. "*La "computación en la nube" o "cloud computing*" examinada desde el ordenamiento jurídico español". Revista de Derecho de la Universidad Pontificia Católica de Valparaíso, XL 2013, 1er Semestre, 689-709. *https://doi.org/10.4067/s0718-68512013000100021*

MARTÍNEZ MARTÍNEZ, R., *El Derecho y el "cloud computing"*, en Martínez Martínez, R. ed., p. 11.

MARKS, Eric A. *Executive Guide to cloud computing,* New Jersey: Wiley, 2010. *https://doi.org/10.1002/wics.139*

ONTAÑÓN RAMOS, Iván. *Regulación de las TIC, Ley Orgánica de Protección de Datos,* Madrid: Roble, 2014.

ORTEGA GIMÉNEZ, A., *"cloud computing", protección de datos y derecho internacional privado (resolución de controversias y determinación de la ley aplicable)*, en Martínez Martínez, R. ed., Derecho y "cloud computing".

PUYOL MONTERO, Javier. *Algunas consideraciones sobre "cloud computing"*, Madrid: Agencia Española de Protección de Datos; Agencia Estatal Boletín Oficial del Estado, 2013.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

RUBÍ NAVARRETE, J., *El proveedor de Cloud como encargado de tratamiento*, en Martínez Martínez, R. ed., Derecho y "cloud computing"

SMALE, Will. *Cómo Drew Houston y Arash Ferdows triunfaron con Dropbox, una em- presa tecnológica que Steve Jobs quiso destruir*. BBC News. Economía 17 de julio de 2018, Acceso el 21 de enero de 2019. *https://www.bbc.com/mundo/noticias-44847080*

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.

Red de Gobierno Electrónico de América Latina y el Caribe (*Red GEALC*) Organización de los Estados Americanos (*OEA*), Banco Interamericano de Desarrollo (*BID*), Centro de Investigación para el Desarrollo Internacional (*IDRC*). "e-Gobierno en la nube". Boletín e-Gobierno Red GEALC 118, octubre 2016.

VERDAGUER LÓPEZ, Jordi. *Prontuario protección de datos*, 2011. Valencia: CISS, 2011.

ZAPATA, Ricardo. *13,8 millones de venezolanos compraron o vieron una tienda online en 2017*. El Nacional Economía Empresa, 31 de mayo de 2018. Acceso el 21 de enero de 2019. *http://www.el-nacional.com/noticias/empresas/138-millones-venezolanos- compraron-vieron-una-tienda-online-2017_237981*

ANEXO 1
Modelo de política interna de protección de datos personales

Propuesta de índice

Propuesta de Modelo de Política Interna de Protección de Datos Personales para empresas de Cloud Computing

1. Alcance

El presente Manual de Políticas, le es aplicable ***[nombre del Proveedor de Servicios de Cómputo en la Nube]*** (en adelante "**[PSCN]"**); y departamentos o áreas de [PSCN] que captan, procesan o utilizan y transfieren o remiten Datos Personales para la realización de sus funciones tales como: Recursos Humanos, Compras, Ventas, entre otros.

2. Objetivo

Establecer los lineamientos para la protección de Datos Personales y dar cumplimiento a la "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (la "LFPDPPP"), el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás disposiciones aplicables".

3. Definiciones[32]

- **Aviso de Privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del Titular, previo al tratamiento de sus Datos Personales, de conformidad con el artículo 15 de la LFPDPPP mediante el cual se establecen los términos y condiciones que regirán el Tratamiento de los Datos Personales del Titular.

- **Datos Financieros o Patrimoniales:** Este término no se encuentra definido en la LFPDPPP o su Reglamento, sin embargo, conforme al

[32] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010 y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012.

artículo 8 de la LFPDPPP, el Tratamiento se encuentra sujeto al consentimiento expreso del Titular.

- **Datos Personales:** Cualquier información concerniente a una persona física identificada o identificable. Ejemplos de Datos Personales: Nombre, teléfono, domicilio, número de teléfono, huellas dactilares, así como cualquier otro dato que pueda servir para identificar a la persona.

- **Datos Personales Sensibles:** Aquellos Datos Personales que afecten a la esfera más íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos Datos Personales que puedan revelar aspectos como origen racial o étnico, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual o temas de salud.

