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

"REQUISITOS QUE DEBEN CUMPLIRSE PARA PROTEGER LOS DATOS PERSONALES EN LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE EN LA ADMINISTRACIÓN PÚBLICA FEDERAL"

REPORTE ANALÍTICO DE EXPERIENCIA LABORAL

Que para obtener el grado de MAESTROS EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presentan:

Guadalupe Cosme Cruz

Lucio Flores Cerrillo

Asesor:

Mtro. Arístides Rodrigo Guerrero García

Ciudad de México, junio, 2020.

CONACYT

INFOTEC POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 7 de septiembre de 2020
INFOTEC-DAIC-GCH-SE-0537/2020.

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

REQUISITOS QUE DEBEN CUMPLIRSE PARA PROTEGER LOS DATOS PERSONALES EN LA CONTRATACIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE EN LA ADMINISTRACIÓN PÚBLICA FEDERAL

Desarrollado por los alumnos **Guadalupe Cosme Cruz** y **Lucio Flores Cerrillo**, bajo la asesoría del **Mtro. Arístides Rodrigo Guerrero García**; 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.

Mtra. Julieta Alcibar Hermosillo
Coordinadora 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

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

“ANS”	Acuerdos de Nivel de Servicio
“APF”	Administración Pública Federal
“ARCO”	acceso, rectificación, cancelación y oposición
“DOF”	Diario Oficial de la Federación
“DRP”	Plan de Recuperación de Desastres
“EDN”	Estrategia Digital Nacional
“GDPR”	Reglamento General de Protección de Datos
“HGPTIC”	Herramienta de Gestión de Política en Tecnologías de la Información y Comunicación
“IaaS”	Infraestructura como Servicio
“INAI”	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos
“INFOTEC”	Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación
“ITU”	Unión Internacional de Telecomunicaciones
“LAASSP”	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público
“LOPSRM”	Ley de Obras Públicas y Servicios Relacionados con las mismas
“MAAGTICSI”	Manual administrativo de aplicación general en materia de tecnologías de la información y comunicación y seguridad de la información
“SCJN”	Suprema Corte de Justicia de la Nación
“LFPDPP”	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
“LGPDPPSO”	Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados
“OIC”	Órgano Interno de Control
“PaaS”	Plataforma como servicio

“Prosoft”	Programa para el Desarrollo de la Industria del Software y la Innovación
“SLA”	Acuerdo de Nivel de Servicio
“SHCP”	Secretaría de Hacienda y Crédito Público
“SFP”	Secretaría de la Función Pública
“TIC”	Tecnologías de la Información y Comunicación
“UGD”	Unidad de Gobierno Digital de la Secretaría de la Función Pública
“UTIC”	Unidad de Tecnologías de la Información en el INFOTEC
“UPCP”	Unidad de Política y Control Presupuestario de la Secretaría de Hacienda y Crédito Público

Introducción

El siguiente reporte analítico de experiencia laboral tiene como finalidad identificar y facilitar, al interior de las dependencias y entidades de la Administración Pública Federal, los requisitos que deben observarse para proteger los datos personales en las contrataciones que éstas celebren con los particulares en servicios relacionados con cómputo en la nube; para ello, resaltaremos, dada su importancia, la definición que da la doctrina a un contrato administrativo, los elementos que lo conforman, sus características, cuáles son sus principios rectores, su ámbito de validez, cómo se clasifican y qué debe observarse para diferenciar un contrato administrativo de cualquier otro contrato, cuál es la legislación aplicable y sobre todo, cuál es la finalidad de un contrato administrativo.

Posteriormente, nos adentraremos a estudiar los procedimientos de contratación que lleva a cabo la Administración pública para cumplir con las obligaciones que tiene para con sus gobernados, en qué consiste cada uno de los tres procedimientos, en qué casos opera cada uno de ellos, cuáles son los requisitos de procedibilidad y las formalidades de cada uno de ellos y centraremos nuestra atención en los contratos de cómputo en la nuble, la legislación aplicable y los requisitos a observar para su celebración, cuáles son las cláusulas que debe contener un contrato para establecer las obligaciones de las partes y más aún, resaltaremos la importancia de elaborar un anexo técnico robusto y protegido por parte de las áreas técnicas y/o requirentes, ya que éste es la base fundamental del éxito del procedimiento; en primer lugar, para que éste sea transparente y cumpla con los principios constitucionales; en segundo, atraer el mayor número de participantes y evitar inconformidades y; por último, ser el documento que servirá de base para la elaboración de un instrumento contractual jurídicamente resistente.

A continuación, abordaremos, las que a nuestro juicio, podrían considerarse áreas de oportunidad en la contratación de servicios de cómputo en la nube, la sobre regulación existente y el tema medular: qué debe considerar la administración pública para proteger los datos personales para contratar servicios de cómputo en la nube y cumplir con las facultades de brindar bienes y servicios a sus gobernados,

garantizando la protección de datos en estricto apego a la normativa tanto para sujetos obligados como para particulares y los criterios emitidos por el órgano garante en materia de datos personales para implementar medidas de seguridad tanto físicas como de infraestructura y de recursos humanos.

En el tercer capítulo, mencionaremos los procedimientos de contratación que realiza INFOTEC que, como ente público que es uno de los principales proveedores especializado en tecnologías de la información y comunicación, los requisitos a observar por éste al contratar servicios, y la importancia de su figura en la Administración Pública Federal; qué documentación debe incluir el área requirente para soportar la contratación y qué procedimiento es el más recurrente.

El último capítulo, aborda el compromiso de la Administración Pública en el cumplimiento que mandata la constitución para la protección de los datos personales de sus gobernados, con la vigilancia del órgano garante, el Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales y, la importancia de la capacitación constante de los servidores públicos que intervienen, directa o indirectamente en la contratación de este tipo de servicios, en materia de datos personales; el cual, es un compromiso gubernamental para combatir la corrupción y fomentar las virtudes del servicio público.

Capítulo 1

El contrato administrativo y los procedimientos de contratación pública

Capítulo 1. El contrato administrativo y los procedimientos de contratación pública

1.1. Resumen

En presente capítulo, se retomará el concepto, la naturaleza, los elementos, los sujetos, los requisitos, las características de los contratos administrativos; así como el ámbito de validez, su clasificación y tipos de contratos administrativos, conceptos esenciales en el actuar de la Administración Pública Federal y que resultan indispensables dado que hablaremos a lo largo del camino de los contratos celebrados en la Administración Pública. Explicaremos cada uno de los procedimientos de contratación que lleva a cabo ésta, para allegarse de bienes y servicios para cumplir con sus obligaciones en aras del bien común e interés público, En el presente apartado abordaremos los tres procedimientos de contratación que contempla la Ley de la materia, reglamentaria del artículo 134 Constitucional, el cual establece que los recursos económicos de que dispongan la Federación, las Entidades Federativas, los Municipios y las demarcaciones territoriales de la Ciudad de México, se administrarán con eficiencia, eficacia, economía, transparencia y honradez; establece también, que se privilegiará la licitación pública para la contratación de los bienes y servicios necesarios para el cumplimiento de sus obligaciones, para que cualquier interesado acuda al concurso en igualdad de circunstancias, se estimule la sana competencia y se obtengan los bienes y servicios con la oportunidad que permita al Estado cumplir con las obligaciones que tiene para con sus gobernados.

Señalaremos las diferencias entre los diferentes procedimientos de contratación, en qué casos opera cada uno de ellos ,cuándo deben aplicarse, cuáles son los plazos por observar y, sobre todo, los requisitos a cubrir por todos los involucrados, en qué circunstancias aplica uno u otro, qué requisitos debe observar el Estado antes, durante y después del concurso, en su calidad de convocante, así como los requisitos que debe cumplir la persona física o moral que participe en el procedimiento para la entrega de bienes o prestación de servicios, lo que resulta

determinante al momento de la evaluación de proposiciones en el tipo de servicio objeto de estudio del presente trabajo.

1.2. Objetivos

1) Identificar qué es un contrato administrativo quiénes participan en su celebración, cuáles son los requisitos que deben cumplirse y cómo se clasifican.
2) Diferenciar entre los contratos comunes y los contratos administrativos, cuya finalidad es facilitar al estado el cumplimiento de las obligaciones para con sus gobernados.
3) Evaluar que los contratos administrativos que celebra el Estado, además de celebrarse en apego a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, efectivamente se celebren para cumplir con atribuciones reguladas por ley, reglamento o estatuto específico y por un periodo de tiempo específico.
4) Proporcionar los elementos que permitan identificar los distintos procedimientos de contratación que realiza el Estado para contar con los bienes y servicios que proporciona a sus gobernados, en qué casos opera uno y otro y los medios utilizados.
5) Una vez identificados los requisitos a cumplir entre uno y otro procedimiento, facilitar la elección del procedimiento de acuerdo con el bien o servicio a contratar.
6) Toda vez que la finalidad del presente estudio es la contratación de cómputo en la nube, se buscará que el área contratante identifique fácilmente los aspectos imprescindibles a considerar para proteger los datos personales en este tipo de servicios, observando las leyes de protección de datos personales tanto para sujetos obligados, como particulares así como la normatividad en materia de adquisiciones, estrategia digital y seguridad de la información, para realizar procedimientos de contratación con transparencia, eficacia, eficiencia,

economía y honradez, que permitan al Estado cumplir con sus obligaciones en el menor tiempo posible al eficientar procesos, garantizando con ello, el derecho a la protección de datos y acceso a servicios de calidad.

1.3. Concepto y naturaleza jurídica del contrato administrativo

En la práctica, se conoce al contrato administrativo como la formalización del acuerdo de voluntades entre la administración pública y el particular para crear, modificar, transmitir o liquidar derechos y obligaciones con el fin de satisfacer el interés público, es decir, el instrumento jurídico que permite al estado adquirir bienes o servicios en beneficio de los gobernados conforme las facultades a éste conferidas.

En el contrato administrativo una de las partes es el Estado, dependencia o entidad de la Administración Pública Federal de cualquiera de los tres órdenes de Gobierno. No existen contratos administrativos entre particulares. La finalidad principal del contrato administrativo es el interés general, es decir, proporcionar bienes y servicios a sus gobernados, en cumplimiento de garantías constitucionales y obligaciones de Gobierno.

De la misma forma en que los servicios que proporciona el Estado a sus gobernados se encuentran expresamente determinados en Ley, el procedimiento que siga el Estado para acordar con los particulares un contrato administrativo, así como el que se aplique para su ejecución, serán los previstos y regulados por la Ley administrativa o por el derecho público en general.

1.3.1. Definición de autores[1]

Alfonso Nava Negrete, en el diccionario jurídico mexicano, de 1994, define el término en cuestión como el contrato que celebra la administración pública federal

[1] Sarabia Miramontes, Grecia, *Gestión de obra pública en México: contratos de obra pública y Pidiregas*, capítulo primero, “La actividad del Estado”, México, Universidad de las Américas Puebla, 2003, disponible en *http://catarina.udlap.mx/u_dl_a/tales/documentos/ledf/sarabia_m_g/capitulo 1.pdf,* (fecha de consulta: 20 de junio de 2018).

con los particulares con el objeto directo de satisfacer un interés general, cuya gestación y ejecución se rigen por procedimientos de derecho público.

Gabino Fraga considera que “cuando el objeto o la finalidad del contrato estén íntimamente vinculados al cumplimiento de las atribuciones estaduales de tal manera que la satisfacción de las necesidades colectivas no sea indiferente a la forma de ejecución de las obligaciones contractuales, entonces se entrará en el dominio del contrato administrativo”.

Andrés Serra Rojas lo define como un acuerdo de voluntades celebrado, por una parte, la Administración Pública Federal y por la otra, personas privadas o públicas, con la finalidad de crear, modificar o extinguir una situación jurídica de interés general, o en particular relacionada con los servicios públicos, que unen a las partes en una relación de estricto derecho público, sobre las bases de un régimen exorbitante del Estado.

En tanto, que para la Suprema Corte de Justicia de la Nación es un “…acuerdo de voluntades entre la Administración Pública Federal y un particular con el que se crean derechos y obligaciones para la satisfacción del interés público, y que se encuentra sujeto a un régimen de derecho público[2]”.

De esta manera, habrá que reflexionar en torno a la naturaleza de los contratos administrativos con el Gobierno, según la jurisprudencia; el primer elemento a considerar será la finalidad que se persigue, ya que, si ésta es cumplir con una obligación del Estado para con sus gobernados, efectivamente, se está frente a un contrato administrativo; por el contrario, si el contrato a celebrarse no tiene como fin último el cumplimiento de una atribución, se trataría de un contrato civil. Por ejemplo, si el Gobierno contrata a un proveedor para que éste imprima las Cartillas Nacionales de Salud que el Gobierno entrega a sus gobernados, se estaría ante un contrato administrativo, toda vez que dichas cartillas permitirían un seguimiento personalizado y continuo de las acciones de promoción, prevención y

[2] Tesauro Jurídico de la Suprema Corte de Justicia de la Nación, “derecho administrativo”, p. 58, disponible en: *https://www.sitios.scjn.gob.mx/centrodedocumentacion/sites/default/files/tesauro_juridico_scjn/pdfs/01.%20TJSCJN%20-%20DerAdmin.pdf* (fecha de consulta: 20 de junio de 2018).

control de enfermedades que recibe la población en cada etapa de su vida, atribución conferida a las instituciones de salud públicas por ministerio de Ley. Es decir, aquellos contratos en los que el Gobierno es una de las partes, ya sea que se trate de la adquisición de un bien o la contratación de un servicio, pero que será utilizado para la prestación de los servicios públicos a los que está obligado constitucionalmente o por Ley específica, serán de carácter administrativo.[3]

1.3.2. Elementos del contrato administrativo[4]

Por "elemento" entendemos cada uno de sus componentes del contrato administrativo, estos se dividen en esenciales y no esenciales; los primeros son indispensables para su existencia y los segundos, pueden o no existir y no afectan la finalidad del contrato.

Los elementos esenciales del contrato administrativo son los sujetos, es decir las partes que celebran el contrato (el estado y el particular); el consentimiento que consiste en la manifestación por escrito que hacen las partes para externar su voluntad de celebrar el contrato, cuando nos referimos a este elemento del contrato administrativo, estamos ante la manifestación escrita de las partes en el establecimiento de derechos y obligaciones, siempre y cuando los firmantes se encuentren facultados para ello; dichas facultades deben estar expresamente establecidas para ambas partes en instrumento jurídico; en el caso del estado generalmente se localiza en el manual de organización, estatuto orgánico o reglamento interno, en el caso del particular, en poder para actos administrativos, debidamente protocolizado ante fedatario público; el objeto, es decir para qué se celebra el contrato (adquirir o arrendar bienes o contratar servicios) y la causa: el fin que lleva al estado la celebración del contrato. Existen autores que consideran la forma, la competencia y capacidad, el régimen jurídico especial y la licitación (convocatoria) como elementos. Vale la pena mencionar que, la (LAASSP art. 45)

---

[3] Tesis s/n aislada, *Semanario Judicial de la Federación*, Quinta Época, t CVIII, p. 17.

[4] Fernández Ruiz, Jorge, "Derecho administrativo", México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Secretaría de Cultura, UNAM, Instituto de Investigaciones Jurídicas, 2016 p. 175-179

establece que la "*convocatoria a la licitación, el contrato y sus anexos son los instrumentos que vinculan a las partes en sus derechos y obligaciones"*

1.3.3. Requisitos del contrato administrativo[5]

Un requisito es la condición de validez del contrato, es decir que dicha condición resulta indispensable para hacer válido el instrumento jurídico. Los requisitos son competencia: se refiere a que el ente público que celebre el contrato debe estar facultado por disposición jurídica para ello; capacidad: el particular ya sea persona física o moral debe contar con la aptitud para ser titular de derechos y obligaciones y hacerlos valor por sí y; forma: el Estado debe realizar actos previos, análogos e incluso, posteriores para la celebración de un contrato.

Las formalidades deben ser observadas por su contraparte de acuerdo con las normas aplicables, entre las que se consideran convocatorias, términos de referencia, anexos técnicos, según sea el caso. Éstas resultan de ordenamientos jurídicos y modalidades específicas de contratación, como en el caso de licitaciones, invitaciones a cuando menos tres personas, conocidas como invitaciones restringidas y adjudicaciones directas.

1.3.4. Características esenciales del contrato administrativo

Juridicidad. Los actos de la Administración Pública Federal se dividen en jurídicos y no jurídicos, los primeros, producen consecuencias jurídicas y los no jurídicos, si bien son emitidos por la autoridad en ejercicio de sus funciones no producen efectos jurídicos, en este último caso, tenemos como ejemplo, la opinión que por escrito emita un servidor público sobre determinado asunto.

Bilateralidad. Se dice que un contrato es bilateral porque ambas partes generan derechos, pero también tienen obligaciones. En materia administrativa y el tema que nos ocupa, contratación de servicios por parte de la administración pública

[5] Secretaría de Gobernación, Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, México, Diario Oficial de la Federación, 4 de febrero de 2016

federal, una de las partes tiene derecho a recibir un servicio, pero adquiere la obligación de pagar por el servicio y, el particular, tiene derecho a recibir un pago por el servicio proporcionado, entre otras obligaciones.

Desigualdad de las partes. Este requisito tiene que ver con que una de las partes siempre será el estado y la otra, uno más particulares; ya que, si ambas partes fueran el estado en cualquiera de los tres órdenes de gobierno, estaríamos frente a un convenio de colaboración y no un contrato administrativo y; si ambas partes fueran particulares, no se trataría de un contrato administrativo sino estaríamos frente a un contrato civil.