- **Derechos ARCO:** Es la facultad que otorga la LFPDPPP para que el Titular, como dueño de los Datos Personales, decida a quién proporciona su información, cómo y para qué; estos derechos le permiten al Titular **A**cceder a los Datos Personales que poseemos y a los detalles del tratamiento de los mismos, **R**ectificar en caso de que estén incompletos o sean inexactos, **C**ancelar en caso que considere que no se requieren para alguna de las finalidades señaladas en el Aviso de Privacidad o estén siendo utilizados para finalidades que no hayan sido consentidas y **O**ponerse al tratamiento de sus Datos Personales. Por sus iniciales, son conocidos comúnmente como derechos **ARCO**, son aquellos derechos que toda persona puede ejercer, en relación con el Tratamiento de sus Datos Personales.

- **Encargado:** La persona física o moral que, sola o conjuntamente con otras, trate Datos Personales por cuenta del Responsable. Ejemplo: El Encargado

puede ser una compañía de gestión de nómina contratada por [PSCN] para el manejo de ciertos Datos Personales relacionados con el pago de nóminas.

- **INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Antes "INAI"):** Dentro de las facultades del INAI se encuentra la de fungir como órgano encargado de la protección de los Datos Personales. Como tal, el INAI tiene la autoridad de investigar y vigilar el cumplimiento por parte de los particulares a quienes obliga la LFPDPPP y su Reglamento.

- **LFPDPPP:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- **Listado de Exclusión:** Base de datos en los que se registran de forma gratuita la negativa del Titular al Tratamiento de sus Datos Personales.

- **Reglamento:** Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- **Remisión:** Toda comunicación de Datos Personales entre el Responsable y el Encargado, dentro o fuera del territorio mexicano.

- **Responsable:** Cualesquiera de las compañías que conforman el grupo [PSCN] en México y que traten y decidan sobre el Tratamiento de los Datos Personales recabados.

- **Tercero:** La persona física o moral, nacional o extranjera, distinta del Titular o del Responsable.

- **Titular:** La persona física a quien corresponden los Datos Personales.

- **Transferencia:** Toda comunicación de datos realizada a persona distinta del Responsable o Encargado del Tratamiento.

- **Tratamiento:** la obtención, uso, divulgación o almacenamiento de Datos Personales por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de Datos Personales.

- **UMA.** Unidad de Medida y Actualización. Es referencia económica en pesos para determinar la cuantía del pago de las obligaciones y supuestos previstos en las leyes federales, de las entidades federativas y de la Ciudad de México, así como en las disposiciones jurídicas que emanen de todas las anteriores. Sustituye el uso de Veces Salarios Mínimos que antes se usaba con estos fines.

4. Responsabilidades[33]

Cualquier departamento de [PSCN] que trate Datos Personales deberá:

a) Poner a disposición del Titular el Aviso de Privacidad antes de recabar y/o tratar los Datos Personales por cualquier medio.
b) Informar a los Titulares de los Datos Personales la información que se recaba de ellos y con qué fines, a través del Aviso de Privacidad especifico de [PSCN], que regule la relación jurídica de que se trate (ej. candidatos, empleados, proveedores o clientes).
c) Recabar el Aviso de Privacidad firmado por el Titular y entregarle una copia.
d) Resguardar los Datos Personales que reciba del Titular ya sea de manera verbal, impresa o electrónica.
e) Verificar que el Encargado cumpla con los fines autorizados por [PSCN] y el Titular para el uso de los Datos Personales.
f) Hacer del conocimiento de los Titulares cambios al Aviso de Privacidad.
g) Verificar que aquellos Encargos contratados por [PSCN], sigan y cuenten con las medidas de seguridad necesarias para proteger los Datos Personales que se le remitan.
h) Entregar al Encargado copias del Aviso de Privacidad de [PSCN] para efecto de informarle el tratamiento que deberá realizarse de los Datos Personales que se le remitan.
i) Conservar los Avisos de Privacidad que sean firmados por los Titulares.
j) Verificar el cumplimiento del control de acceso y de información electrónica.
k) Elaborar un inventario de Datos Personales y actualizarlo anualmente.
l) Depurar o eliminar los Datos Personales del Titular cuando corresponda y de forma segura. Los Datos Personales se deben eliminar cuando se hayan agotado los fines de tratamiento establecidos en el Aviso de Privacidad (ej. para el área de Recursos Humanos los Datos Personales se pueden almacenar por tiempo indefinido, en tanto esté justificado, así como cuando

[33] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010 y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012.

una persona sea considerada como posible candidato para desempeñar un cargo en [PSCN], o tratándose de un extrabajador que se considere pueda ser recontratado).

m) Dar cursos de capacitación anualmente al personal de [PSCN] sobre el buen tratamiento de los Datos Personales y de los lineamientos que se deben seguir para su protección.
n) Responder en tiempo a las solicitudes de ejercicio de Derechos ARCO, asimismo dar seguimiento a las solicitudes de revocación de consentimiento o de limitación de uso y divulgación de los Datos Personales.
o) Entregar a todos los empleados de la compañía, por medio impreso o electrónico, la LFPDPPP y el Reglamento.