Restricción de la libertad de las partes. Podría interpretarse como un acto unilateral de la autoridad, ya que el particular, en los procedimientos de contratación solamente se apega al modelo de contrato publicado por la Convocante

Interés público prevaleciente. Es requisito indispensable que la celebración de un contrato administrativo tenga como finalidad satisfacer el interés público y, por último, el régimen jurídico exorbitante del derecho privado se da, al existir desigualdad de las partes; ya que si bien, existe un acuerdo de voluntades; frecuentemente el particular se sujeta a las condiciones del Estado; es decir, las obligaciones, no son negociables.

1.3.5. Principios rectores del contrato administrativo[6]

Principio de legalidad. En la celebración del contrato administrativo, la Administración Pública Federal no debe incluir condiciones que no estén expresamente contempladas en alguna Ley, reglamento, decreto, lineamiento o acuerdo con efectos jurídicos ante terceros; es decir, que dicha normativa haya sido publicada en el Diario Oficial de la Federación.

Principio de continuidad. Debe entregarse la totalidad de los bienes o proporcionarse la totalidad de los servicios contratados, de lo contrario, se aplican

[6] Fernández Ruiz, Jorge, “Derecho administrativo”, México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Secretaría de Cultura, UNAM, Instituto de Investigaciones Jurídicas, 2016 p. 172-173

deductivas y/o penalizaciones; se hace efectiva la garantía de cumplimiento de contrato que, por ministerio de Ley, debe otorgar el particular, y en caso contrario, la Administración Pública, está facultada para iniciar el procedimiento de rescisión. En resumen, el contrato no puede solamente dejar de surtir sus efectos sin consecuencias jurídicas.

Principio de mutabilidad. En la doctrina este principio se considera el más importante ya que el contrato administrativo, puede ser unilateralmente modificado dentro de ciertos límites por la Administración Pública Federal contratante, no así por el particular, siempre justificando el interés público.

Principio del equilibrio financiero. Se refiere a la capacidad de las partes para hacer frente a sus obligaciones en los plazos pactados, con el fin de evitar perjuicio a las partes o que los perjuicios ocasionados se reduzcan a su mínima expresión, recordemos que el estado contrata con el fin de atender las necesidades de sus gobernados, por lo que, en caso de retraso en el cumplimiento de las obligaciones por parte del particular, la afectación debe ser mínima.

1.3.6. Ámbito de validez

Implicaciones jurídicas de los contratos en materia de adquisición o arrendamientos de bienes muebles y la prestación de servicios a que se refiere la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP):

El ámbito de validez de las normas del derecho debe ser considerado, según Kelsen, desde cuatro puntos de vista: espacial, temporal, material y personal. El ámbito *espacial* de validez se refiere al espacio en que un precepto legal es aplicable; es decir, en los contratos celebrados al amparo de la LAASSP se incluye una cláusula de jurisdicción y competencia, en la que las partes se someten al espacio –territorio- donde se firmó o prestará el servicio; el *temporal* está constituido por el lapso durante el cual conserva su vigencia; el *material*, por la materia que regula, y el *personal*, por los sujetos a quienes obliga.

Ámbito material de validez. El contrato administrativo será válido hasta donde permitan las normas jurídicas que se expiden para regular algún campo de la vida social. Como se mencionó anteriormente, el Estado no puede ir más allá de lo que

le permite la norma jurídica, encaminada a regular la organización y actividad del Estado en sus relaciones con el particular.

1.3.7. Clasificación de los contratos administrativos

Los contratos administrativos se clasifican en unilaterales y bilaterales, en los primeros, una de las partes contrae obligaciones para con la otra sin que la segunda contraiga obligación alguna y; en los bilaterales, ambas partes contraen derechos y obligaciones y por lo tanto ambos asumen carácter de deudores y acreedores.

Por las prestaciones pactadas, los contratos pueden ser *a)* a título gratuito, es decir, una de las partes tiene derecho a recibir algo en su beneficio, pero la otra parte, no recibe pago por ello, un ejemplo de este tipo de contrato es la donación, supongamos que el ente público es una institución educativa que cuenta con una biblioteca y recibe en donación la colección privada de un famoso escritor, caricaturista o cualquier otra persona ya sea física o moral, en este caso la institución educativa no está obligada a pagar por dicha colección cuando el dueño de la obra, manifestó su voluntad, por escrito, de entregar en donación su colección para beneficio de la comunidad estudiantil de dicha institución. *b)* a título oneroso, en este tipo de contratos ambas partes reciben un beneficio, un ejemplo podría ser la compra de mobiliario para la biblioteca mencionada, la institución educativa recibe el mobiliario y la otra parte, tiene derecho a recibir una contraprestación[7].

Por el momento de su perfeccionamiento, los contratos se clasifican en consensuales, reales, formales y solemnes. Consensuales son aquellos en los que basta el simple consentimiento de las partes; se denomina reales a los contratos que es necesario la entrega del bien o la prestación del servicio; formales que son aquellos que para su existencia se debe observar determinada forma y observar un conjunto de elementos, en el caso de los contratos celebrados por la administración pública para adquirir bienes o contratar servicios, se requiere, de conformidad con la LAASSP, la formalización por escrito y el cumplir con requisitos mínimos

[7] *Ibidem* P. 180-183

señalados en el artículo 45 de ésta y 81 de su reglamento y; por último, los contratos solemnes, son aquellos para su existencia, debe observarse cierto protocolo, por ejemplo, la licitación pública, invitación a cuando menos tres personas, procedimientos que deben desahogarse cada una de las etapas que establece la ley de la materia para adjudicar el contrato.

Por su previsión en la Ley, los contratos pueden ser nominados cuando estén expresamente previstos en ordenamiento legal señalando los elementos que debe contener, consecuencias y causas de terminación, como es el caso de la LAASSP e innominados, son aquellos contratos que, a pesar de estar nombrado en ley, no se encuentra reglamentado.

Por la certeza de sus prestaciones, los contratos pueden ser conmutativos cuando los derechos y obligaciones de las partes sean ciertas desde que se celebra el contrato y, aleatorios cuando los derechos y obligaciones dependan de un acontecimiento incierto, en el caso de los contratos celebrados con la administración pública podríamos mencionar los contratos abiertos; cuando no se conoce con exactitud la cantidad a adquirir y se establece una cantidad mínima y máxima ya sea de bienes o en presupuesto.

Por su relación con otro contrato serán principales los que existan por sí solos y accesorios los que dependan jurídica y lógicamente de otro, es decir, para que exista un contrato accesorio (o específico) debe existir previamente un contrato principal, ejemplo de ello son los contratos marco contemplados en el artículo 17 de la LAASSP. Contratos que promueven la Secretaría de Hacienda y Crédito Público, la Secretaría de la Función Pública y la Secretaría de Economía, con diversos proveedores para un bien o servicio determinado. Estas dependencias establecen los términos y condiciones a los que deben sujetarse las entidades de la Administración Pública Federal y el procedimiento para la contratación; una vez que concluye el procedimiento, la formalización del contrato con el licitante adjudicado se conoce como contrato específico.

Por el tiempo en que se realizan las prestaciones, los contratos administrativos se dividen en: *a)* de ejecución inmediata, es decir, la entrega de los bienes o la prestación de los servicios la efectúan las partes en el momento de su

celebración; *b)* de ejecución instantánea, aquel que se agota en el momento en que se ejecuta; *c)* de ejecución diferida, se refiere a aquellos contratos que tanto sus derechos como obligaciones se cumplen en diversos momentos, por ejemplo, un contrato abierto de suministro de bienes.

Los contratos administrativos pueden ser *negociados*, es decir, las partes acuerdan las obligaciones que plasmarán en el instrumento jurídico y, *de adhesión*, en los que una de las partes (el estado) impone sus condiciones a la otra, un ejemplo de este último sería el pago de cuota en una caseta de cobro, pues si bien no se firma un contrato como tal, el conductor paga la cuota establecida y se le entrega un recibo que hace las veces de contrato y no existe la posibilidad de negociación, simplemente paga y pasa o no paga y no hace uso de la carretera federal.

En relación con las cualidades específicas del cocontratante, los contratos administrativos pueden ser *intuito personae*, se trata de contratos que para su celebración se exige al particular cumpla ciertas requisitos de carácter legal, técnico, financiero, económico o moral; en el caso de la administración pública y específicamente, servicios relacionados con tecnologías de la información y comunicación, objeto de estudio del presente trabajo, se exige a los proveedores contar con los recursos humanos, técnicos y financieros que garanticen el cumplimiento de la obligación adquirida, que el objeto social de su empresa esté estrechamente relacionado con el servicio a proporcionar.

En la administración Pública podemos distinguir los siguientes tipos de contratos administrativos: obra pública, adquisición de bienes muebles, arrendamiento de bienes muebles, enajenación de bienes muebles, prestación de servicios, suministro, préstamo y empréstito públicos. Además de otras figuras afines al contrato administrativo, como incorporación al empleo público y la concesión administrativa[8].

[8] *Ibidem* p. 183-198

1.3.8. Criterios para diferenciar el contrato administrativo

En el derecho administrativo existen diversos criterios para identificar los contratos administrativos, entre lo que destacan el criterio subjetivo, se dice que un contrato es administrativo cuando una de las partes forma parte de la Administración Pública de cualquiera de los tres niveles de gobierno y en ejercicio de sus atribuciones, contrata con un particular; el criterio legal considera contratos administrativos solamente aquellos que la Ley administrativa determine como tales, en el objeto de estudio, la LAASSP contempla los servicios de cómputo en la nube, por lo que estamos ante un contrato administrativo y; criterio objetivo, el cual está estrechamente relacionado con el objeto del contrato, es decir que el Estado contarte con particulares con el fin de satisfacer las necesidades de sus gobernados.

A diferencia del derecho civil, el derecho administrativo contempla el criterio de la cláusula exorbitante:9 El hecho de que los contratos administrativos sean celebrados por el Estado con particulares para satisfacer las necesidades de sus gobernados a través de la prestación de servicios diversos y cuya facultad está contemplada en Ley, justifica, en cierta medida, el uso de cláusula exorbitantes por parte del Estado, es decir, es el único momento en que pueden darse este tipo de cláusulas, en las que no interviene la voluntad del particular; ni siquiera del Estado, al ser condiciones previstas en el ordenamiento legal.

1.4. Los procedimientos de contratación Pública

1.4.1. ¿En qué consisten?[10]

Los procedimientos de contratación Pública son aquellos en los que el Estado, a través de una convocatoria pública se obliga a celebrar un contrato para la adquisición de un bien o contratación de un servicio, en la que puede participar

9“Contratos de la administración pública”, disponible en: *https://derechopublicoadministrativo.blogspot.com/2012/03/teoria-de-las-clausulas-exorbitantes.html* (fecha de consulta: 28 de marzo de 2019).

[10] Secretaría de la Función Pública, “1.3.1 Licitación pública (LOPSRM y LAASSP)”, 9 de mayo de 2017, disponible en: *https://www.gob.mx/sfp/acciones-y-programas/1-3-1-licitacion-publica* (fecha de consulta: 30 de julio de 2018).

cualquier persona física o moral, con una persona física o moral –llamada licitante- que cumpla los requisitos establecidos en la convocatoria, su actividad principal esté relacionada con el bien o servicio a contratar, para que el Estado en ejercicio de sus facultades, satisfaga una finalidad pública.

En cumplimiento del artículo 134 constitucional y las mejores prácticas internacionales, la Secretaría de la Función Pública considera fundamental que los entes públicos privilegien la celebración de licitaciones públicas en sus procedimientos de contratación, porque es el procedimiento que, como regla general, garantiza al Estado obtener las mejores condiciones de contratación en cuanto al precio, calidad y oportunidad. Sin embargo, existen excepciones a dicho procedimiento debidamente regulados en la ley de la materia: válidamente pueden utilizarse la adjudicación directa e invitación a cuando menos tres personas.

1.4.2. Sujetos obligados

La Secretaría de la Función Pública entiende como "sujetos" a los que les es aplicable tanto la LAASSP como la Ley de Obras Públicas y Servicios Relacionados con las Mismas (LOPSRM),11 así como a todos los servidores públicos que intervengan en los procesos de contratación de bienes, arrendamientos y contratación de servicios de cualquier naturaleza.12

Los sujetos obligados son:13 la Administración Pública Federal que es el conjunto de organismos o instituciones llamados a gestionar negocios, asuntos o

11"Secretaría de la Función Pública, Criterios Técnicos para la Contratación, por parte de los sujetos obligados, de adquisiciones y arrendamiento de bienes muebles, prestación de servicios, de obras públicas y servicios relacionados con las mismas, Diario Oficial de la Federación, 27 de septiembre de 2017, disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5498762&fecha=27/09/2017 (fecha de consulta: 27 de julio de 2018).

12 Instituto Mexicano para la Competitividad, *Guía práctica de compras públicas*, disponible en: *https://imco.org.mx/wp-content/uploads/2013/7/Guia_de_compras_publicas_011012.pdf* (fecha de consulta: 27 de julio de 2018)

13López Elías, José Pedro, *Aspectos jurídicos de la licitación pública en México*, México, UNAM, Instituto de Investigaciones Jurídicas, 1999, pp. 124-126, disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/2/543/9.pdf*. (fecha de consulta: 27 de julio de 2018)

intereses públicos, es decir, las instituciones facultadas para satisfacer las necesidades de los gobernados, para cubrir las garantías constitucionales a las que tiene derecho la sociedad. De conformidad con el artículo 1o. de la LAASSP, ésta regula las contrataciones que realicen:

I. Las unidades administrativas de la Presidencia de la República;
II. Las Secretarías de Estado y la Consejería Jurídica del Ejecutivo Federal;
III. La Procuraduría General de la República;
IV. Los organismos descentralizados;
V. Las empresas de participación estatal mayoritaria y los fideicomisos en los que el fideicomitente sea el Gobierno Federal o una entidad paraestatal, y
VI. Las entidades federativas, los municipios y los entes públicos de unas y otros, con cargo total o parcial a recursos federales, conforme a los convenios que celebren con el Ejecutivo Federal.

El particular. También llamado “administrado”, comprende no sólo a las personas físicas sino a las personas morales, quienes se obligarán ante el Estado para coadyuvar con éste en el cumplimiento de sus obligaciones constitucionales para con sus gobernados. A los particulares que tienen obligaciones contractuales con el Estado, la Ley los denomina “proveedores” y “contratistas”. Los primeros son quienes celebran contratos de adquisiciones, arrendamientos o servicios, mientras que los segundos son quienes celebran contratos de obras públicas y de servicios relacionados con las mismas.

1.4.3. Medio-formas de realizarse

La legislación federal en la materia contempla, en su artículo 26Bis tres posibles métodos para llevar a cabo procedimientos de contratación de acuerdo con los medios utilizados:

Presencial. Procedimiento en el cual la junta de aclaraciones, el acto de presentación y apertura de proposiciones y el acto de fallo, se realizarán de manera presencial con o sin asistencia de los licitantes; en caso de que se realice sin

presencia de los licitantes, en la convocatoria debe preverse que éstos podrán enviar sus proposiciones por mensajería o servicio postal.

Electrónica. En la cual exclusivamente se permite la participación de los licitantes a través de CompraNet. La junta de aclaraciones, el acto de presentación y apertura de proposiciones y el acto de fallo, se realizan a través de CompraNet y sin la presencia de los licitantes.

Mixta. En la cual los licitantes, a su elección, participan en forma presencial o electrónica y la junta de aclaraciones, el acto de presentación y apertura de proposiciones y el acto de fallo se llevarán a cabo tanto de manera electrónica como presencial.

Es importante señalar que los tres tipos de procedimiento pueden realizarse por cualquiera de los tres medios anteriores; sin embargo, la Ley prevé que, si la convocante se encuentra certificada como unidad compradora en el sistema CompraNet, invariablemente deberá realizar todos los procedimientos de licitación por medio electrónico.

1.4.4. Licitación pública

Para la compra de bienes y contratación de servicios, el método de contratación que fomenta primordialmente la transparencia y la competencia es la licitación pública, además, así lo expresa el artículo 134 constitucional. Este procedimiento consiste en una convocatoria dirigida a todas aquellas personas, cuya actividad principal esté estrechamente relacionada con el bien o servicio a contratar y con un posible interés en presentar ofertas.

La licitación fomenta la competencia porque varios proveedores del bien o servicio tienen la posibilidad de concurrir y ofrecer lo que consideran la mejor combinación precio/calidad para ganar el contrato. Para aquellas circunstancias excepcionales en las que la licitación no resulte adecuada o viable, por ejemplo, si hay una necesidad urgente, si se requiere la confidencialidad porque se involucra la defensa o seguridad del Estado o si sólo hay un posible vendedor, existen al menos dos métodos alternativos de contratación pública: la invitación restringida a un número específico de proveedores y la adjudicación directa.

Las buenas prácticas señalan que:14 *a)* cuando hay múltiples proveedores del mismo bien o servicio, es decir en un mercado con alta competencia y, por ende, donde los precios tienden a ser más estables porque ningún proveedor tiene la capacidad de cambiar el precio por sí solo, la licitación pública es el método más indicado para asegurar el mejor precio; *b)* cuando hay pocos proveedores y éstos tienen poder de mercado, y es el Gobierno quien compra una cantidad importante de las existencias, lo mejor es utilizar la adjudicación directa; sin embargo, en este procedimiento confluyen factores diversos, mismos que se explicarán más adelante, pero es importante señalar que la adjudicación directa puede ser por "monto" o "causa", y *c)* cuando hay poca oferta, pero el Gobierno por su volumen de compras visualiza que en el mediano plazo tiene la capacidad de desarrollar proveedores, debe buscar alterar el mercado a su favor para fomentar la entrada de nuevos competidores a través del diseño de los eventos.

Para Serrano Rodríguez la licitación pública "constituye el medio idóneo para la contratación administrativa y se fundamenta en el doble propósito de lograr las mejores condiciones técnicas y económicas para la Administración Pública".[15] "La licitación, desde el punto de vista administrativo, es considerada como un procedimiento administrativo por el cual la Administración Pública Federal elige cocontratante a la persona, física o moral que le ofrece las condiciones más convenientes para el Estado".[16]

1.4.5. Invitación a cuando menos tres personas

Es aquel procedimiento de contratación administrativa en el que solo intervienen las personas que han sido invitadas directamente por el Estado a participar en el procedimiento; de ellos, se elegirá al que resulte más conveniente, de acuerdo con los requisitos impuestos por la dependencia o entidad responsable de la contratación.

14*Ibidem*, p. 26.

[15] Serrano Rodríguez, Carlos Eduardo, *La contratación administrativa*, San José, Universidad de Costa Rica, 1991, p. 38.

[16] Sala, Vicente, *Diccionario latino-español*, París, Librería de Garnier Hermanos, 1873, p. 476.

Se trata, pues, de una facultad discrecional del Estado para elegir a su cocontratante a través de la invitación a determinadas personas; sin embargo, esto no implica que el Estado tenga prerrogativas de contratación arbitrarias, ya que está obligado a cumplir con los requisitos que le imponen los ordenamientos, además tiene la obligación de realizar la invitación a personas reconocidas por su capacidad para cumplir con la entrega de los bienes o con la presentación de los servicios requeridos. Su característica principal radica en que la invitación se dirige a personas cuyas actividades comerciales o profesionales están relacionadas con los bienes o servicios objeto del contrato a celebrarse.[17]

Para Manuel Lucero Espinosa, aun cuando el llamado no se hace públicamente, las dependencias y entidades están facultados para invitar a personas que reconocidamente sean consideradas como capaces para cumplir con la entrega de bienes o prestación de servicios o la realización de obras públicas, pues como lo menciona Escola, "*la licitación privada no debe ser una oposición entre personas sin aptitud o competencia, sino entre quienes reúnan esas condiciones, para que entre ellas se elija la mejor oferta*".18

El procedimiento de invitación a cuando menos tres personas es un procedimiento en el que, al igual que la licitación pública existe competencia e igualdad entre los licitantes; garantizando las mejores condiciones de contratación; la diferencia sustancial radica en que los invitados a participar en el procedimiento son previamente seleccionados considerando el objeto social, el cual debe estar estrechamente relacionado con el bien o servicio a contratar.

De conformidad con la LAASSP, la selección del procedimiento de excepción que realicen las dependencias y entidades deberá fundarse y motivarse, dependiendo las condiciones, en criterios de economía, eficacia, eficiencia, imparcialidad, honradez y transparencia para obtener las mejores condiciones para el Estado. El acreditamiento del o los criterios en los que se funda; así como la justificación de las razones por las cuales se eligió el procedimiento de invitación y

[17] Sala, Vicente, *Diccionario latino-español*, París, Librería de Garnier Hermanos, 1873, p. 476.
18Lucero Espinosa, Manuel, *La licitación pública*, 4a. ed., México, Porrúa, 2009, pp. 37-39.

constar por escrito y ser firmado por el titular del área usuaria o requirente de los bienes o servicios.

Las dependencias y entidades tienen la obligación de invitar a personas que cuenten con capacidad de respuesta inmediata, los recursos técnicos y financieros y cuyas actividades comerciales o profesionales estén relacionadas con los bienes o servicios objeto del contrato a celebrarse. Estos requisitos deben plasmarse en la convocatoria respectiva y derivan de la investigación de mercado que se realice, la cual arroja el número de proveedores existentes en el mercado, el precio promedio, la capacidad de respuesta, el tiempo de entrega y la calidad, entre otros.

1.4.5.1. Características específicas

La invitación con los requisitos que deben cumplir los licitantes se publica, para fines informativos, en el sistema CompraNet y en la página de Internet de la Convocante, , ya que, al tratarse de una “invitación restringida” solamente podrán participar las personas que han sido invitadas, debiendo ser como mínimo tres, el número de invitados dependerá del resultado de la investigación de mercado, seleccionando, preferentemente, a aquellos que se encuentren inscritos en el padrón de proveedores y contratistas que administra la Secretaría de la Función Pública. Dependiendo del tipo de procedimiento (presencial, electrónico o mixto) el acto de presentación y apertura de proposiciones puede realizarse con o sin licitantes; pero la convocante tiene la obligación de invitar al órgano interno de control.

Para proceder a la adjudicación, lo ideal es que la convocante cuente con un mínimo de tres proposiciones susceptibles de analizarse técnicamente; sin embargo, si no se cumple con el mínimo de proposiciones, la Ley faculta a la convocante para declarar desierta la invitación o continuar con el procedimiento y evaluar las proposiciones presentadas. De hecho, si solamente contara con una proposición y ésta cumple con los requisitos legales, administrativos, técnicos y económicos solicitados por la convocante, y el precio ofertado se encuentra dentro del presupuesto autorizado, se podrá adjudicar dicho procedimiento.

A diferencia de la licitación pública, en la invitación restringida, el plazo para presentar proposiciones, a partir de la entrega de la última invitación, se reduce a cinco días, mientras que en la licitación pública es de quince días. Otra diferencia significativa es que, mientras que en la licitación pública es obligatorio realizar al menos una junta de aclaraciones para atender las dudas que pudieran tener los licitantes, en la invitación restringida puede no haber junta de aclaraciones, por lo que el plazo entre la entrega de la última invitación y presentación de ofertas se reduce a cinco días, lo que garantiza contar con los bienes y/o servicios en menor tiempo.

Por último, un aspecto fundamental que permite definir si se realizará un procedimiento restringido, radica en los montos de actuación autorizados a cada dependencia o entidad, según lo señalado en el anexo 9 del Presupuesto de Egresos de la Federación para el ejercicio fiscal que corresponda. En dicho anexo, se establecen los montos máximos de adjudicación directa al amparo del artículo 42 de la LAASSP, así como el monto máximo de adjudicación por invitación a cuando menos tres personas.

Los montos de actuación facultan a las dependencias y entidades a llevar a cabo procedimientos de contratación distintos a la licitación pública, en todo momento buscando las mejores condiciones y siempre y cuando, dichas contrataciones se apeguen a los principios constitucionales de eficiencia, eficacia, economía, transparencia y honradez.

1.4.6. Adjudicación directa

La adjudicación directa es un procedimiento que se realiza, en la mayoría de las ocasiones sin que los licitantes compitan entre sí, adjudicándose el contrato a un proveedor que ha sido preseleccionado para tales efectos por la dependencia o entidad. Es el medio más sencillo para el establecimiento de acuerdos de voluntades entre el Estado y el particular cocontratante y contempla una gran cantidad de ventajas para obtener las mejores condiciones para el contratante. Se trata de un procedimiento facultativo del Estado, pues éste puede elegir de manera directa y discrecional a la persona que ejecutará las obligaciones contractuales,

siempre y cuando dicho procedimiento se encuentre establecido en un ordenamiento jurídico determinado.

Por esta razón, debe considerarse como parte de los procedimientos restrictivos y no un sistema de libre elección. Es decir, la contratación directa no puede realizarse de manera arbitraria, sino que la persona elegida para contratar debe ser la idónea y con la mayor capacidad para el cumplimiento del contrato.

La contratación directa goza de diversas características, entre las cuales destacan: la facultad de concurrencia u oposición de ofertas; la facultad del Estado para solicitar libremente la presentación de una oferta a quien le parezca conveniente para ello, y la facultad de la administración de contratar libremente, aun en los casos en que se requiera la solicitud de tres ofertas, y siempre bajo la estricta responsabilidad del titular del área contratante en la dependencia o entidad.

Este procedimiento se encuentra regulado por la LAASSP en sus artículos 40, 41 y 42 y; 71 y 72 de su Reglamento; siempre deberá fundarse y motivarse en criterios de economía, eficacia, eficiencia, imparcialidad, honradez y transparencia en busca de las mejores condiciones para el Estado.

A diferencia de la licitación pública, en este procedimiento el área requirente debe acreditar los criterios señalados en el párrafo que antecede a fin de demostrar que la adjudicación directa, en comparación con la licitación pública es el procedimiento idóneo para allegarse de los bienes o servicios que el ente público requiere para satisfacer las necesidades de la sociedad, así como la justificación de las razones en las que se sustente dicho procedimiento.

Para llevar a cabo este procedimiento, el ente público invitará a personas que cuenten con capacidad de respuesta inmediata, recursos técnicos, financieros y humanos para el cumplimiento de la obligación y, cuyas actividades comerciales o profesionales estén relacionadas con los bienes o servicios objeto del contrato.[19].

Ahora bien, la legislación contempla dos supuestos esenciales a considerar para llevar a cabo la adjudicación directa: adjudicación directa por “causa” y

[19] Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 2014, Diario Oficial de la Federación México.

adjudicación directa “por monto”. En la primera, independientemente del importe al que ascienda el bien o servicio a contratar, si dicha contratación encuadra en alguno de los supuestos normativos del artículo 41 de la LAASSP, ésta podrá llevarse a cabo cumpliendo con una serie de requisitos que se detallan más adelante, y en la segunda, la condición principal es que el importe de los bienes a adquirir o servicios a contratar no rebasen el monto de actuación autorizado por el Comité de Adquisiciones, Arrendamientos y Servicios de la dependencia o entidad según lo establecido por el Presupuesto de Egresos de la Federación.

Las contrataciones realizadas al amparo del artículo 41 de la Ley, deben cubrir los siguientes requisitos: justificación en la que se detalle con precisión los bienes o servicios a contratar, plazo, lugar y condiciones para la entrega de los bienes o prestación de los servicios, el resultado de la investigación de mercado, fundamentos y motivos para llevar a cabo la adjudicación directa, monto aproximado y forma de pago, la persona (física o moral) propuesta para contratar, el acreditamiento del o los criterios para llevar a cabo la contratación (siempre en relación al procedimiento, es decir, por qué resulta idónea la contratación por adjudicación directa y no por licitación pública), requisición de bienes y/o servicios, suficiencia presupuestal y, en el caso de bienes, la constancia de no existencia de éstos en el almacén.

1.4.6.1. Supuestos normativos del artículo 41 de la Ley

La normativa federal permite a la Administración Pública Federal realizar contrataciones mediante excepciones a la licitación, mediante el procedimiento de adjudicación directa, siempre y cuando el bien a adquirir o el servicio a contratar “encuadre” en alguno de los siguientes supuestos normativos.

La fracción I del artículo es comúnmente utilizada en aquellas contrataciones que involucran derechos de autor, patentes, marcas, licenciamiento exclusivo o cuando solamente existe un posible oferente; para acreditar dicho supuesto, resulta necesario acompañar las documentales que lo acrediten, en el *argot* de adquisiciones se le conoce como *apostilla,* el área requirente es la encargada de

presentar los títulos, permisos, reserva de derechos, títulos de propiedad o el documento que acredite la titularidad, la dictaminación es facultad del Comité de Adquisiciones, Arrendamientos y Servicios de la dependencia o entidad.

Si el bien o servicio a contratar pone en riesgo el orden social, la economía, los servicios públicos, la salubridad, la seguridad o el ambiente de alguna zona o región del país como consecuencia de caso fortuito o de fuerza mayor, la fracción II es el fundamento indicado para llevar a cabo la contratación, en este caso, es el titular del área requirente quien debe dictaminar la procedencia de la contratación.

Cuando existan circunstancias que puedan provocar pérdidas o costos adicionales importantes, cuantificados y justificados, puede recurrirse a la fracción III, conocida en las compras gubernamentales como “adhesión”; la característica primordial de este supuesto radica en que las dependencias o entidades pueden celebrar contrato con un proveedor previamente adjudicado por la misma u otra dependencia o entidad como consecuencia de un procedimiento de licitación, siempre y cuando el proveedor acepte otorgar al ente público las mismas condiciones y precios que a quien realizó la licitación; para ello, el área requirente debe demostrar, con la investigación de mercado, los ahorros económicos al contratar con esta opción, además de la eficiencia, transparencia, imparcialidad, honradez y/o eficacia en comparación con la licitación pública; dicho supuesto es dictaminado por el Comité de Adquisiciones, Arrendamientos y Servicios.

Las contrataciones que se realicen con fines exclusivamente militares o para la Armada podrán realizarse bajo este supuesto, fracción IV, y será el titular del área requirente el responsable de su dictaminación.

Si por fuerza mayor o caso fortuito, no es posible obtener bienes o servicios mediante el procedimiento de licitación pública en el tiempo requerido para atender la eventualidad de que se trate, procede invocar la fracción V; también es facultad del titular del área requirente y debe documentarse con notas periodísticas, declaratorias de emergencia o cualquier otro documento emitido por autoridad competente que demuestre indubitablemente el caso fortuito o fuerza mayor, ejemplo de ello, es el brote de epidemia AH1N1, ocurrido en México en 2009.

Se podrá invocar la fracción VI cuando se haya rescindido un contrato, previamente adjudicado mediante licitación pública, siempre y cuando la propuesta del licitante que haya obtenido el segundo lugar en el procedimiento no rebase el 10% de la propuesta ganadora. En este supuesto, la dictaminación es responsabilidad del área requirente.

La fracción VII procede cuando se haya declarado desierta una licitación pública, siempre y cuando se conserven los requisitos solicitados en el procedimiento de licitación. La dictaminación será responsabilidad del área requirente o usuaria.

En el caso de la fracción VIII procede la contratación para adquirir bienes de una marca determinada, si el área requirente justifica fehacientemente las razones para ello, la dictaminación de este supuesto está a cargo del Comité de Adquisiciones, Arrendamientos y Servicios de la dependencia o entidad.

Dada la naturaleza de los bienes, si se trata de perecederos, granos y/o productos alimenticios básicos o semiprocesados, semovientes, podrá contratarse invocando el supuesto de la fracción IX, cuya responsabilidad será del área usuaria o requirente.

Al tratarse de servicios de consultorías, asesorías, estudios o investigaciones, se podrá contratar al amparo de la fracción X cuando la información que se deba proporcionar a los licitantes para la elaboración de su proposición, se encuentre reservada en los términos establecidos en la Ley Federal de Transparencia y Acceso a la Información Pública, la dictaminación corresponde al Comité de Adquisiciones, Arrendamientos y Servicios y la evaluación de proposiciones deberá hacerse, preferentemente, mediante el mecanismo de puntos o porcentajes.

Será responsabilidad del área usuaria o requirente la adquisición de bienes arrendamientos o servicios en los casos en que el proveedor pertenezca a un grupo de campesinos o grupos urbanos marginados, como personas físicas o morales; fracción XI y la dictaminación será responsabilidad del área usuaria o requirente.

Cuando se trate de adquisición de bienes que realicen las dependencias y entidades para su comercialización directa o para someterlos a procesos

productivos que las mismas realicen en cumplimiento de su objeto o fines propios expresamente establecidos en el acto jurídico de su constitución, podrá realizarse la contratación al amparo de la fracción XII; la dictaminación será responsabilidad del Comité de Adquisiciones, Arrendamientos y Servicios; un ejemplo de lo anterior son los productos que comercializan las tiendas del IMSS e ISSSTE.

La fracción XIII aplica cuando se trate de adquisiciones de bienes provenientes de personas que, sin ser proveedores habituales, ofrezcan bienes en condiciones favorables, por encontrarse en Estado de liquidación o disolución, o bien, bajo intervención judicial; la dictaminación será responsabilidad del Comité de Adquisiciones, Arrendamientos y Servicios.

La fracción XIV es comúnmente utilizada por los entes públicos para contratar a personas físicas, siempre que los servicios prestados sean realizados por ellas mismas sin requerir de la utilización de más de un especialista o técnico; la dictaminación, corresponde al Comité de Adquisiciones, Arrendamientos y Servicios.

En el caso de contratación de servicios de mantenimiento de bienes muebles en los que no sea posible precisar su alcance, establecer las cantidades de trabajo o determinar las especificaciones correspondientes, podrá contratarse invocando la fracción XV; la dictaminación de la procedencia de excepción será facultad del Comité de Adquisiciones, Arrendamientos y Servicios.

La fracción XVI procede si el objeto del contrato es el diseño y fabricación de un bien que sirva como prototipo para efectuar las pruebas que demuestren su funcionamiento; la dictaminación será facultad del Comité de Adquisiciones, Arrendamientos y Servicios.

La fracción XVII procede cuando se trate de equipos especializados, sustancias y materiales de origen químico, físico-químico o bioquímico, para ser utilizados en actividades experimentales requeridas en proyectos de investigación científica y desarrollo tecnológico, siempre que dichos proyectos se encuentren autorizados por quien determine el titular de la dependencia o el órgano de Gobierno de la entidad; la dictaminación será facultad del Comité de Adquisiciones, Arrendamientos y Servicios.

La fracción XVIII es poco recurrida y se utiliza cuando se acepte la adquisición de bienes o la prestación de servicios a título de dación en pago, la dictaminación será facultad del Comité de Adquisiciones, Arrendamientos y Servicios.

También será el Comité de Adquisiciones, Arrendamientos y Servicios el que dictamine la procedencia de la fracción XIX para aquellas adquisiciones de bienes y servicios relativos a la operación de instalaciones nucleares.