Cualquier prestador de servicios de [PSCN] (Encargados) al que se le remitan Datos Personales deberán:

a) Realizar el Tratamiento de los Datos Personales de acuerdo con el contrato de prestación de servicios celebrado con [PSCN], sin llevar a cabo uso o tratamiento distinto al previsto en el Aviso de Privacidad de [PSCN].
    - Proporcionar al personal de [PSCN] el acceso a sus bases de datos.
b) Cumplir las medidas de seguridad necesarias para proteger los Datos Personales que sean remitidos por [PSCN]. En este punto es importante tomar en cuenta que es responsabilidad de [PSCN] cerciorarse que el Encargado se ciñe a procedimientos internos necesarios para proteger los Datos Personales que le son remitidos.
c) Responder a las obligaciones propias de un Responsable, cuando destine o utilice los Datos Personales remitidos con una finalidad distinta a la autorizada por [PSCN] o efectúe una Transferencia, incumpliendo las instrucciones de [PSCN].

Dependiendo de los servicios prestados por el Encargado de Tratamiento, éste podrá encontrarse obligado a:

d) Vigilar que los sistemas de seguridad utilizados por [PSCN] para proteger Datos Personales se encuentren operando de forma debida, y en caso de detectar deficiencias, reportarlas de inmediato.

5. Políticas Aplicables

a) Aviso de Privacidad de [PSCN]
b) [Insertar otras políticas internas]

6. Ámbito de aplicación de la LFPDPPP

Los sujetos regulados por la LFPDPPP son los particulares, ya sean personas físicas o morales de carácter privado, que lleven a cabo el Tratamiento de Datos Personales[34], con excepción de:

a) Agencias de Gobierno, Tribunales y el Congreso (la LFPDPPP solo aplica a particulares de carácter privado).
b) Las sociedades de información crediticia en los supuestos de la LFPDPPP para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
c) Las personas que lleven a cabo la recolección y almacenamiento de Datos Personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Las disposiciones del Reglamento (y por tanto las de la LFPDPPP), no son aplicables a información de:

a) Personas morales;
b) Datos Personales que refiera a personas físicas en su calidad de comerciantes y profesionistas, y

[34] Artículo 2 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

c) Personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono fijo y móvil; siempre que esta información sea tratada para fines de representación del empleador o contratista.

7. Clasificación de datos personales[35]

La LFPDPPP clasifica los Datos Personales en tres tipos:

Datos Personales Generales: Cualquier información concerniente a una persona física que no sea un Dato Sensible o Financiero. Ejemplos de Datos Personales: Nombre, teléfono, domicilio, número de teléfono, huellas dactilares, así como cualquier otro dato que pueda servir para identificar a la persona.

Datos Personales Sensibles: Aquellos Datos Personales que afecten a la esfera más íntima de su Titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos Datos Personales que puedan revelar aspectos como: origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, y preferencia sexual.

Datos Financieros o Patrimoniales: Este término no se encuentra definido en la LFPDPPP o su Reglamento, sin embargo, este tipo de datos se deben tratar como “sensibles” ya que conforme al artículo 8 de la LFPDPPP, el tratamiento se encuentra sujeto al consentimiento expreso del Titular.

[35] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010 y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

8. Tratamiento de datos personales

El tratamiento de Datos Personales se encuentra sujeto al consentimiento de su Titular, que puede manifestarse de las siguientes formas (cada uno de los tipos de Datos Personales exige un nivel diferente de consentimiento):

a) **Consentimiento Expreso**: cuando la voluntad del Titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, o por cualquier otra tecnología o por signos inequívocos.

b) **Consentimiento Tácito**: cuando habiéndose puesto a su disposición el Aviso de Privacidad el Titular no manifieste su oposición al Tratamiento.

Para el caso del tratamiento de Datos Sensibles el consentimiento deberá de ser otorgado de manera expresa y además por escrito, esto quiere decir que debe de recabarse la firma autógrafa o electrónica del Titular, o crear cualquier mecanismo de autenticación del Titular y que se pueda probar su consentimiento expreso.

Para el tratamiento de Datos Personales Patrimoniales o Financieros, el Responsable debe obtener el consentimiento expreso del Titular.

En caso de llevar a cabo el Tratamiento de Datos Personales ordinarios o meramente identificativos, bastará obtener el consentimiento tácito del Titular. Lo anterior puede realizarse cuando en el primer contacto que se tenga con el Titular, se ponga a disposición de éste el Aviso de Privacidad, y éste no manifieste su oposición al Tratamiento.