Por último, la fracción XX opera cuando se trate de la suscripción de contratos específicos que deriven de un contrato marco; en este supuesto será el titular del área requirente o usuaria quien dictamine la procedencia. Cabe resaltar que los contratos marco vigentes se publican en la página del sistema electrónico de información pública gubernamental sobre adquisiciones, arrendamientos y, servicios (CompraNet), administrado por la Oficialía Mayor de la Secretaría de Hacienda y Crédito Público.

En estas contrataciones, el titular del área responsable de la contratación, a más tardar el último día hábil de cada mes, enviará al órgano interno de control en la dependencia o entidad de la que se trate, un informe relativo a los contratos formalizados durante el mes inmediato anterior, acompañado de una copia de la justificación y de un dictamen que contenga el análisis detallado de las razones para la adjudicación, considerando, en todo momento, el resultado de las proposiciones recibidas, los criterios de eficacia, eficiencia, economía, imparcialidad, honradez y transparencia.

1.4.6.2. Adjudicación directa por el monto a contratar

Como se mencionó en párrafos anteriores, la Ley, específicamente el artículo 42, prevé que las dependencias y entidades puedan contratar a través del procedimiento de adjudicación directa cuando el importe de cada operación no exceda los montos máximos que al efecto se establecerán en el Presupuesto de Egresos de la Federación. Para ello, existen diversas condiciones, la principal es que la contratación no se fraccione, seguida de contar con, al menos, tres

cotizaciones obtenidas máximo 30 días previos a la adjudicación y que el importe a contratar no rebase el monto máximo para adjudicación directa autorizado por el CAAS, de conformidad con el anexo 9 del Presupuesto de Egresos de la Federación.

Al igual que cualquier contratación, para que el área contratante dé inicio al procedimiento de contratación, el área requirente debe acompañar su solicitud con la requisición de bienes y/o servicios, suficiencia presupuestal y, en el caso de bienes, la constancia de no existencia de éstos en el almacén. El procedimiento puede realizarse ya sea de manera presencial, electrónica o mixta.

Una de las ventajas de realizar el procedimiento de adjudicación directa de forma electrónica, a través del sistema CompraNet, es que la dependencia o entidad podrá adjudicar el contrato aun cuando solamente reciba una cotización por el sistema, independientemente de si el procedimiento es cerrado o abierto a cualquier interesado.

Ahora bien, las dependencias y entidades deben, en este tipo de contratación, tener especial cuidado en observar lo que señala el artículo 42, en el sentido de que la suma de las contrataciones realizadas durante el ejercicio no rebase el 30% del monto total autorizado en el presupuesto global destinado a la adquisición de bienes y contratación de arrendamientos y servicios, ya que, como lo establece la Carta Magna, debe privilegiarse la licitación pública; esta circunstancia se reporta de manera trimestral al Comité de Adquisiciones, Arrendamientos y Servicios.

De igual forma, deben cuidar que las operaciones realizadas al amparo de este artículo no se fraccionen para ubicarlas en este supuesto de excepción, de ahí la importancia de planear, programar y, en su caso, consolidar las contrataciones. Es importante señalar que para que se considere que existe fraccionamiento de operaciones, deben configurarse las siguientes circunstancias: que todas las contrataciones estén fundadas en el artículo 42 y la suma de sus importes superen el monto máximo indicado en el Presupuesto de Egresos de la Federación para cada procedimiento de excepción; que los bienes o servicios objeto de las contrataciones sean exactamente los mismos; que las operaciones se efectúen en

un solo ejercicio fiscal; que el área contratante o el área requirente pudieron prever las contrataciones en un sólo procedimiento, sin que se haya realizado de esta forma, y las solicitudes de contratación se realicen por la misma área requirente y el área contratante sea la misma, o bien, el área requirente sea la misma y el área contratante sea diferente.

1.5. Aspectos básicos de la contratación pública del cómputo en la nube

El presente estudio versa sobre la importancia que reviste para la Administración Pública Federal el reforzar la contratación de servicios de cómputo en la nube, independientemente del procedimiento de contratación que se lleve a cabo para su formalización.

En función del progreso tecnológico que se registra a nivel internacional, el sector público también ha tenido que adecuarse al vertiginoso planteamiento de nuevas herramientas tecnológicas como es el caso del cómputo en la nube. En tal caso, el auge del cómputo en la nube es tan impresionante que, entre los expertos, ya es considerado como el nuevo nirvana de la computación.

A través de una estrategia de economía digital, el sector público ha conseguido otorgar el derecho a la protección de datos entre la población. De la misma forma, el aspecto jurídico ha tenido que evolucionar la normativa para regular el cómputo en la nube. Sin embargo, aunque los instrumentos internacionales en materia de protección de datos personales no vinculan jurídicamente a México, estos instrumentos han ejercido una importante influencia en la legislación mexicana.

De este modo, el 26 de enero de 2017 se publicó, en el *Diario Oficial de la Federación*, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados. A nivel normativo, esta Ley es de gran relevancia debido a que el sector público cuenta —por primera vez— con una legislación para la protección de la información.

Los fundamentos legales del derecho a la protección de los datos personales en México están regulados por la Ley Federal de Protección de Datos Personales

en Posesión de Particulares (LFPDPPP), la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y sus Lineamientos (LGPDPPSO), así como por las leyes estatales de protección de datos.

Particularmente, la LGPDPPSO tiene por objetivo distribuir competencias —en materia de protección de datos personales— entre el INAI, así como entre los organismos garantes de la Federación y las entidades federativas. De igual forma, la Ley General prevé algunas figuras clave para la protección de datos personales: Titular: persona física a quien corresponden los datos personales; Responsable: sujeto obligado por la LGPDPPSO que decide sobre determinado tratamiento de datos personales. Es decir, que determina el tipo de datos personales a tratar, la categoría de titular, las finalidades o usos a los que serán sometidos los datos personales, entre otras decisiones y; Encargado: persona física o jurídica, pública o privada, ajena a la organización del responsable, que trata datos personales a nombre y por cuenta de éste.

Por otra parte, la LGPDPPSO incluye diversos conceptos clave, entre ellos los datos personales, datos sensibles, tratamiento y, ciertamente, el cómputo en la nube. Al respecto, la Ley General lo describe como el modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

En otras palabras, el modelo de cómputo en la nube es aquel que facilita la operatividad gubernamental para afirmar la certeza jurídica de los servicios que ofrece este tipo de tecnologías. Justamente, el alcance y aplicación de la LGPDPPSO incluye cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos.

Precisamente para que el sector público lleve a cabo la contratación de cómputo en la nube, la LGPDPPSO señala que es la figura del responsable la que puede contratar o adherirse a servicios, aplicaciones e infraestructura, cuando el proveedor (encargado) cuente con políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables.

Sin embargo, aunque la LGPDPPSO apoya el argumento de que el acceso a la información pública es un derecho fundamental, lo cierto es que no siempre toda la información es accesible. Esto se debe a que la información puede ser reservada, lo que significa que se compromete la seguridad nacional o de cualquier persona; o bien, que la información es de acceso confidencial, la cual está protegida por el derecho fundamental a la privacidad.

Conjuntamente, para reforzar la protección de los datos personales, la Ley General se poya de los Lineamientos Generales de Protección de Datos Personales para el Sector Público,20 los cuales se refieren a los estándares que deben seguir los sujetos obligados para la protección de los datos.

A este respecto, los Lineamientos coadyuvan a la regulación para el almacenamiento de los datos del sector público en el cómputo en la nube. Asimismo, a través de ellos se argumenta que el sector público no está exento del uso de las tecnologías de la información para brindar un mejor servicio y atención a la ciudadanía. Dichos lineamientos apoyan el hecho de que las dependencias y entidades únicamente pueden transmitir datos personales mediante el consentimiento del titular, o en casos como la portabilidad de los datos.

En este sentido, por las características propias de la información y con lo que establece el artículo 2o. de los Lineamientos —los cuales establecen los parámetros, modalidades y procedimientos para la portabilidad de los datos personales—21 se señala que la portabilidad es la prerrogativa del titular a que se refiere el artículo 57 de la LGPDPPSO o los que correspondan en las legislaciones estatales en la materia, el cual plantea el tratamiento de datos personales vía electrónica en un formato estructurado y comúnmente utilizado, es decir, el titular en ejercicio de su derecho, puede obtener una copia de los datos objeto del tratamiento para seguir utilizándolos.

---

20 Lineamientos Generales de Protección de Datos Personales para el Sector Público, Diario Oficial de la Federación, México, 26 de enero de 2018.

21 *A*cuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. *Diario Oficial de la Federación*, México, 12 de febrero de 2018.

No obstante, cuando el tratamiento tiene como base un contrato, el titular tiene derecho a transmitir dichos datos personales —y cualquier otra información que haya facilitado— por medio de un sistema de tratamiento automatizado.

De la misma forma, el derecho a la portabilidad permite a las personas obtener los datos personales que han proporcionado a una entidad, empresa u organización responsable del tratamiento. Pero además abre la posibilidad, no sólo de obtener los datos y reutilizarlos, sino también de transmitirlos directamente a otro proveedor de servicios.[22]

Sin embargo, debido a que el derecho a la protección de datos es un derecho relativamente nuevo, es pertinente distinguir la aportación de este en contraposición con la portabilidad, tal como se muestra en la siguiente tabla:

Derecho a la protección de datos personales	**Derecho a la portabilidad de datos personales**	**¿Cómo se pueden adaptar mejor ambos conceptos en el cómputo en nube?**
Los datos personales pueden estar en documentos físicos y/o electrónicos.	Los datos personales que únicamente se encuentren en formatos electrónicos o automatizados.	La portabilidad refuerza el control de los datos personales, de modo que el tratamiento se efectúa por medios automatizados. Asimismo, se transmiten al responsable del tratamiento, siempre que el tratamiento se legitime con base en el consentimiento o en el marco de la ejecución de un contrato.

[22] Agencia española de Protección de datos, ¿Qué es el derecho a la portabilidad?, 2018, Disponible en: *https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad* (fecha de consulta: 27 de agosto de 2019)

Su ejercicio es independiente de la causa de legitimación del tratamiento de datos personales.	Se ejerce cuando el tratamiento se base exclusivamente en el consentimiento del titular o en un contrato.	Debido a que la portabilidad de los datos personales es un elemento que otorga mayor poder de control del interesado sobre sus datos personales, es conveniente que ambos enfoques se aproximen a lo que establece el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) en el sentido de que el interesado tiene derecho a recibir los datos personales que le conciernan, que haya facilitado a un responsable del tratamiento.
El titular tiene derecho de acceder a sus datos personales que obren en los archivos, registros, expedientes y/o sistemas en posesión del responsable.	Sólo son portables aquellos datos personales que el titular puede solicitar, en un formato estructurado y comúnmente utilizado, a un sistema en posesión de otro responsable.	Debido a que la portabilidad tiene por objetivo facultar a los interesados respecto del traslado, copia o transmisión de los datos personales de un entorno informático a otro. Sin embargo, es importante cuestionar si los datos que circulan de un responsable a otro —a instancia del interesado— deben ser exactos y

		limitados a las exigencias de este último.
El titular tiene derecho a acceder a todos sus datos personales que obren en los archivos, registros expediente y/o sistemas en posesión del responsable	Sólo son portables los datos que el titular proporciona directamente al responsable de forma activa y consciente y con los metadatos asociados al tratamiento de éstos.	En materia de transparencia, la portabilidad facilita la rendición de cuentas y la fiscalización en tiempo real. En este sentido es pertinente la publicación de directrices que faciliten al responsable y al encargado la orientación en la reproducir los datos.
El derecho de acceso a datos personales no implica la transferencia de estos a otro responsable.	En la portabilidad de los datos, una de las modalidades es que el titular puede solicitar la transmisión de sus datos personales, mediante un formato estructurado, hacia un sistema en posesión de otro responsable.	Es recomendable que ambos criterios se apeguen a lo que establece el Reglamento General de Protección de Datos (GDPR) respecto de la supresión determinando que la portabilidad de los datos no conlleva a la supresión de estos de manera automática. Es decir, el interesado puede seguir beneficiándose del servicio si así lo considera.
La reproducción de los datos personales se lleva a cabo por medio de copias simples, medios	La portabilidad la reproducción de los datos personales únicamente puede realizarse en un formato	Con el objetivo de llevar a cabo la reproducción de los datos más controlada, se sugiere establecerlos mediante un anexo para

electrónicos, sonoros, visuales, holográficos o cualquier otra tecnología.	estructurado y comúnmente utilizado, que implique la reutilización o aprovechamiento de estos.	solicitud de la reproducción. El anexo debe informar puntualmente lo referente a la reproducción de los datos. Asimismo, complementar con información adicional respecto de los fines y legitimación de la reproducción de los datos.

Cuadro 1. Derecho a la protección de datos personales y derecho a la portabilidad de datos personales

Fuente: Elaboración propia con información de los Lineamientos para la portabilidad de datos personales[23]

Del cuadro anterior destaca que, tanto la protección como la portabilidad de los datos son conceptos complementarios y que los beneficios de su aplicación pueden potenciarse al unificar el valor agregado de cada uno de ellos. Asimismo, se considera pertinente la unificación de ambos criterios a efecto de asegurar el cumplimiento de los propósitos del cómputo en la nube. Por ejemplo, al unificar criterios se reducirían los intervalos de control y de corrupción que existen en la Administración Pública Federal en correlación con la reducción de costos y tiempos del tratamiento de datos.

En estricto sentido, la dinámica de la normativa y el avance tecnológico ha posibilitado la transición a sistemas de interconectividad ciclópeos como el cómputo en la nube, en el que contribuye a la gestión de trámites y servicios a través de plataformas de datos personales como es el caso de la portabilidad.

En virtud de ello, la Administración Pública Federal puede direccionar su objetivo hacia un nuevo paradigma en el que la interacción entre el responsable y

[23] Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. 2018, México

el encargado de la información se sustente con la aplicación de una normativa definida, pero al mismo tiempo flexible que coadyuve a la eficiencia no sólo de la portabilidad de los datos sino de otros mecanismos de protección de datos como el cifrado, encriptado, o la interoperabilidad. De tal forma que en la práctica el responsable de los datos tenga pleno conocimiento del tratamiento de la información y que el encargado cumpla en términos de transparencia.

En este sentido, la LGPDPPSO puede mostrarse más flexible en el sentido de la especificidad de los términos cuando son expuestos en un contrato, como en el caso de que las cláusulas establezcan que los casos en los que el interesado tiene derecho a recibir los datos personales que le conciernan por haberlos facilitado al responsable del tratamiento, sin que éste se niegue a facilitarlos.

Lo anterior debido a que, en el artículo 10 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, se establece que el responsable no está obligado a almacenar, preservar, guardar, mantener o conservar todos los datos personales en su posesión en un formato estructurado y comúnmente utilizado, sólo para efecto de garantizar la portabilidad de éstos.

Finalmente, aunque los expertos señalan que el retroceso en la normativa mexicana se debe, en gran parte, a que México se limita a reproducir lo que otros países como Estados Unidos y la Unión Europea generan en materia de normativa y de certificación, el marco jurídico ha mejorado dos aspectos: la imposición de deberes y obligaciones para el tratamiento de datos personales y el desarrollo tecnológico para recabar, procesar, tratar, transmitir o remitir grandes volúmenes de información en tiempo real. Ambos aspectos han coadyuvado a reducir la brecha jurídica a través de los siguientes hechos:

- Anteriormente, la normativa no promovía la aplicación a la protección de datos personales en el sector público.
- La legislación en materia de protección de datos personales en el sector público no garantizaba la totalidad de los derechos como ahora lo hacen los derechos ARCO (acceso, rectificación, cancelación y oposición).

Por lo tanto, los resultados en el corto plazo y de las adecuaciones que se hagan a la Ley General contribuirán a que el responsable de la información y el encargado tengan conocimiento, en términos de transparencia, del uso de la información y estén al tanto de lo que sucede con ésta al término de un contrato de servicios de cómputo en la nube.

1.5.1. Propuestas para la protección de datos personales en los procedimientos de contratación pública de cómputo en la nube

En materia legal, los servicios o aplicaciones de almacenamiento en la nube contemplan la protección de datos personales. Así, el artículo 64 de la LGPDPPSO establece que, para la adhesión en el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, el responsable y el encargado deben apegarse a las condiciones o cláusulas generales de contratación. Sin embargo, también establece que sólo podrán utilizar aquellos servicios en los que el proveedor cumpla con condiciones específicas.

La legislación ordena a los responsables del tratamiento de datos personales en servicios, aplicaciones e infraestructura en la nube, utilizar determinados servicios sólo si el proveedor cumple con determinadas políticas de protección de datos personales como transparentar la contratación, abstenerse de asumir la titularidad de los datos y garantizar la confidencialidad.

Por otra parte, respecto de los mecanismos, el propio artículo expresa que los proveedores deben proteger los datos a través de medidas de seguridad, establecer límites y garantías para la supresión de los datos personales, así como impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso.

Por ello, las siguientes tablas tiene por objetivo mostrar un planteamiento complementario de las condiciones generales en el tratamiento de datos

personales, y de esta manera coadyuvar a mejorar la relación entre el responsable y el encargado de servicios de la nube.[24]

Condiciones que el responsable debe cumplir[25]	Comentario
a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;	Se requiere que el responsable tenga pleno conocimiento de las políticas de protección de datos personales con el objeto de identificar su homologación con los principios y deberes contenidos en la LGPDPPSO. La afectación de esta condición es que comúnmente la figura del responsable no quiere asumir los compromisos respecto de la protección de datos personales.
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;	Es decir, para no afectar la prestación del servicio contratado, es conveniente que las partes emitan un acuerdo de consentimiento expreso para transparentar la información.
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio.	Esta condición se refiera a que bajo ninguna situación la información que procesa y/o almacena el encargado podrá considerarla de su propiedad o titularidad. En tal sentido, se recomienda que en caso de que el

[24] Ricard Martínez “LOPD y Seguridad”, Cloud en el nuevo reglamento mexicano de protección de datos, España, 2011. Disponible en: *http://lopdyseguridad.es/11* (fecha de consulta: 27 de agosto de 2019).

[25] Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, *Diario Oficial de la Federación, México*, 26 de enero de 2017, artículo 64.

	encargado realice el procesamiento de datos, definir que la propiedad de la información resultado del procesamiento de datos pertenecerá al responsable.
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.	Debido a la importancia que representa la confidencialidad en la protección de datos, es fundamental que no sólo se guarde la confidencialidad, como lo establece la presente condición, sino que es pertinente que también se guarde información adicional, siempre que se mantenga por separado. Asimismo, sería recomendable que, mediante un acuerdo de confidencialidad, integrado como anexo dentro del contrato, se implementen las medidas técnicas y organizativas necesarias para garantizar el cumplimiento global de la confidencialidad.

Cuadro 2. Condiciones generales en el tratamiento de datos personales

Fuente: Elaboración propia con información de la LGPDPPSO

Mecanismos mínimos con los que el encargado debe contar26	Comentarios
a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;	Si bien el aviso de privacidad es una herramienta para la protección de datos que se debe poner a disposición de los interesados, hacerse público y difundirse, es conveniente que en la presente condición se agregue la revisión del formato de autoevaluación de avisos de privacidad que propone el INAI. Esta herramienta de autoevaluación tiene como objetivo único que el responsable verifique que sus avisos de privacidad contengan los elementos informativos obligatorios que señalan los artículos 27 y 28 de la LGPDPPSO, los relativos de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LG) y los artículos 11, 14, 15, 16 y 19 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales (Lineamientos de Portabilidad).27

26Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, *Diario Oficial de la Federación, México*, 26 de enero de 2017, artículo 64.

27 Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales Guía para el aviso de privacidad, Disponible en: *http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx*. (fecha de consulta: 27 de agosto de 2019).

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se proporciona el servicio;	Se considera conveniente que en esta condición se agregue un mecanismo de control absoluto sobre fines y usos limitando de la información, en el cual el poder de disposición de la información por parte del encargado se limita a aspectos meramente técnicos.
c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;	Es conveniente que el responsable obligue al encargado a implementar mecanismos más elaborados de seguridad para la protección que garanticen la integridad y confidencialidad de la información. Entre más eficaces sean las medidas de seguridad, las partes interesadas podrán tener decisiones más efectivas para proteger los defectos personales. Por ejemplo, la aplicación de directrices de medidas de seguridad integrados en el anexo técnico.
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio proporcionado al responsable y que este último haya podido recuperarlos, y	Es un derecho del titular solicitar la supresión de sus datos, cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Sin embargo, no es tan fácil que se cumpla esta garantía, ya que en ocasiones el titular no podrá ejercer dicho derecho, cuando el responsable considere necesario el tratamiento de sus datos.

	En este sentido, se propone fijar condiciones que coadyuven a garantizar la supresión de datos, previas a la finalización del contrato, de manera que no se afecten los derechos de los interesados.
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.	Esta disposición posee un valor añadido fundamental, ya que no sólo defiende el acceso a la información por parte de personas que no cuentan con el permiso, sino, por otra parte, hace del conocimiento al responsable en caso de que se haya incumplido. De tal modo que esta dicotomía coadyuva a compactar el canal de comunicación entre el responsable y el encargado, derivando en una garantía sólida para la protección de los datos.

Cuadro 3. Mecanismos de control por parte del encargado

Fuente: elaboración propia con información de la LGPDPP.

Además de las consideraciones anteriores, se recomienda que los responsables y encargados del tratamiento de datos personales, reconozcan que a medida que la tecnología avanza, la seguridad en la nube podría considerar otros aspectos para ampliar las opciones de protección de información, para que, en su momento, las autoridades correspondientes, como es el caso del Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI), participen en la ampliación del régimen jurídico aplicable a la seguridad en la nube.

Es decir, ya que el avance tecnológico es superior a la aportación en materia legal, los modelos y los supuestos de seguridad se enfrentan al reto de superar el principio de protección tradicional de dispositivos de seguridad. Por lo que es

recomendable, en el caso del sector público reevaluar el enfoque normativo de protección tradicional, con el fin de evolucionar las capacidades de seguridad avanzada tales como la encriptación, autenticación, autorización y geolocalización.

Por tal motivo, aunque las condiciones o cláusulas generales de contratación expuestas en el artículo 64 de la LGPDPPSO son una importante aportación reguladora, también pone sobre la mesa la necesidad de actuación por parte de las autoridades competentes en el sentido de adecuar el marco normativo del sector público para ajustarse al avance tecnológico, ya que jurídicamente se tienen vacíos legales que no consideran casos específicos.

En este sentido, la normatividad mexicana determina mínimas consecuencias jurídicas, que a su vez limitan el alcance de la protección en el tratamiento de datos personales. Tal es el caso de la protección de la información del cómputo en la nube, tema que requiere considerar otros aspectos más contundentes como el de la seguridad.

Por ejemplo, la fortaleza del cómputo en la nube radica en los patrones de diseño, ya que por medio de ellos es posible la creación de aplicaciones confiables, escalables y seguras. No obstante, esta fortaleza se ha consolidado y definido por los cambios y adaptaciones de la seguridad de la información antes y después del cómputo en la nube, tal como se muestra el siguiente cuadro comparativo:28

Sin nube	Seguridad en la nube
Centros de datos internos	Centros de datos terceros
Costos iniciales elevados	Bajas inversiones iniciales en infraestructura
Escalado lento	Rápidamente escalable
Menor eficiencia	Utilización eficiente de los recursos

28 Amazon Web Services, Seguridad en la nube de AWS, Infraestructura y servicios que elevan su seguridad en la nube Disponible *https://aws.amazon.com/es/security/introduction-to-cloud-security* (fecha de consulta: 27 de agosto de 2018)

Proceso de comercialización más prolongado	Reducción del proceso de comercialización
Mayor costo	Costo basado en el uso

Cuadro 4. Seguridad de la información antes y después del cómputo en la nube

Fuente: Elaboración propia con información de Seguridad en la nube de AWS.

Si bien, la tabla muestra aspectos a considerar en materia financiera y tecnológica que giran en torno a la seguridad en la nube, lo cual constituye una prioridad para quien está a cargo de la información, es útil considerar los siguientes aspectos que refuerzan la contratación de servicios de la nube para la protección de datos:

Renombre del proveedor. Los proveedores de servicios de nube son los principales oferentes de soluciones que proporcionan las herramientas para mejorar la seguridad de los datos y el acceso a las aplicaciones en línea. No obstante, estos proveedores ofrecen también soluciones completas para el despliegue, la distribución y la aceleración de aplicaciones, además de herramientas que permiten a sus clientes disfrutar de una mayor visibilidad y un mayor conocimiento de la experiencia de los usuarios finales.

Confidencialidad. Como parte de los compromisos del proveedor de servicios de la nube está el garantizar la confidencialidad utilizando la información y los datos exclusivamente para los servicios contratados. Asimismo, la confidencialidad circunscribe el compromiso por parte del capital humano a su cargo, en el sentido de mantener la reserva de los servicios prestados. Por otra parte, en materia legal la confidencialidad es fundamental para la elaboración y cumplimiento del contrato, cuyas cláusulas deben ser muy específicas respecto de las medidas técnicas y organizacionales que el proveedor tiene previsto implantar para garantizar la seguridad de los datos.

Integridad en los servicios de seguridad. La principal inquietud en el ámbito público o privado es la forma de protección de la información en la nube. Esta expectativa es comprensible por los riesgos a los que la información es expuesta,

motivo que obliga a poner especial atención en los aspectos como el almacenamiento seguro en la nube, las amenazas de seguridad, así como el grado de protección que depende de cómo se implementan las medidas generales de protección de datos. En este sentido, las recomendaciones legales por parte de los expertos coinciden en que la mayoría de las cuestiones legales asociadas al cómputo en nube se suele resolver durante la evaluación de la oferta de proveedores o en la negociación del contrato.29

Otra recomendación entre las partes es revisar a detalle las cláusulas particularmente a sus derechos y obligaciones respecto de las notificaciones en caso de vulneración de seguridad, transferencia de datos, creación de obras derivadas, cambio de control y acceso a los datos por parte de las autoridades legislativas[30].

Por último, en un supuesto de interrupción en la subcontratación de infraestructura interna crítica, las partes deben considerar detenidamente si las limitaciones estándar de la responsabilidad se ajustan a las respectivas asignaciones de responsabilidad considerando el uso de la nube por las partes, o las responsabilidades concernientes a la infraestructura[31].

El sector público hace uso del cómputo en la nube con el objetivo de resguardar los datos personales de los que disponen en manos de terceros. No obstante, durante en el cruce de la información hay diferentes puntos de intersección, mismos que cuentan con sus respectivos canales de acceso. Por tanto, la seguridad de estos puntos está en permanente vulneración, por lo que en el proceso de contratación de servicios en la nube no se debe dejar pasar los siguientes aspectos:

---

29 European Union Agency For Cibersecurity, Beneficios, riesgos y recomendaciones para la seguridad de la información, Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish. (fecha de consulta: 27 de agosto de 2019).

30 *idem*

31 idem

Determinar el tipo de contrato. Con el fin de que las partes tengan pleno conocimiento de las cláusulas y consideraciones del servicio de cómputo en la nube, es preciso elaborar un contrato que sea muy claro en términos de derechos, obligaciones y responsabilidades de las partes, licenciamiento, precios, facturación y pago, penalizaciones, confidencialidad, protección de datos, propiedad intelectual, modelo de Gobierno, subcontratación, gestión de cambios, resolución de controversias, lugar y alcance de los servicios.

Cumplimiento de normatividad. Aunado al cumplimiento del contrato *per se*, es preciso que el enfoque contractual garantice el cumplimiento de la normativa de protección de datos personales de servicios de la nube. En el caso de la Administración Pública Federal, se rige bajo la LGPDPPSO, su Reglamento, además del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTICSI) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público. Asimismo, es preciso hacer hincapié en que los cambios a nivel normativo tienen su impacto en la negociación de estas cláusulas en cualquier contrato de *software* y en las relaciones jurídicas entre proveedores y clientes.

Régimen de los datos. Definir el régimen de los datos es indispensable para establecer las cláusulas por las que el proveedor no tendrá la facultad de disponer de los datos personales ni hacer uso de ellos para ningún fin distinto al autorizado. El principal objetivo del régimen está orientado a determinar la manera en la que se va a posibilitar el conocimiento, actualización y rectificación de la información que se haya recogido sobre las personas en las bases de datos o archivos y la protección de las demás potestades, facultades y garantías que emanan de la normativa con respecto al tema.

1.5.2. Cláusulas tradicionales de un contrato de servicios de la nube

En un contrato de servicios de la nube se establecen las especificaciones técnicas y de calidad, alcances, precios y condiciones que regularán la prestación de servicios, que, posteriormente, formalizarán las dependencias o entidades, con fundamento en el artículo 17 y en la fracción XX del artículo 41 de la Ley de

Adquisiciones, Arrendamientos y Servicios del Sector Público, así como en el artículo 14 de su Reglamento.[32]

Con respecto a su estructura, el contrato se compone de la siguiente documentación: anexo técnico, que incluye las especificaciones técnicas y de calidad; alcances y condiciones que regularán la prestación de servicios; formato de oferta económica, que en ocasiones incluye el algoritmo de la fórmula del contrato, un esquema general que representa el producto de los precios o cantidades, y guía de usuario, que opcionalmente algunos contratos incluyen a manera de referencia.

Medidas de seguridad exigibles. El uso de servicios de cómputo en la nube ofrece un gran número de ventajas, pero también presenta riesgos específicos, por lo cual, es muy importante que se analicen las condiciones de prestación de servicios que permitan que el tratamiento de datos se realice sin merma de las garantías que le son aplicables. En este sentido, las medidas de seguridad deben basarse en la falta de transparencia sobre las condiciones en las que se presta el servicio y falta de control del responsable sobre el uso y gestión de los datos personales por parte de los agentes implicados en el servicio.

Control de los datos. En función de las peculiaridades del modelo de tratamiento en la nube, como parte de la ausencia de transparencia en la información, la falta de control del responsable se ve reflejada en las dificultades para conocer en todo momento la ubicación de los datos, así como en la incapacidad para disponer de los datos en poder del proveedor o de poder obtenerlos en un formato válido e interoperable, y en los obstáculos para una gestión efectiva del tratamiento de los datos. Además, debe incorporar otro tipo de cláusulas específicas para proteger a los responsables y/o encargados mediante las dos consideraciones siguiente:

Confidencialidad. Se refiere a que tanto el responsable como el encargado acuerdan revelar exclusivamente aquella información que sea necesaria para el

[32] Secretaría de la Función Pública, uso de contratos marco, 2017 México. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/96955/Contratos_Marco-2015.pdf. (fecha de consulta: 27 de agosto de 2019).

cumplimiento de las obligaciones establecidas en el contrato. Asimismo, las partes se comprometen a no revelar información confidencial a terceros. Sin embargo, sí podrán revelar la Información confidencial únicamente a aquellos empleados, representantes o subcontratistas a quienes se les exija protegerla contra la divulgación no autorizada de acuerdo con un nivel de protección no menor al establecido en virtud del contrato.

Protección de datos. La protección de datos reside en función de la política de privacidad, la cual puede estar sujeta a modificaciones a discreción. No obstante, las modificaciones no tendrán como consecuencia una reducción significativa del nivel de protección brindado a los datos personales proporcionados por el responsable. Así, el encargado desempeña el rol de procesador de los datos, y actúa de conformidad con las instrucciones respecto del tratamiento de los datos personales según se detalla en el contrato.

Limitación de responsabilidad. Establece que ninguna de las partes es responsable por los daños indirectos, incidentales, especiales, punitivos o consecuentes, ni por lucro cesante o pérdida de ingresos, datos o uso de datos. La responsabilidad total del encargado por cualquier daño y perjuicio que surja en virtud o como consecuencia del contrato se limita al monto total pagado al encargado por los servicios conforme a la orden que da origen a la responsabilidad.

Especificaciones del servicio. Tiene que ver con la descripción detallada de los servicios en virtud de lo solicitado y que comprende tanto el almacenamiento, como políticas de soporte y seguridad y de entrega de la información y alojamiento en la nube.

Notificaciones. Se refiere a aquellos casos en que se presente un conflicto en la interpretación o cumplimiento en cualquiera de las cláusulas, dicha circunstancia deberá hacerse del conocimiento del encargado de forma inmediata. Asimismo, en caso de solicitar la terminación de los servicios de conformidad con el contrato, el responsable deberá presentar una solicitud de servicio al encargado. Sin embargo, el encargado podrá otorgar avisos a la base de clientes de los servicios en la nube mediante la publicación de un aviso general o por correo electrónico a la dirección registrada en la información de cuentas del encargado.

La dificultad se presenta cuando el responsable y el encargado desconocen las disposiciones de la normativa que favorecen el cómputo en la nube. Particularmente cuando, en un contrato, las partes desconocen las disposiciones jurídicas, hecho que dificulta la toma de decisiones para afrontar los imprevistos en los servicios contratados de cómputo en la nube.

Entonces, por más esfuerzos que se hagan sobre la reglamentación y de los instrumentos jurídicos, si las partes no conciben la relación con el desarrollo tecnológico con las cláusulas, difícilmente se tendrán contratos que integren las posturas, los servicios y los datos a proteger. Un ejemplo de lo que se puede lograr cuando existe concordancia con lo mencionado es el caso del "Contrato de servicios en la nube administrados y servicios de actualización de licencia de software y soporte" celebrado entre el H. Ayuntamiento Constitucional de Zapopan y la empresa Oracle de México S.A. de C.V.[33] En dicho contrato, se identificaron los siguientes elementos:

1.5.2.1. Cláusula. Privacidad y seguridad de los datos

A continuación, se muestran algunas razones para incluir la cláusula de privacidad en los contratos de cómputo en la nube:

Argumento	Explicación
La política de privacidad de los servicios de Oracle se encuentra sujeta a modificaciones a discreción de Oracle; no obstante, las modificaciones de Oracle a la política no tendrán como consecuencia una reducción significativa en el nivel de protección	Se refiere a que las modificaciones que se realicen en la política de privacidad no tendrán consecuencias en el nivel de protección de la información para sus clientes.

[33] Municipio de Zapopan, Jalisco, Gobierno de Zapopan, contrato de servicios en la nube administrados y servicios de actualización de licencias de software y soporte. Disponible en: https://www.zapopan.gob.mx/wp-content/uploads/2015/05/173.pdf (fecha de consulta: 27 de agosto de 2019)

brindado a sus datos personales proporcionados como parte de sus datos durante el periodo de servicios de su documento de pedido.	
El contrato de Procesamiento de Datos para los Servicios en la Nube de Oracle describe los respectivos roles de las partes en cuanto al procesamiento y control de los datos personales que usted proporcione a Oracle como parte de los servicios administrados en la nube de Oracle. Oracle desempeñará el rol de procesador de los datos, y actuará de conformidad con sus instrucciones respecto del tratamiento de sus datos personales residentes en el entorno, según se detalla en el Contrato Marco, el Contrato de Procesamiento de Datos, y el respectivo Documento de Pedido.	Si bien, la empresa llevará a cabo el procesamiento de los datos, se limita, de algún modo, a actuar de conformidad con las instrucciones del responsable con base en lo que establece el contrato. Es decir, el encargado no decide respecto del tratamiento más allá de las condiciones que se pactaron.
Usted no debe brindar a Oracle acceso a información de salud, tarjeta de pago o información personal sensible de naturaleza similar que imponga obligaciones específicas relativas a la protección de los datos para el procesamiento de dichos datos a menos que se especifique en su orden.	Esta cláusula se relaciona con los mecanismos mínimos con los que el encargado debe contar. En este sentido, el encargado solicita al responsable no revelarle información más que la necesaria para llevar a cabo el procesamiento de datos.