Ahora bien, en vista de que la carga de la prueba recae en el Responsable, para comprobar el uso adecuado de los Datos Personales, se recomienda que el Responsable obtenga el consentimiento por escrito del Titular mediante la firma del Aviso de Privacidad.

Los Datos Personales solo podrán ser tratados para los fines mencionados en el Aviso de Privacidad, a menos que lo permita una ley o reglamento de forma explícita. Si se pretende dar un uso distinto de los Datos Personales del Titular que no resulte análogo o compatible a los fines establecidos en el Aviso de Privacidad, se requerirá obtener nuevamente el consentimiento del Titular.

El Responsable procurará que los Datos Personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para las finalidades por las cuales fueron recabados. Sólo se podrán crear bases de datos de Datos Sensibles cuando se obtenga la autorización del Titular. De igual forma, su creación deberá justificarse por los siguientes medios:

a) Obedezca a mandato legal.
b) Se justifique para la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros.
c) El Responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

Cuando los Datos Personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el Aviso de Privacidad y las disposiciones legales aplicables, deberán ser cancelados. Para esto [PSCN] deberá implementar un sistema en el cual el Responsable pueda saber el momento en que se deban cancelar los Datos Personales (por ejemplo, a través de un aviso por parte de la base de datos en el sistema).

El Responsable estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de 72 meses, contado a partir de la fecha en que se materialice el mencionado incumplimiento.

9. Transferencia de datos personales

Los Datos Personales pueden ser transferidos a Terceros en México o en el extranjero, siempre y cuando:

a) La transferencia de Datos Personales se realice conforme a lo dispuesto en el Aviso de Privacidad y conste en éste el consentimiento del Titular para efectuar dichas transferencias.
b) Se entregue al Tercero una copia del Aviso de Privacidad entregado al Titular.
c) El Tercero deberá de realizar el Tratamiento de los Datos Personales conforme a las finalidades establecidas en el Aviso de Privacidad.
d) El Tercero asuma las mismas responsabilidades que el Responsable. Por consiguiente, se debe hacer constar lo anterior dentro de los contratos celebrados entre el Responsable y el Tercero.

Las Transferencias no requieren el consentimiento del Titular en los siguientes supuestos:

a) Cuando así sí se establezca en una ley o tratado internacional del que México sea parte.
b) Cuando sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios (por ejemplo, cuando ocurra un accidente de trabajo y se requiera divulgar Datos Sensibles para su debida atención por parte de médicos o paramédicos).
c) Sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del Responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del Responsable que opere bajo los mismos procesos y políticas internas.
d) Sea necesaria por virtud de un contrato celebrado o por celebrar en interés del Titular, por el Responsable y un Tercero.

e) Sea necesaria o legalmente exigida para salvaguardar el interés público, o para la procuración o administración de justicia (por ejemplo, cuando por escrito de autoridad se requiera la divulgación de Datos Personales para perseguir un delito).
f) Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial (esto puede ser en caso de que se requiera divulgar la información para la defensa de [PSCN] ante la Junta de Conciliación y Arbitraje, entre otras autoridades).
g) Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el Responsable y el Titular (cuando, por ejemplo, se requiera para el cumplimiento de un contrato o la prestación de un servicio o la venta de un producto de [PSCN]).

10. Derechos de acceso, rectificación, cancelación y oposición (ARCO)

Los Titulares de los Datos Personales tendrán de conformidad con la LFPDPPP y su Reglamento el derecho de **acceder** a los Datos Personales que [PSCN] posea y a conocer los detalles del tratamiento de los mismos; **rectificar** en caso de que estén incompletos o sean inexactos; **cancelarlos** en caso que éste considere que no se requieren para alguna de las finalidades señaladas en el Aviso de Privacidad, estén siendo utilizados para finalidades que no hayan sido consentidos, haya finalizado la relación con [PSCN]; o bien, **oponerse** al tratamiento de los Datos Personales que haya proporcionado para fines específicos[36].

Para el ejercicio de los derechos de acceso, rectificación, cancelación y/u oposición al tratamiento de Datos Personales, en términos de la LFPDPPP, cualquier solicitud de ejercicio de los derechos mencionados el Titular deberá necesariamente proporcionar e indicar: i) nombre y domicilio, ii) una copia de su identificación oficial (pasaporte, credencial de elector o licencia de conducir), iii)

[36] Artículos 22 a 27 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

descripción clara y precisa de los Datos Personales a los que desea acceder o que desea rectificar, cancelar u oponerse y cualquier otro elemento que facilite la localización de los Datos Personales, así como iv) cualquier otro requisito establecido por la LFPDPPP y/o demás disposiciones aplicables[37].