Todo dato suministrado por usted que resida en su(s) entorno(s) será su información confidencial, según se define en los términos generales.	En este caso, el encargado especifica que la privacidad de los datos es competencia del responsable.

Cuadro 5. Cláusula de privacidad

Fuente: Elaboración propia con información de Oracle[34].

1.5.2.2 Cláusula. Limitación de la responsabilidad

El siguiente cuadro muestra la explicación del por qué se incluye en los contratos de servicio de cómputo en la nube la cláusula de limitación de la responsabilidad:

Argumento	Explicación
Ninguna de las partes será responsable por daños en los datos o uso de datos.	Bajo este argumento, el encargado se exime de cualquier responsabilidad por daños en los datos.
Oracle América, Inc. se adhiere a los Principios de Puerto Seguro de Estados Unidos/Unión Europea y, como resultado, aparece en la lista del Departamento de Comercio de Puerto Seguro de Estados Unidos a partir de la fecha de vigencia del documento de pedido. La Certificación de Puerto Seguro de Oracle, incluye específicamente el rendimiento de servicios de alojamiento de Oracle de la información personal proporcionada por el cliente.	Aunque esta condición no aplica para el caso de México, es una aportación que en algún momento se pudiera implementar en el país, particularmente por los avances en materia de protección de datos personales por parte de las autoridades, como la adhesión al Convenio 108 y el 108+.

[34] Oracle Corporation *Protección de datos*, Disponible en https://www.oracle.com/es/database/security/ (Fecha de consulta: 27 de agosto de 2019)

Todo dato suministrado por usted que resida en sus entornos será información confidencial de su propiedad según se define en el Contrato. Usted será exclusivamente responsable de la exactitud, calidad, integridad, legalidad, confiabilidad, adecuación y propiedad de la totalidad de sus datos.	En esta cláusula el encargado limita la posesión de la información, aclarando que cualquier aspecto relacionado con la confidencialidad y calidad es competencia del responsable.
Usted acepta otorgar los avisos y obtener los consentimientos relacionados con el uso que usted haga de los servicios y la prestación de los servicios por parte de Oracle, incluidos aquellos relacionados con la recopilación, el uso, el procesamiento, la transferencia y la revelación de datos personales.	El encargado impone al responsable las atribuciones relacionadas con el uso que haga de los servicios, aceptando el otorgamiento de avisos y obtención de los consentimientos.
Si estuvieran disponibles, usted podrá adquirir servicios de Oracle (ejemplo, Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services) diseñados para cumplir con requisitos particulares relacionados con la protección de datos que resulten aplicables a su negocio o sus datos.	La cláusula advierte al responsable que cuenta con otros servicios más sofisticados de protección que los establecidos en el contrato, los cuales se pueden contratar a parte.

Cuadro 6. Cláusula de limitación de la responsabilidad.

Fuente: Elaboración propia con información de Oracle.

Por otra parte, para fortalecer las cláusulas de protección de datos se proponen los siguientes ajustes: una cláusula que se refiera a la “Limitación de responsabilidad”, en la que se establezca que ninguna de las partes será responsable por lucro cesante o pérdida de ingresos, datos o usos de datos; lo cual coadyuvará a no perjudicar al responsable de los datos.

Cuando el país de origen del encargado es distinto al mexicano, por lo que comúnmente se rige por sus propios mecanismos de protección de datos, se recomienda que en el contrato se considere una cláusula en la que se establezca que se apegará a los Principios de Puerto Seguro del país de origen. Con la inclusión de esta cláusula, se busca contar con una herramienta para hacer válida la protección de datos, al exigir que se reconozca en la normativa mexicana la figura de encargado de los datos.

1.5.2.3 Otras cláusulas

Además de lo hasta ahora visto, hay otros aspectos que deben considerarse al momento de elaborar un contrato de servicios en la nube. Por ejemplo, las cláusulas de propiedad intelectual son fundamentales, pues los medios necesarios para proporcionar los servicios objeto del contrato, programas informáticos, aplicaciones, sistemas de gestión, etcétera, se encuentran protegidos por derechos de este tipo.

Es importante considerar que, en función del grado de protección de los servicios en la nube, el responsable pueda instalar o tener acceso a equipos, o programas por medio de los cuales tenga el control sobre los datos que el encargado está alojando en sus servidores. En este sentido, convendría establecer una cláusula en la que las partes reconozcan que, por medio del uso, motivo de la ejecución de los datos, el titular autoriza al encargado el uso de su información.

De igual forma, resulta útil contar no solamente con una cláusula como parte del contrato sino con un anexo específico para generar una protección más precisa de la información. Si bien, las cláusulas contenidas en los contratos están considerablemente estandarizadas, su revisión y ajuste por las partes resulta altamente recomendable.

1.5.3. Obligaciones de las partes

En el contrato de cómputo en la nube es común relacionar a las partes con obligaciones específicas, pues la omisión de alguna de las obligaciones podría dar lugar a dudas en el cumplimiento del contrato, o bien, a un conflicto entre las partes. Por lo que, en la elaboración de un contrato de servicios en la nube resulta indispensable determinar las obligaciones y responsabilidades de las partes en función de contribuir al cumplimiento de las cláusulas. Asimismo, es conveniente que se preste especial atención al tratamiento para la protección de datos personales ya que existe, por ejemplo, la posibilidad de que los propios proveedores externalicen parte de sus servicios a través de contratos de tercerización.

Si lo anterior ocurre, se debe identificar la cadena de responsabilidades de los servicios en los diferentes procesos para tener un control efectivo respecto de los compromisos adquiridos por las partes. En otros términos, en la prestación de servicios en la nube, las obligaciones de las partes deben establecerse, concretamente, al tipo de servicio, ya que esto puede dar una mejor idea del tipo de servicios en la nube que regula el contrato en cuestión.

1.5.4. La importancia del anexo técnico

En el estricto sentido, el anexo técnico es lo fundamental, ya que establece a detalle las especificaciones particulares que asegurarán la conveniencia y satisfacción de las necesidades del contratante. Asimismo, contiene las consideraciones técnicas que le otorgan mayor importancia que el contrato *per se*.

Es decir, el anexo técnico contiene los pormenores respecto del alcance de los servicios que serán proporcionados por el proveedor y la descripción de los mismos con las características mínimas solicitadas para cada uno de ellos. De la misma forma, es frecuente que el anexo cuente con el detalle de los procedimientos a seguir para los servicios de operación y mantenimiento a cargo del proveedor de servicios en la nube. En virtud de ello, el anexo debe especificar responsabilidades para cada uno de los que intervienen durante el desarrollo del instrumento contractual; entre ellas, que el encargado debe comprometerse a garantizar la

confidencialidad utilizando los datos sólo para los servicios contratados y que, al término de la relación contractual, los datos de carácter personal sean destruidos o devueltos a la entidad contratante responsable o al encargado del tratamiento que ésta hubiese designado[35].

Por otra parte, el anexo técnico debe incluir medidas específicas de seguridad en función del cumplimiento de la normativa vigente, ya que la mayoría de las infraestructuras en esquemas de cómputo en la nube son compartidos por múltiples empresas o usuarios; por lo que resulta importante establecer medidas de seguridad tales como:

- Normas técnicas para estandarizar las características técnicas y de interoperabilidad que coadyuven a enfrentar la constante evolución de los servicios en la nube.
- Manejar la configuración de aspectos legales como la gestión y el asesoramiento en la elaboración del contrato, así como los profesionales expertos en cuestiones técnicas que soportan los servicios de la nube.
- Definir de manera explícita y clara el proceso o procedimiento para la gestión de incidentes, en donde el encargado le informe al responsable el histórico de incidencias con el servicio o que se ha puesto en riesgo la seguridad de la información.
- Establecer acuerdos de nivel de servicios en los que se detallen aspectos como controles, reglamentación a cumplir, medidas de protección y seguridad, plazos de recuperación del servicio, indicadores y forma de medición de la calidad del servicio con sus respectivos valores mínimos aceptables, penalizaciones y el régimen de responsabilidad por los daños y perjuicios ocasionados por incumplimiento del encargado.

En concreto, la relevancia del anexo técnico y, consecuentemente, el detalle de las penalizaciones por incumplimiento del contrato, constatan la importancia no

[35] Privacy Driver, Responsabilidad del tratamiento en la mediación de seguros, Ley Orgánica 15/1999, de 13 de diciembre 1999, de Protección de Datos de Carácter Personal, Disponible en *https://www.privacydriver.com/es/responsabilidad-del-tratamiento-mediacion-seguros-c356* (fecha de consulta: 7 de diciembre de 2018)

sólo de que se presta el servicio en la nube, sino que la prestación de éste se lleva a cabo conforme lo establece la normativa.

En razón de lo anterior, para efectos de este trabajo, consideremos como ejemplo de un Anexo Técnico, los objetivos, requerimientos de cumplimiento obligatorio y niveles de servicio, los que a continuación se detallan para una nube híbrida, debiendo indicar que el cómputo en la nube es un modelo para habilitar el acceso a la red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con mínimo esfuerzo de administración o de interacción con el proveedor del servicio[36].

1.5.4.1. Objetivo de los servicios

Contar con un servicio de nube híbrida para el almacenamiento y procesamiento de información y aplicativos, con una plataforma tecnológica de Infraestructura como Servicio (IaaS) y de Plataforma como Servicio (PaaS), que brinde la elasticidad y consumo bajo demanda por un periodo de 24 meses.

Lo anterior permitirá instrumentar de forma eficiente y oportuna las soluciones tecnológicas que satisfagan los requerimientos de negocio orientados a brindar un mejor servicio y a tener un control más adecuado de la información con la que cuenta la dependencia.

1.5.4.2. Objetivos específicos

- Con un modelo elástico bajo demanda de servicios que puedan ser provistos y apagados automáticamente con base en las necesidades de la dependencia.
- Gestión de los servicios.
- Pago de los servicios de acuerdo con el uso efectivo de los mismos.

---

[36] Emiliano Nieto, Facultad de Informática, Universidad de la Plata, Diseño de aplicaciones SaaS sobre plataformas de cloud computing, Disponible en *http://sedici.unlp.edu.ar/bitstream/handle/10915/46834/Documento_completo.pdf?sequence=1* (fecha de consulta: 7 DE DICIEMBRE DE 2018)

- Garantizar la continuidad operativa de las aplicaciones hospedadas.
- Contar con una nube híbrida con neutralidad tecnológica y apegada a estándares de la industria que permitan la interoperabilidad, portabilidad, seguridad y confiabilidad de la información.

Adicional a lo anterior, resulta necesario contar con servicios de seguridad activa para nube híbrida, que garanticen la privacidad, integridad y disponibilidad de la información que transite o resida en la nube pública, así como de los servicios y aplicaciones desplegadas en la nube pública, en cualquiera de las modalidades de servicio IaaS o PaaS, así como, de cualquier tipo de ataque ya sea que provenga del exterior, o que pudiera propagarse desde el interior de la red de la dependencia.

La capa de seguridad que administre los accesos del personal autorizado a los componentes que conforman los servicios, tanto de procesamiento como de seguridad, debe garantizar una interoperabilidad transparente y funcional con la solución de identidades de la dependencia. El acceso remoto a las consolas de gestión y monitoreo debe llevarse a cabo a través de comunicaciones seguras, por medio de clientes VPN.

La nube pública que ofrezca el licitante debe contar con las siguientes funcionalidades subyacentes de seguridad:

Generar y configurar listas de control de acceso de red (ACLs) creando una capa adicional de seguridad en una Red Virtual Privada, independiente de los Grupos de Seguridad (Security Groups), la cual actúa como un firewall virtual que controla el tráfico de ingreso y egreso a una o más subredes.

Grupos de Seguridad (SGs), que contengan una lista de reglas de control de acceso (ACLs), las cuales permiten habilitar o restringir el tráfico de red a diferentes instancias de máquina virtual en una red virtual. Los SGs se pueden asociar con una subred completa o con las instancias individuales de máquina virtual de cada subred y son implementados dependiendo del proveedor de nube pública mediante firewalls virtuales y/o ACLs en la capa de acceso.

La naturaleza del cómputo en la nube requiere que la seguridad de las unidades de servicio considere conceptos similares a ambientes tradicionales como

lo son la autenticación, disponibilidad, confidencialidad, manejo de identidades, integridad de los datos, auditorías y gestión de las políticas de seguridad.

El proveedor con la dependencia establecerá los mecanismos necesarios que aseguren que la información que se genera procesa, almacena y se transmite en el ambiente de la nube, sea tratada con carácter confidencial y reservado, de manera que se asegure la confidencialidad, integridad y disponibilidad, así como la autenticación, confiabilidad y trazabilidad, evitando una posible violación o la sustracción de la información.

El licitante deberá presentar la manera en que aprovisionará los mecanismos de seguridad necesarios para el modelo de despliegue de la nube privada *on-premises*, bajo alguno de los siguientes modelos operativos: Integrar el orquestador de la solución existente en la dependencia a su propuesta de orquestador; integrar por separado el orquestador de red (APIC) y los controles de seguridad (FW y Balanceador de Carga/SSL Offloading) a través de APIs e incluir en su propuesta de nube privada los firewall redundantes y balanceadores redundantes de su preferencia, siempre y cuando al integrarlos a su solución ofrezcan beneficios y ventajas técnicas a la dependencia

Será responsabilidad del proveedor configurar y habilitar las interfaces de programación de aplicaciones (APIs por sus siglas en inglés Aplication Programming Interface) o bien desarrollar la integración con la interfaz del controlador. De manera general, el módulo de seguridad debe comprender al menos los siguientes servicios:

Protección perimetral en nube pública: Debe proveer los recursos indispensables para llevar a cabo los mecanismos de protección lógica de los recursos que almacenan y procesan la información contenida en el servicio de nube.

A continuación, se describen las funcionalidades mínimas que deberá cumplir la protección perimetral de los servicios bajo el modelo de despliegue de nube pública:

- Protección contra ataques externos
- Control de acceso a los servicios/datos/software/hardware
- Generación y administración de servicios de VPN

- Monitoreo del ancho de banda en caso de ataque
- Sistema de detección y prevención de Intrusos
- Mecanismos de protección contra ataques de denegación de servicios
- Control de flujos de tráfico de comunicaciones de entrada y salida
- Bloqueo y apertura de puertos lógicos de comunicaciones

Control de acceso a los servicios: Servicios de autenticación, autorización y auditorías de acceso, que permitan asegurar el acceso a la información y recursos, por parte de las personas autorizadas.

La solución de control de acceso a los servicios debe cumplir con al menos los siguientes puntos:

- El portal único del servicio debe contar con la capacidad y soporte necesario para el control de identidades institucional. La unión deberá ser llevada a cabo a través de estándares y/o protocolos como OASIS XACML, SAML2, OAuth u otro que se considere aplicable para llevar a cabo dicha integración.
- Permitir la asignación de la temporalidad (tiempo de vida) a los accesos de servicio.
- Generación de estadísticos entre los que se encuentran: reportes de accesos autorizados y rechazados, brindando datos de la fecha y hora de este, así como la cantidad de intentos realizados.

Cifrado Función de cifrado con llaves que le proporcione la dependencia, tanto de la información almacenada, como aquella que es transportada a través de los enlaces de comunicaciones de datos que se incluyen en el proyecto. Con el objetivo de garantizar la información que se genera, procesa, almacena y trasporta bajo el presente servicio, el proveedor debe evitar las siguientes acciones:

- Violación y/o modificación de la información
- Robo de información
- Pérdida de información
- Servicios de Protección para servidores

Tanto en nube pública como privada se deberá soportar el uso de *scripts* para automatizar la implementación de los servicios de protección para servidores que

proporcionará la dependencia y deberá permitir el aprovisionamiento automatizado y la activación de las políticas de seguridad, así como la activación de las políticas de seguridad en la configuración de grupos de elasticidad.

Módulo de Gestión y Monitoreo: Este módulo tiene como objetivo la administración y visibilidad general del servicio de manera integral y a nivel de unidades de servicio, operando con herramientas de recolección de eventos (poleos), con información actualizada y con elementos en su plataforma que aseguren un esquema de alta disponibilidad para dicho módulo. Deberá brindar por lo menos la información sobre las métricas de desempeño, estado de los servicios, consumos, disponibilidad, los cuales deberán proporcionar los elementos que permitan la toma de decisiones en caso de que la dependencia lo requiera. El proveedor deberá proporcionar los desarrollos para la integración de las vistas con el portal único del servicio.

El esquema de operación para este módulo debe ser bajo un diseño fuera de banda, es decir, los flujos de gestión y monitoreo no deben viajar a través del mismo canal donde se transportan los flujos de la operación, ya sea de manera física o lógica. Esta información debe ser almacenada en un repositorio proporcionado por el proveedor.

Entre los diferentes servicios a gestionar y monitorear se deberán considerar por lo menos los siguientes:

- Fallas
- Configuración y aprovisionamiento de servicios
- Visibilidad del catálogo de servicios
- Control de actualización de infraestructura, software, licenciamiento y parches
- Métricas del rendimiento o niveles de servicio, tales como desempeño y disponibilidad de cada uno de los componentes
- Seguridad
- Administración de eventos en formato del tipo registros (logs)
- Visibilidad de la cantidad de los recursos disponibles y consumidos asignados a cada unidad de servicio.