En todos los casos [PSCN] deberá responder cualquier solicitud completa en un plazo máximo de veinte (20) días hábiles o el máximo permitido por la ley. La respuesta de [PSCN] deberá indicar si la solicitud de acceso, rectificación, cancelación u oposición es procedente y, en su caso, [PSCN] hará efectiva la determinación dentro de los quince (15) días hábiles siguientes a la fecha en que comunique la respuesta al titular de los Datos Personales o a su representante en su caso[38].

Estos plazos podrán ampliarse una sola vez por un periodo igual, cuando lo amerite el caso. En este caso se deberá dar aviso al Titular de la ampliación del plazo y justificar el motivo de la ampliación en los términos del artículo 97 del Reglamento.

En el caso de que la información proporcionada en la solicitud sea insuficiente o errónea para atenderla, [PSCN] podrá requerir al Titular, por una vez y dentro de los cinco (5) días siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma. El Titular contará con diez días para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente. En caso de que el Titular atienda el requerimiento de información, el plazo para que [PSCN] dé respuesta a la

[37] Artículo 29 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010
[38] Artículo 32 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

solicitud empezará a correr al día siguiente de que el Titular haya atendido el requerimiento[39].

En caso de que [PSCN] no requiera al Titular documentación adicional para la acreditación de su identidad o de la personalidad de su representante, se entenderá por acreditada la misma con la documentación aportada por el Titular desde la presentación de su solicitud.

11. Particularidades de los derechos ARCO

Para el Derecho de Acceso

[PSCN] podrá proporcionar copias electrónicas de la información personal del Titular en caso de que éste ejerza su derecho de **acceso**[40].. Peculiaridades

Para el Derecho de Cancelación

Con relación al derecho de **cancelación** de Datos Personales, el Titular podrá proceder respecto de la totalidad de los Datos Personales contenidos en una base de datos, o sólo parte de ellos, según su solicitud[41].

De resultar procedente la cancelación [PSCN] deberá[42]:

a) Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su Tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al Titular o a su representante en la respuesta a la solicitud de cancelación.
b) Atender las medidas de seguridad adecuadas para el bloqueo.

[39] Artículo 96 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012
[40] Artículo 33 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010
[41] Artículo 106 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012
[42] Artículo 107 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

c) Llevar a cabo el bloqueo en el plazo de quince días hábiles siguientes a la fecha en que se comunica la respuesta a la solicitud del Titular.
d) Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad establecidas para dicho fin.

El Responsable no estará obligado a cancelar los Datos Personales cuando:

a) Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
b) Deban ser tratados por disposición legal.
c) Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
d) Sean necesarios para proteger los intereses jurídicamente tutelados del Titular.
e) Sean necesarios para realizar una acción en función del interés público.
f) Sean necesarios para cumplir con una obligación legalmente adquirida por el Titular.
g) Sean objeto de Tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho Tratamiento se realice por un profesional de la salud sujeto a un deber de secreto (por ejemplo, médicos y/o paramédicos).

En caso de ser procedente, [PSCN] deberá de otorgar una constancia al Titular de que sus Datos Personales fueron cancelados.

Para el Derecho de Oposición[43]

El Titular tendrá en todo momento el derecho a **oponerse** al Tratamiento de sus Datos Personales cuando:

[43] Artículo 109 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

a) Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el Tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al Titular.
b) Para que no se lleve a cabo el Tratamiento de Datos Personales para fines específicos.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el Tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al Responsable.

Para el ejercicio del derecho de oposición, los Responsables podrán gestionar Listados de Exclusión propios en los que incluyan los Datos Personales de las personas que han manifestado su negativa para que se sigan tratando sus Datos Personales; se deberá avisar a los Titulares de su inclusión en dichos listados.

El Listado de Exclusión es una medida de seguridad para el Responsable a fin de que tenga control de los Titulares que solicitaron la cancelación y/o oposición en el Tratamiento de sus Datos Personales.

12. Negativa al ejercicio de derechos ARCO[44]

El Responsable podrá negar el ejercicio de los derechos ARCO, en los siguientes supuestos:

a) Cuando el solicitante no sea el Titular de los Datos Personales, o el representante legal no esté debidamente acreditado para ello.
b) Cuando en su base de datos, no se encuentren los Datos Personales del solicitante.
c) Cuando se lesionen los derechos de un tercero.

[44] Artículo 34 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

d) Cuando exista un impedimento legal, o la resolución de una autoridad competente que restrinja el acceso a los derechos ARCO.
e) Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

El ejercicio de los derechos ARCO podrá restringirse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente debidamente fundada y motivada.