Con base en las características antes mencionadas, el proveedor debe proporcionar la siguiente información detallada en la propuesta para cumplir con el servicio del módulo de gestión y monitoreo:

- Descripción funcional clara y precisa de cada uno de los módulos que conforman la solución de gestión y monitoreo
- Información relacionada con objetivo, interacción, relación y dependencias de cada uno de los módulos que conforman la solución de gestión y monitoreo
- Descripción clara y precisa de cómo se atenderán los siguientes puntos: rendimiento, seguridad lógica, administración, planeación de capacidad y habilitadores, donde se muestre cómo se integran en la solución.

Módulo de recursos físicos y virtuales. El módulo de recursos físicos y virtuales tiene como objetivo establecer los elementos en cuanto a infraestructura activa que el proveedor debe proporcionar para ofrecer los servicios solicitados. La infraestructura activa se refiere a los elementos de redes de comunicaciones de datos, procesamiento de cómputo físico y virtual, almacenamiento de información, seguridad lógica, que soportarán y conformarán los servicios que estarán distribuidos entre los diferentes esquemas de despliegue de nube pública y nube privada *on-premises*.

El proveedor deberá proporcionar los servicios virtuales que se encargan de la emulación de los recursos de procesamiento de cómputo, llamadas instancias o máquinas virtuales, las cuales hacen uso de los recursos físicos que tienen disponibles (procesamiento de cómputo, almacenamiento de información, comunicación de datos y memoria RAM), y los presentan como recursos propios.

Es responsabilidad del proveedor proporcionar todos los recursos físicos, de licenciamiento, virtuales, humanos y todo lo necesario (por ejemplo, cableado, *switches*, entre otros) para la habilitación y entrega de los servicios.

Portal único del servicio: La plataforma de administración de nube híbrida deberá contar de manera integrada con un portal único del servicio que servirá como

el exclusivo punto de ingreso para las actividades de autoservicio y de administración.

El portal único del servicio deberá gestionar integralmente los recursos bajo los modelos de despliegue de nube pública, nube privada *on-premises*. El portal único del servicio debe proporcionar la capacidad de utilizar el auto aprovisionamiento de los recursos de manera ágil que permita reducir los tiempos en la habilitación de requerimientos que demande la dependencia, así como en la capacidad de supervisar la utilización y consumo de los servicios y sus respectivos recursos de infraestructura, la habilitación y configuración de parámetros que permitan la automatización de las tareas manuales y procesos para la operación del servicio.

Servicios de Soporte a la Operación: Los servicios de soporte a la operación habilitan las capacidades para la operación eficaz de los servicios en un ecosistema de nube híbrida a través del portal único del servicio y alimentados y soportados por el orquestador. Los servicios mínimos contemplados para el soporte a la operación que deben ser implementados son los siguientes:

Flujo de autorizaciones: permite automatizar el proceso de aprovisionamiento y despliegue, incluyendo procesos como la solicitud de servicios iniciales, autorización de cambios, aplicación de políticas de seguridad, cumplimiento de políticas de operación, liberación de aplicaciones, publicación de elementos al catálogo de servicio, y otros flujos de autorización que surjan a partir de la operación.

Aprovisionamiento: ofrece las capacidades para aumentar o disminuir rápidamente los recursos informáticos. El aprovisionamiento debe estar basado en un catálogo para realizar un despliegue automático de servicios en la nube a partir de una solicitud o requerimiento.

Servicio de Capacidad y Desempeño (Administración de Cargas de Trabajo): permite la asignación eficiente y el uso óptimo de los recursos de la nube. Analiza en tiempo real el desempeño de la ejecución de servicios en la nube y ajusta automáticamente la carga de trabajo.

Servicio de Plantillas: ofrece instancias que se pueden volver a recrear un número ilimitado de veces. En caso de IaaS, las plantillas describen cómo las instancias deben ser configuradas (imágenes de máquinas, conectividad de red, requisitos de almacenamiento, entre otros) y desplegadas en un entorno de infraestructura dinámica. El servicio también permite el aprovisionamiento automático de aplicaciones/re-despliegue en una plataforma de servicios de nube.

Servicio de Ciclo de Vida (Servicio de Gestión de Entrega): controla el ciclo de vida de los servicios en la nube, considerando el aprovisionamiento y desaprovisionamiento dinámico. También proporciona la visibilidad, control y automatización a través de los entornos de nube para hacer frente a los desafíos críticos para el negocio.

Servicio de Cumplimiento de Niveles de Servicio: con el fin de garantizar un alto nivel de estándares en servicios de la nube híbrida, la dependencia define la aplicación estricta de los acuerdos de niveles de servicios (*Service Level Agreement* o SLA) para evitar en la mayor medida posible la degradación del rendimiento del servicio. El servicio de cumplimiento de niveles de servicio ayuda a tener visibilidad y a asegurar su cumplimiento y mejorar su entrega. Este servicio ofrece la evaluación en tiempo real y los informes de cumplimiento de SLA's en la nube.

Servicio de Incidencias y Manejo de Problemas: se ocupa de las incidencias relacionadas con el servicio y los problemas asociados y realiza el análisis de la causa raíz. Se debe almacenar información en una base de datos de conocimiento para el análisis adicional que puede incluir el estudio de tendencias para permitir la evolución de los servicios en la nube para prevenir futuros incidentes.

Integración de Servicios de Nube: sirve como un conector entre el medio ambiente de una nube a otra (de la nube privada a la nube pública y viceversa) para permitir la interoperabilidad. La interconexión de servicios en la nube debe garantizar una conectividad segura, cruzando sin problemas diferentes límites de la red, y aplicando capacidades de mejora de rendimiento (por ejemplo, compresión de datos).

Gestión de la Configuración: proporciona herramientas para automatizar la creación de máquinas virtuales en la nube híbrida y administrar sus detalles de

configuración y; por último, respaldo: permite programar respaldo de información a través de políticas definidas con base en las necesidades de negocio.

1.5.5. Estrategia de transición e implementación de la nube privada

La estrategia para la transición de los servicios deberá estar diseñada de forma que no interrumpa la prestación del servicio. La misma deberá ser propuesta por parte del proveedor en los pasos y detalles técnicos requeridos para su ejecución, pero deberá respetar las actividades en el orden que se indica más adelante.

Asimismo, la dependencia tiene previsto implementar un Plan de Recuperación de Desastres (*DRP, Disaster Recovery Plan*, por sus siglas en inglés), reutilizando aquellos servidores de procesamiento de cómputo (de navaja o *blades*) que se vayan liberando, producto de la migración de aplicaciones hacia el modelo de despliegue de nube pública y nube privada. Para lograr lo anterior, se habilitará un centro de datos principal con los ambientes productivos y un centro de datos alterno para habilitar el DRP, cuya definición, diseño e implementación será responsabilidad de la dependencia, aunque el proveedor deberá habilitar la plataforma tecnológica que soporte el DRP como parte de la nube privada, así como colaborar con la dependencia en reuniones, soporte técnico, recomendaciones para agilizar dicha implementación.

Integración de la infraestructura de DRP. El alcance de la integración del DRP se limita para el proveedor, a la integración de infraestructura necesaria para habilitar dicho servicio, quedando fuera los procesos de análisis, diseño e implementación del DRP, sin dejar de colaborar de manera estrecha en las actividades mencionadas con la dependencia.

Al ser parte del servicio, la infraestructura de *blades* que será entregada al proveedor deberá reconfigurarse para operar integrada al servicio bajo el concepto de nube privada y deberá contar con los mismos alcances de servicios expresados para el Portal Único del Servicio.

El proveedor podrá proporcionar equipo nuevo para el DRP en lugar de reutilizar la infraestructura de *blades* actuales, sin que esto implique un costo

adicional, considerando que la capacidad mínima del DRP a implementar corresponde a la capacidad física que la dependencia le entregará.

En cualquiera de los dos casos, el proveedor de SENHA será responsable de todos los insumos o componentes habilitadores para la conexión a la red de datos y almacenamiento que sean necesarios para garantizar la implementación del DRP, tales como: cableados LAN/SAN, Gbics, interconexión entre salas, racks y reubicación entre bunkers.

Continuidad del Servicio. El proveedor tomará la operación de la infraestructura de procesamiento, le será entregada la infraestructura, licenciamiento y equipo productivo que compone el servicio de procesamiento actual, del cual será responsable de dar continuidad operativa en tanto se terminan los servicios de migración y con los cuales proveerá y soportará los servicios de DRP hasta el término de la vigencia del contrato.

El proveedor será responsable de dar soporte a dichos equipos y garantizar la prestación del servicio, pudiendo realizar los ajustes de configuración que requiera, para garantizar la continuidad operativa de la mejor forma para la institución. Dado que esta infraestructura será de transición y para el uso del DRP únicamente, el proveedor podrá utilizar aquellos activos que vaya dando de baja por eficiencia o migración de servicios para utilizarse como base de refacciones y manteniendo la continuidad operativa bajo los niveles de servicio requeridos.

Implementación de la Nube Privada y Pública. Como primera etapa del servicio, el proveedor deberá habilitar la infraestructura con la que prestará el servicio de USP en el caso de nube privada. Simultáneamente, podrá habilitar los servicios de nube pública. Ambos servicios deberán quedar habilitados de forma suficiente y confiable para comenzar a recibir la migración de las aplicaciones *cloud-ready* y los ambientes virtualizados en los que actualmente operan hacia la nube con las consideraciones establecidas en el Servicio de Migración.

Migración Inicial. La migración de los ambientes virtualizados de la dependencia a las nubes correspondientes se deberá realizar dando prioridad hasta un máximo de 100 aplicaciones “*cloud-ready*”, quedando estas con sus ambientes

de producción funcionando en la nube privada y sus demás ambientes en la nube pública

Consolidación y Mudanza de Infraestructura. El proveedor, una vez concluida la migración de las máquinas virtuales de la infraestructura actual de cada Centro de Datos a la nube privada o pública, deberá consolidar la infraestructura física liberada (incluyendo las redes SAN y LAN) con vida útil, en el Centro de Datos que será designado para la función de sitio de DRP. Dicho proceso de mudanza, estiba, desinstalación, instalación, configuración y arranque, así como los gastos asociados a dichos procesos deberá ser cubierto por el proveedor.

El proveedor privilegiará la infraestructura de las generaciones más recientes de *blades* que le será entregada para la integración de un servicio de DRP que deberá contar con capacidad suficiente para cubrir el 100% de la demanda del sitio principal de la nube privada del servicio. En caso de que la demanda de la nube privada supere la capacidad de la infraestructura que será entregada al proveedor, no será necesario que la misma sea escalada ya que ella solo se operará como DRP.

El proveedor es responsable de la desinstalación, empaquetamiento y traslado de la infraestructura actual que se vaya dando de baja hacia el sitio donde la dependencia lo determine.

Niveles de Servicio. De acuerdo con lo establecido en los artículos 53 y 53 Bis de la Ley de Adquisiciones Arrendamientos y Servicios del Sector Público, 96 y 97 de su Reglamento se aplicarán las penas convencionales y deducciones respectivamente, por atraso en la prestación del servicio y, con motivo, del incumplimiento parcial o deficiente en que pudiera incurrir el proveedor.

Para la medición del cumplimiento se definen las siguientes métricas:

Disponibilidad de las unidades de servicio. La disponibilidad se define como el porcentaje de tiempo en que un servicio cumple con el objetivo de la función para la que fue diseñado, en relación con el tiempo total de medición. Se considera que el servicio está disponible cuando la totalidad del servicio incluyendo hardware y software de su configuración opera correctamente bajo los requerimientos mínimos solicitados, y bajo la medición del cumplimiento. La falta de muestras de monitoreo,

ocasionadas por errores en las herramientas de monitoreo, serán consideradas como falta de disponibilidad para aquél o aquellos elementos para los que no exista información. Los casos donde no se cuente con información respecto del estado que guarda alguno de los sistemas o componentes que conforman el servicio, aun cuando esto se deba a una falla en los sistemas de gestión y monitoreo administrados por el proveedor, esto será considerado como una falla en la disponibilidad del servicio, por lo que será causal de aplicación de la deducción correspondiente.

Tiempo de solución a incidentes. El proveedor asegurará un adecuado proceso de administración de incidentes que dé como resultado el cumplimiento del tiempo para la solución de incidentes, sobre los distintos componentes del servicio que forman parte de las unidades de servicio. La medición de la resolución de incidentes se realizará por medio de reportes que se generen o los reportes automáticos generados por las herramientas de monitoreo o servicios de orquestación de los servicios proporcionados por el proveedor, en los cuales se identifique la descripción del problema, la hora en que se recibe la incidencia, la hora en que se soluciona la incidencia. El tiempo empieza a contar a partir de que se generó de forma automática por medio de herramientas de monitoreo y gestión y, para aquellos casos en los que se generen alarmas y/o notificaciones automáticas, el tiempo iniciará a partir de que el sistema las haya registrado. El intervalo de medición será mensual. Serán contabilizados por tipo de servicio a fin de que sean integrados y evaluados dentro del periodo en cuestión. Los criterios anteriores serán aplicados y contabilizados como parte de la métrica de “Tiempo de Solución a Incidentes” cuando la falla resulte en falta de disponibilidad del servicio de forma parcial o total.

Entrega del servicio La entrega del servicio se medirá como la diferencia en tiempo de las solicitudes levantadas comparadas contra las solicitudes solventadas de forma satisfactoria dentro de la ventana de tiempo definida. Una solicitud se considerará como atendida satisfactoriamente, cuando se hayan implementado correctamente, a través de pruebas de aceptación del servicio realizado, la solicitud de alta/baja/cambio y quede debidamente documentada.

1.5.6. Consideraciones jurídicas diversas

Además de los aspectos anteriores, se encuentran otros elementos que en la contratación de cómputo en la nube son de suma importancia. Éste es el caso de la seguridad de la información que, desde una perspectiva técnica como la confidencialidad y el control de acceso, interviene en el aspecto jurídico en el elemento más representativo que es la confidencialidad.

En este sentido, el encargado debe permitir verificar de forma automática la integridad de los datos en cualquier momento. Asimismo, configurar la recuperación de copias de seguridad para proteger los procesos más críticos de confidencialidad. Además, es recomendable que el encargado tenga acceso a un portal personalizado para la recuperación de ficheros, discos o al sitio completo. El encargado debe contar, de ser posible, con un plan de recuperación de desastres que facilite la migración en caso de que se presente algún incidente ajeno a su control, como es el caso del delito cibernético.

De este modo, el hecho de que se reconozca la confidencialidad constituye una forma de preservar la naturaleza de la seguridad de la información. Es recomendable que el encargado, cuente además con un acuerdo de confidencialidad para evitar divulgue la información a que tiene acceso. Por tal motivo, los responsables de las áreas jurídicas y de tecnología de las organizaciones deben trabajar de forma coordinada en el establecimiento de las obligaciones contractuales, para garantizar qué requisitos de seguridad se pueden solicitar y alcanzar contractualmente mediante el establecimiento de métricas y estándares adecuados.

Es decir, independientemente de los aspectos que deben tenerse en cuenta al momento de seleccionar el modelo de servicio en la nube, infraestructura, plataforma o *software* y el modelo de despliegue, nube privada, pública, comunitaria o híbrida, existen importantes cuestionamientos que deben hacerse con carácter previo a la contratación, desde el punto de vista de protección de datos.

Aunque no siempre es posible, se recomienda que se sepa en qué país se almacenará la información, qué tipo de datos se tratan en la empresa y cuáles de

ellos se subirán a la nube, así como garantizar las medidas de seguridad que la compañía necesita según el tipo de datos personales o datos sensibles, así como si las condiciones generales de contratación por parte del proveedor de servicios en la nube cumplen con la normativa de protección de datos.

Son aspectos relevantes al momento de contratar los siguientes: la jurisdicción y normativa aplicable, las obligaciones del encargado en el tratamiento de los datos con base en la normativa mexicana en materia de protección de datos personales y seguridad jurídica en la nube.

Promover la certeza respecto de las garantías de privacidad y seguridad a través de la celebración de contratos que cumplan con un nivel de diligencia adecuado para garantizar la salvaguarda de los datos personales, puntualizando las medidas de seguridad que se implementarán a través de jurisdicción por deslocalización y/o cambio de jurisdicción, alcance de los servicios en la prestación por terceros, condiciones de uso, finalidad del uso, modelos de contratación.

Auditoría de los sistemas de seguridad, la cual está a cargo del responsable del tratamiento de los datos, para evaluar los servicios en la nube, a través de la codificación de parámetros específicos y niveles mínimos requeridos para cada elemento del servicio. La auditoría coadyuva a detallar la infraestructura del sistema y los estándares de seguridad que debe mantener el proveedor del servicio en la nube.

Propiedad intelectual. Determinar a quiénes les pertenecen los datos, la información, las aplicaciones y los servicios. En este sentido, se debe reflexionar cómo se procederá jurídicamente para respetar la propiedad intelectual del contenido o el *software* que el responsable origine, almacene o transmita a través del *software*, plataforma o infraestructura que se pone a su disposición.