Se debe de establecer en el Aviso de Privacidad el medio (teléfono o correo electrónico de la persona que debe dar respuesta a las solicitudes correspondientes o del departamento de control).

El ejercicio de los derechos ARCO será sencillo y gratuito, debiendo cubrir el Titular únicamente los gastos de envío, reproducción y, en su caso, certificación de documentos.

No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a 3 veces la UMA a menos que existan modificaciones sustanciales al Aviso de Privacidad que motiven nuevas consultas[45].

Cuando se niegue el ejercicio de cualquiera de los derechos ARCO se deberá justificar su respuesta, así como informar al Titular el derecho que tiene para solicitar el inicio del procedimiento de protección de derechos ante el INAI.

[45] Artículo 35 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

13. Revocación del consentimiento y limitación del uso y divulgación[46]

El Titular tiene derecho de **revocar su consentimiento**, de continuar con el Tratamiento de sus Datos Personales, en cualquier momento. Para que el Titular pueda revocar su consentimiento, el Responsable debe de establecer los mecanismos y procedimiento para ello en el Aviso de Privacidad, una vez que sea procedente la solicitud de revocación de consentimiento se debe cesar con el Tratamiento de los Datos Personales del Titular y comunicar dicha situación a los Encargados.

Por otro lado, el Titular también cuenta con el derecho de **limitar el uso y divulgación** de sus Datos Personales, para lo cual se sujetará a las mismas reglas de las solicitudes antes mencionadas y a los medios establecidos en el aviso de privacidad para ejercer dicho derecho[47].

14. Medidas de seguridad en el tratamiento de datos personales[48]

[PSCN] deberá adoptar las medidas de seguridad administrativas, físicas y técnicas, así como los procedimientos necesarios para proteger los Datos Personales contra daños, pérdidas, alteraciones, destrucción, así como cualquier Tratamiento, acceso o uso no autorizado. Dichas medidas deben ser las mismas que utilice el Responsable para salvaguardar su propia información.

Para esto se deben adoptar, entre otras medidas, las siguientes:

a) Asignar usuarios y claves de acceso o *passwords* para las personas designadas de llevar a cabo el Tratamiento de Datos Personales dentro de

[46] Artículo 21 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012
[47] Lineamiento Trigésimo de los Lineamientos del Aviso de Privacidad, *Diario Oficial de la Federación,* 17 de enero de 2013.
[48] Artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

[PSCN], a fin de identificarlos y autorizarlos a acceder a las bases de datos que los almacenen.

b) El uso de archivos bajo llave, en los que se almacenen expedientes con Datos Personales.

c) Controles en el Intranet de [PSCN], mediante los cuales se monitoree las personas que tienen acceso a los Datos Personales.

d) Controles de acceso en las computadoras utilizadas por las personas autorizadas, a fin de prevenir el acceso no autorizado a los Datos Personales, así como para evitar el daño o interferencia a dichos equipos y sistemas de control.

e) No permitir el almacenamiento de Datos Personales en dispositivos móviles o dispositivos de almacenamiento tales como USBs.

f) Respaldos de los Datos Personales almacenados en el servidor de [PSCN].

g) Entrega a las personas autorizadas para Tratar Datos Personales y a los empleados de [PSCN], las políticas internas para salvaguardar Datos Personales.

h) Impartir cursos de capacitación al personal de la empresa respecto de la protección de los Datos Personales y sobre la normatividad aplicable.

i) Realizar auditorías de manera interna o por auditores externos a efecto de evaluar el correcto Tratamiento de Datos Personales dentro de [PSCN].

j) Establecer los mecanismos para corregir las deficiencias detectadas en las auditorías que se realicen.

k) Identificar y clasificar la información para distinguir los tipos de Datos Personales que se recaban y la implementación de medidas de seguridad conforme a lo anterior.

l) Implementar medidas que garanticen la eliminación de forma segura, cuando corresponda, de Datos Personales.

m) Entregar a todos los empleados de [PSCN], por el medio que estime pertinente, la LFPDPPP y el Reglamento.

n) Elaborar un inventario de Datos Personales.

o) Determinar las funciones y obligaciones de los Encargados del Tratamiento de Datos Personales.

p) Realizar un registro de los medios de almacenamiento de los Datos Personales.

Las medidas de seguridad se deben actualizar cuando:

a) Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad de [PSCN].

b) Se produzcan modificaciones sustanciales en el Tratamiento que deriven en un cambio del nivel de riesgo;

c) Se vulneren los sistemas de tratamiento, lo que incluye:
   - La pérdida o destrucción no autorizada de Datos Personales.
   - El robo, extravío o copia no autorizada.
   - El uso, acceso o tratamiento no autorizado.

- El daño, la alteración o modificación no autorizada.

d) Exista una afectación a los Datos Personales, distinta a las anteriores.

En el caso de Datos Sensibles, los Responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes al menos, una vez al año.

El Responsable deberá informar al Titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió dicha vulneración. El informe debe contener al menos lo siguiente:

a) La naturaleza del incidente.

b) Los Datos Personales comprometidos.

c) Las recomendaciones al Titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.

d) Las acciones correctivas realizadas de forma inmediata.

e) Los medios donde puede obtener más información al respecto.

En caso de que ocurra una vulneración a los Datos Personales, se deberán analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

15. De la persona encargada o el departamento de control del tratamiento de datos personales

[PSCN] deberá designar un departamento o persona específica que se encargue de verificar que se cumpla con los mecanismos de seguridad para la protección

y preservación de los Datos Personales que sean sometidos a Tratamiento dentro de la organización[49].

Dicha persona o departamento dará trámite a todas las solicitudes de los Titulares para ejercitar sus de Derechos ARCO, de revocación y de limitación al uso y divulgación. Además, vigilará que se dé cumplimiento a las disposiciones de la LFPDPPP y su Reglamento, las cuales se encuentran resumidas en el presente documento y cuando exista duda contactar al departamento legal de [PSCN]. De igual forma esta persona o departamento deberá fomentar la protección de los Datos Personales dentro de [PSCN].

15.1. Funciones específicas

La Persona encargada o el Departamento de control del tratamiento de Datos Personales, tendrán como mínimo las siguientes funciones:

a) Establecer y administrar procedimientos para la recepción, tramitación, seguimiento y atención oportuna de las solicitudes para el ejercicio de los Derechos ARCO, así como para la atención de quejas o solicitudes presentadas por los Titulares relacionadas con las políticas y/o prácticas de protección de Datos Personales,

b) Monitorear los avances o cambios legislativos en materia de privacidad y protección de datos personales que pudieran impactar en los ejes rectores y acciones desarrolladas en este tema al interior de la organización, haciendo las adecuaciones necesarias, y

c) Fomentar la protección de Datos Personales al interior de [PSCN]; de manera general la persona o departamento designado, deberá realizar la implementación política de difusión dentro de la empresa relativas a la

[49] Artículo 30 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

protección de Datos Personales, a fin de dar a conocer a todo el personal el cuidado que debe tenerse respecto al manejo y Tratamiento de Datos Personales y los mecanismos que de manera interna se han implementado.

En cuanto a la función de dar trámite a las solicitudes de los Titulares que se realicen a [PSCN], para el ejercicio de los derechos ARCO, se han establecido métodos sencillos para que los Titulares de los Datos Personales puedan ponerse en contacto con la [PSCN] y ejercer sus derechos ARCO. Al respecto, como método de contacto principal se ha implementado el correo electrónico. Asimismo, y en un afán de dar mayores posibilidades de contacto a los Titulares de Datos Personales, dentro del Aviso de Privacidad de [PSCN] se establece que los mismos podrán contactarnos a través de nuestra dirección postal o número telefónico.

16. Aviso de Privacidad

De conformidad con la LFPDPPP, su Reglamento, y sobre todo con los Lineamientos del Aviso de Privacidad, éste deberá contener, al menos, la siguiente información[50]:

a) La identidad y domicilio del Responsable que realice el Tratamiento de los Datos Personales.

b) Los Datos Personales que serán sometidos al Tratamiento;

c) El señalamiento expreso de los Datos Personales Sensibles que se Tratarán;

d) Las finalidades del tratamiento de los Datos Personales;

[50] Lineamiento Vigésimo de los Lineamientos del Aviso de Privacidad, *Diario Oficial de la Federación,* 17 de enero de 2013.

e) Los mecanismos para que el Titular pueda manifestar su negativa para el Tratamiento de sus Datos Personales respecto de aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el Responsable.

f) Las Transferencias de Datos Personales que en su caso se efectúen, el Tercero receptor de los Datos Personales, y las finalidades de estas;

g) La cláusula que indique si el Titular acepta o no la Transferencia, cuando así se requiera;

h) Los medios y procedimientos para ejercer los Derechos ARCO;

i) Los mecanismos y procedimientos para que, en su caso, el Titular pueda revocar su consentimiento al tratamiento de sus Datos Personales;

j) Las opciones y medios que el Responsable ofrece al Titular para limitar el uso o divulgación de los Datos Personales;

k) La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica y otra tecnología, que permitan recabar Datos Personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso, y

l) El procedimiento y medio por el cual el Responsable comunicará a los Titulares de cambios al Aviso de Privacidad, de conformidad con lo previsto en la LFPDPPP.

Cualquier cambio al Aviso de Privacidad debe darse a conocer al Titular y se recomienda establecer el mecanismo para que se pueda comprobar esto, como el entregar el nuevo Aviso de Privacidad y que la entrega sea acusada de

recibido. Si se envía por correo electrónico, también se deberá contar con el correo que compruebe que el Titular recibió el nuevo Aviso de Privacidad.

El Aviso de Privacidad debe ponerse a disposición de los Titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

a) Cuando los Datos Personales hayan sido obtenidos personalmente del Titular, el Aviso de Privacidad deberá ser facilitado en la modalidad integral, es decir, incluyendo todos los requisitos a que se refieren los párrafos anteriores. Se debe entregar el Aviso de Privacidad previamente al momento en que se recaban los Datos Personales.

b) Cuando los Datos Personales sean obtenidos directamente del Titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, por ejemplo vía correo electrónico, se puede optar por entregar una modalidad "simplificada" del aviso de privacidad, en cuyo caso se deberá proporcionar al Titular, al menos, la información mencionada en los puntos a) y b) del contenido del Aviso de Privacidad, así como proveer los mecanismos para que el Titular conozca el texto completo del Aviso de Privacidad.

17. Relación entre el responsable y el encargado[51]

En vista de que el Encargado puede Tratar Datos Personales por cuenta del Responsable (por ejemplo, prestadores de servicios), la relación entre estos deberá especificar que el Encargado deberá cumplir con todas las medidas de seguridad necesarias para proteger los Datos Personales.

[51] Artículo 51 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

A la compartición de Datos Personales entre [PSCN] (Responsable) y sus Encargados se le denomina por el Reglamento de la LFPDPPP como "remisiones" de Datos Personales.

Las emisiones nacionales e internacionales de Datos Personales no se tienen que informarse al Titular, ni es necesario contar con consentimiento expreso para dicha Remisión. Sin embargo, será necesario que estas se describan en el Aviso de Privacidad[52].

[PSCN] será el Responsable del Tratamiento de los Datos Personales que le remita a sus Encargados, a menos que éstos:

a) Destinen o utilicen los Datos Personales que les fueron remitidos con una finalidad distinta a la autorizada por [PSCN], o

b) Efectúen una Transferencia, incumpliendo las instrucciones de [PSCN], es decir, los usos autorizados a través del Aviso de Privacidad.

En ambos casos los Encargados asumirán el rol de Responsables y deberán asumir todas aquellas obligaciones que así se establezcan en la LFPDPPP.

18. Subcontrataciones

Toda subcontratación de servicios por parte del Encargado que implique el tratamiento de Datos Personales deberá ser autorizada por [PSCN] (Responsable), y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el Encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.

[52] Artículo 53 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

[PSCN] no podrá contratar servicios con prestadores que no garanticen la debida protección de los Datos Personales en su posesión y que no cuenten con las medidas de seguridad necesarias para garantizar lo anterior[53].

19. Infracciones, sanciones y delitos

Infracciones y Sanciones. Las infracciones se encuentran enumeradas en el artículo 63 de la LFPDPPP. Para mayor referencia, a continuación, se cita el artículo en comento:

> *Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:*
>
> *I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;*
>
> *II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;*
>
> *III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;*
>
> *IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;*
>
> *V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;*

[53] Artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2012

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y

XIX. Cualquier incumplimiento del responsable.

El INAI podrá sancionar con[54]:

a) El apercibimiento para que el Responsable lleve a cabo los actos solicitados por el Titular, en los supuestos previstos en la fracción I del artículo 63.

b) Multa de 100 a 160,000 veces la UMA, en los casos previstos en las fracciones II a VII.

c) Multa de 200 a 320,000 veces la UMA, en los casos previstos en las fracciones VIII a XVIII.

En caso de que, en forma reiterada persistan las infracciones, se impondrá una multa adicional que irá de 100 a 320,000 veces la UMA. En caso de infracciones cometidas en el tratamiento de Datos Sensibles, las sanciones podrán incrementarse hasta dos veces el monto establecido.

[54] Artículo 64 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010

Delitos por el Tratamiento indebido de los Datos Personales[55]:

a) Al que, estando autorizado para Tratar los Datos Personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia, se impondrán de 3 meses a 3 años de prisión.

b) Se sancionará con prisión de 6 meses a 5 años al que, con el fin de alcanzar un lucro indebido, trate Datos Personales mediante el engaño, aprovechándose del error en que se encuentre el Titular o la persona autorizada para transmitirlos.

Tratándose de Datos Sensibles, las penas antes mencionadas se duplicarán.

[55] Artículos 67 a 69 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 5 de julio de 2010