Por otra parte, es importante mencionar que no es procedente una adjudicación directa por seguridad nacional como procedimiento de contratación, toda vez que el artículo 41, fracción IV, de la Ley de Adquisiciones, Arrendamientos y Servicios del sector Público, en relación con el diverso 72, fracción IV, de su Reglamento, ordena a cualquier dependencia que, sólo podrá contratar servicios -por seguridad nacional- sin sujetarse al procedimiento de licitación pública, cuando

se realicen con fines exclusivamente militares o para la armada, o su contratación mediante licitación pública ponga en riesgo la seguridad nacional o la seguridad pública, en los términos de las leyes de la materia y, en los casos particulares, no se actualizan dichas hipótesis normativas, toda vez que los requerimientos -citados- son de carácter técnico, operativo y administrativo, en razón que no están afectos a fines exclusivamente militares o para la armada, o aquéllos que no estén relacionados con la preservación de la seguridad nacional o la seguridad pública.

Es decir, sólo las dependencias o entidades integrantes del Consejo de Seguridad Nacional podrán sustentar las contrataciones que realicen con fundamento en el primer párrafo de la fracción IV, del artículo 41 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, cuando los bienes o servicios que requieran se encuentren en la base de datos que administra el Comité Técnico del citado Consejo. En estos casos, la investigación de mercado se tendrá por realizada a través de la consulta que se formule a dicha base de datos y el escrito a que se refiere el segundo párrafo del artículo 40 de la Ley referida, será elaborado por el área requirente conforme al modelo que haya autorizado dicho Comité, el cual debidamente requisitado obrará en el expediente de contratación respectivo.

En lo que respecta a la ubicación de los datos, podemos emitir las siguientes consideraciones jurídicas: El artículo 9 del “Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información, así como el Manual Administrativo de Aplicación General en dichas materias” (MAAGTICSI) publicado en el Diario Oficial de la Federación el 08 de mayo de 2014 y su última reforma publicada en el mismo medio de difusión el 23 de julio de 2018, establece que para la contratación de servicios de hospedaje de infraestructura y aplicaciones en un centro de datos, incluyendo hospedaje en la nube, las Instituciones y los proveedores deberán someterse a la jurisdicción de las leyes y tribunales mexicanos sin importar el territorio en el que los datos se encuentren alojados.

El artículo 13 del propio MAAGTICSI, ordena que, en el caso de servicios de Centros de Datos, las Instituciones, deberán de identificar la infraestructura de Centro de Datos con la que cuentan y la utilización de ésta, así como espacio físico, energía eléctrica, capacidad de procesamiento y almacenamiento; evaluar la conveniencia de contratar servicios de Centro de Datos, tomando en cuenta el beneficio económico, eficiencia, privacidad, seguridad de los datos y de la información, en comparación con la de utilizar un Centro de Datos propio o compartido con otra Institución y, finalmente, analizar el alojamiento de su infraestructura crítica en un Centro de Datos de una Institución agrupada en su mismo sector, o en su defecto, en un Centro de Datos de otra Institución, bajo un modelo de cómputo en la nube, cuando no cuenten con un Centro de Datos propio y no tengan contratados servicios de Centro de Datos.

El artículo 15 del cuerpo normativo indicado, ordena que, en las contrataciones relacionadas con servicios de plataformas de procesamiento de datos, las Instituciones deberán prever en la convocatoria a la licitación pública, en la invitación a cuando menos tres personas o en las solicitudes de cotización, o bien en los contratos que celebren con otros entes públicos, según corresponda, que en la prestación de los servicios se separe en capas el acceso a dichas plataformas; la administración e infraestructura esté clasificada en zonas de seguridad basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento y; se privilegie el procesamiento de datos en territorio nacional. En aquel procesamiento de datos que por su alto volumen exceda las capacidades de cómputo existentes en territorio nacional, ya sea del Gobierno Federal o de terceros, podrá contratarse el servicio de cómputo en la nube para procesamiento de datos desde el extranjero, verificando en todo momento que cumpla con los estándares de seguridad de la información y la legislación aplicable en materia de archivo y de protección de datos personales, así como de mejores prácticas nacionales e internacionales en materia de cómputo en la nube.

1.5.7. La portabilidad en la contratación de los servicios de nube

Es de todos sabido que, en nuestro país, el sector privado está más adelantado que el sector público en la incorporación de novedades tecnológicas en su actividad. El caso del cómputo en la nube no es diferente porque son cada vez más las propiedades que se le atribuyen tal es el caso de la portabilidad, el cual es considerado un nuevo derecho que tiene por objetivo facultar a los interesados con respecto a sus propios datos personales, ya que mejora su capacidad de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro.

1.5.7.1. Características de la portabilidad

Favorablemente, la portabilidad surge del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), factor que le otorga cierto reconocimiento e importancia, debido a que, por medio de este derecho, el interesado recibe los datos personales proporcionados a un responsable en un formato estructurado, de uso común y lectura mecánica, o bien, transmite sus datos personales al responsable receptor.

Sin embargo, debido a que el modelo de cómputo en la nube implica un movimiento de los datos entre distintos entornos, incluso, entre distintos proveedores, expertos en la materia consideran que la portabilidad es el factor más importante en la contratación de servicios, sólo por detrás de la seguridad, que ocupa el primer lugar. Es decir, el crecimiento del cómputo en la nube está condicionado por la capacidad de las organizaciones para gestionar la información, teniendo la necesidad de elegir entre distintas opciones tecnológicas cuya característica sea la flexibilidad para migrar los datos según las necesidades, pero sin arriesgar la seguridad. En este sentido, es importante resaltar el apoyo que otorgan otros derechos más fortalecidos como es el caso de los derechos ARCO, para asegurar la facilidad de la migración de datos y aplicaciones de un proveedor a otro.

1.5.7.2. Obligaciones del sector público sobre el derecho de portabilidad

Es importante destacar los esfuerzos por parte del Gobierno mexicano para fortalecer temas como el de la portabilidad, como es el caso de los Lineamientos para el ejercicio de este derecho que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales,[37] lo cual significa un buen ejercicio para que las entidades federativas y las dependencias gubernamentales puedan ejercer su responsabilidad en el ejercicio de este derecho. En este sentido, el sector público tiene una gran oportunidad, para lo cual debe considerar las siguientes obligaciones:

- La Administración Pública Federal no puede apropiarse de la modernización tecnológica sin antes conocer el entorno y sus particularidades. Por lo tanto, es responsabilidad del sector público capacitarse en el uso de las nuevas tecnologías de la información que facilitan la interconexión de fuentes de datos gubernamentales antes aisladas.
- Como parte de la diseminación del conocimiento, las entidades federativas y las dependencias deben propiciar los canales de comunicación para dar a conocer los derechos en la protección de datos personales, que repercutan de forma directa en la administración y sus ciudadanos, en sectores como la investigación científica, la seguridad y todos aquellos servicios públicos que se benefician del uso de servicios del cómputo en la nube.
- Establecer el cumplimiento de estándares formales de portabilidad para no dificultar la migración de un servicio a otro. Una solución puede ser que los responsables adopten estrategias propias para no depender de un único proveedor o para utilizar múltiples proveedores.

---

[37] acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, Diario Oficial de la Federación, 12 de febrero de 2018, disponible en: *http://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018*. (Fecha de consulta: 25 de agosto de 2018).

- Invertir en la capacitación del personal de las dependencias y entidades para establecer buenas prácticas en la elaboración de contratos, a fin de mitigar posibles daños al ejercer este derecho a la portabilidad.

1.6. Conclusiones

Una vez que tenemos claro que un contrato administrativo es un acuerdo de voluntades que contiene derechos y obligaciones, que éstos son el instrumento jurídico que celebra el Estado con particulares para obtener bienes y servicios que resultan necesarios para cumplir con su obligación de brindar servicios a sus gobernados, los contratos administrativos solamente pueden ser formalizados por aquellos servidores públicos con facultades conferidas en ordenamiento legal, exprofeso para ello, es decir, si bien los contratos administrativos los celebra el Estado en ejercicio de sus facultades, no cualquier servidor público puede formalizarlos, resaltamos los principios del contrato administrativo: legalidad, en el que la Administración Pública Federal solamente puede hacer aquello que contempla la Ley; continuidad, que significa que sus efectos no pueden interrumpirse. Es decir, una vez celebrado el contrato, las obligaciones deben cumplimentarse y no puede interrumpirse por simple voluntad del particular; principio de mutabilidad, al igual que el anterior, solo interviene la voluntad del Estado para su modificación y; el principio de equilibrio financiero, es decir, se debe evitar un perjuicio financiero al Estado y, en caso de esto ser inevitable, procurar que se reduzca al mínimo indispensable, considerando, en todo momento, el interés público y beneficio social.

Identificamos que para la celebración de un contrato administrativo, el Estado requiere previo a su formalización, llevar a cabo un procedimiento de contratación, ya sea licitación pública, nacional o internacional, en la que libremente puede participar cualquier persona física o moral que no esté inhabilitado por resolución de la Secretaría de la Función Pública y que su actividad esté directamente relacionada con el bien o servicio objeto de la contratación; invitación a cuando menos tres personas, en el que el Estado invita a determinadas personas físicas o

morales cuya actividad comercial esté directamente relacionada con el objeto de contratación y que cuenten con capacidad de respuesta inmediata, garantizando al Estado las mejores condiciones en cuanto oportunidad, eficiencia y eficacia y; por último, la adjudicación directa, procedimiento mediante el cual, el Estado adjudica a aquella persona física o moral que oferte el mejor precio, precisamos que para que opere la adjudicación directa, el importe adjudicado, no debe rebasar el monto máximo de actuación que conforme al Presupuesto de Egresos de la Federación para el ejercicio fiscal que corresponda autorice el Comité de Adquisiciones, Arrendamientos y Servicios, Arrendamientos y Servicios de la Dependencia o Entidad correspondiente

Tal como se mencionó en uno de los objetivos del presente capítulo, una vez identificados los diferentes tipos de contratos administrativos, los procedimientos de contratación que debe implementar el Estado, las principales cláusulas que debe contener un contrato de servicios de cómputo en la nube, las diversas consideraciones jurídicas a observar en los contratos de cómputo en la nube, así como la importancia que reviste el anexo técnico que utiliza el Estado como base fundamental para la contratación de servicios, la interacción que debe existir entre las áreas técnicas y contratantes en este tipo de servicios, destaca el control de la información, el aprovechamiento de las herramientas tecnológicas, garantizando la continuidad de la operación al interior de la dependencia o entidad, cuidando la interoperabilidad, portabilidad, seguridad, confiabilidad e integridad de la información.

Esto último se logra considerando, en la contratación de los servicios de cómputo en la nube, el cifrado de la información para evitar robo, perdida o violación a la misma, implementando políticas de seguridad y monitoreo constante con información medible y cuantificable de ataques y disponibilidad, así como desempeño y disponibilidad, niveles de servicio y mantenimiento y, actualización de infraestructura, entendiéndose ésta el software, licenciamiento y parches necesarios para el adecuado funcionamiento del servicio.

Capítulo 2

La protección de datos personales y áreas de oportunidad en los procedimientos de contratación pública de servicios de la nube de la Administración Pública Federal

Capítulo 2. La protección de datos personales y áreas de oportunidad en los procedimientos de contratación pública de servicios de la nube de la Administración Pública Federal

2.1. Resumen

En el presente capítulo haremos un recorrido por la evolución de la legislación mexicana para garantizar a sus gobernados la protección de su información personal, así como para el ejercicio de su derecho a estar informados sobre el quehacer de la Administración Pública; este último aspecto, solo será mencionado ya que el presente trabajo versa sobre la contratación de servicios de cómputo en la nube por parte de la Administración Pública. Señalaremos cuáles, a nuestra consideración, son las cláusulas que deben contener los contratos con el fin de "blindarlos", los requisitos a cubrir, así como los aspectos a considerar para proteger los datos personales a que tiene acceso la Administración Pública Federal, así como las áreas de oportunidad en la celebración de dichos contratos.

De igual forma, mencionaremos algunos obstáculos jurisdiccionales que pudieran encontrarse en la contratación de servicios de cómputo en la nube y la importancia que reviste el que México se haya adherido al Convenio 108, lo complejo que puede ser la sobre regulación en la celebración de contratos con la Administración Pública; así como la importancia del estricto cumplimiento de las Leyes sobre la protección de datos personales para brindar, por parte del Estado, la garantía y certeza jurídica a sus gobernados que sus datos personales estarán protegidos, sin olvidar la aplicación de los criterios recomendados por el INAI.

2.2. Objetivos

1) Conocer la normativa relacionada con la protección de datos personales aplicable en México para robustecer y brindar seguridad jurídica a la Administración Pública Federal en este tipo de contrataciones, como

consecuencia de la intervención de terceros en el tratamiento de datos personales.

2) Resaltar los aspectos básicos a considerar en la contratación de servicios de cómputo en la nube, tales como seguridad, propiedad intelectual y niveles de servicio.
3) Señalar las responsabilidades y obligaciones al contratar servicios de cómputo en la nube.
4) Identificar las áreas de oportunidad en materia de contrataciones públicas en México con el fin de hacer un buen uso de los recursos con que cuenta el Estado al contratar servicios de cómputo en la nube.

2.3. La protección de datos personales y áreas de oportunidad en los procedimientos de contratación pública de servicios de la nube de la Administración Pública Federal

El origen del derecho al acceso a la información es relativamente nuevo. Sin embargo, durante la última década su importancia ha aumentado al grado de reconocerse como un derecho fundamental por los ordenamientos internacionales sobre derechos humanos. En una vertiente de contención, contrapeso y vigilancia, que, de acuerdo con los modelos internacionales, debe tener todo Estado moderno democrático.[38]

De este modo, la trayectoria de la protección de datos personales acontece con la publicación de instrumentos internacionales como el Pacto Internacional de Derechos Civiles y Políticos de 1966, el cual desarrolla los derechos civiles y políticos y las libertades recogidas en la Declaración Universal de los Derechos Humanos y la Convención Americana sobre los Derechos Humanos de 1969, que constituyen el eje principal del sistema interamericano de protección de los derechos humanos.

[38] Rabindranath Guadarrama Martínez, Secretaría de Gobernación, Orden jurídico Nacional, Antecedentes de la Ley federal de Transparencia y acceso a la información pública gubernamental, Disponible en *http://www.ordenjuridico.gob.mx/Congreso/pdf/39.pdf* (Fecha de consulta: 25 de agosto de 2019)

No obstante, el impacto de este derecho ha sido tan importante que en México ya se han realizado importantes esfuerzos: antes de la aprobación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en 2001, se promueve la primera iniciativa de Ley para la protección de datos personales. A partir de entonces surgieron diferentes iniciativas, ocho en total, que por su irrelevancia no se citan. Sin embargo, cabe destacar que no prosperaron debido a la fluctuación entre la garantía de la protección de datos y el enfoque liberalizado, el cual no planteaba puntos mínimos regulatorios ni otorgaba certeza al titular.

Posteriormente, en abril de 2009 la Comisión de Gobernación de la Cámara de Diputados de la LX Legislatura, aprueba un dictamen que no logra ser discutido en el Pleno debido a la epidemia de influenza, razón ajena al ámbito parlamentario. No obstante, debido a la relevancia del tema, el 27 de abril de 2010 el Congreso de la Unión aprueba la LFPDPPP, decisión que permite a México ser parte de los regímenes que promueven el derecho a la protección de datos personales, derechos propios de las democracias en el mundo.

Así, el 5 de julio de 2010 se publica en el *Diario Oficial de la Federación* la LFPDPPP, cuyo ámbito de aplicación corresponde a personas físicas o morales, que por sus actividades llevan a cabo el tratamiento de datos personales. A partir de su publicación, esta Ley ha direccionado el panorama normativo de México a nivel nacional e internacional, lo cual ha coadyuvado a la implementación de mejores prácticas para garantizar la protección de datos personales en el país. No obstante, posterior a su publicación, la LFPDPPP ha tenido momentos trascendentales como a continuación se exponen:39

El 20 de julio de 2007 se reforma el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, con el objetivo de proteger los datos personales, lo que permitió, entre otras vicisitudes, que el Estado garantizara el derecho a la

39 Paloma Aviles,2013, ContadorMX, Ejemplos de aviso de privacidad y para la protección de datos personales en México. Disponible en: https://contadormx.com/2013/05/06/ejemplos-de-aviso-de-privacidad-y-para-la-proteccion-de-datos-personales-en-mexico. (Fecha de consulta: 25 de agosto de 2018).

información. Se reforman las fracciones I y II en las que, expresamente, se reconoce el derecho a la protección de datos personales. Puntualmente, estas fracciones señalan que la información a la que se refiere la vida privada será protegida en términos de la Ley y que toda persona tiene derecho a acceder y rectificar sus datos personales.

El 30 de abril de 2009 se publica la reforma constitucional al artículo 73 que otorga facultades al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de los particulares.

El 1o. de junio de 2009 se reforma el artículo 16 constitucional a efecto de que los encargados de la información emitan el "aviso de privacidad" para otorgarle garantía constitucional a la privacidad. Con estas modificaciones, se refuerza el marco jurídico de México en materia de protección de datos personales. No obstante, la LFPDPPP aún debe perfeccionar otros aspectos como la propiedad intelectual; de igual forma, los conceptos emergentes derivados del desarrollo tecnológico como en los temas de inteligencia artificial y el blockchain en el tratamiento de los datos.

Con la finalidad de complementar la estructura jurídica relacionada con la protección de datos personales e identificar el punto medio entre la protección y la reducción en el impacto por los costos de cumplimiento para los sujetos regulados por la LFPDPPP, se publicó el Reglamento de la LFPDPPP,[40] en el cual es posible encontrar temas relacionados con las tecnologías de la información; siendo uno de ellos el cómputo en la nube, el cual es definido en el Reglamento como un "modelo de provisión externa de servicios de cómputo bajo demanda. Es decir, que el suministro de infraestructura, plataforma o *software*, se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos dinámicamente compartidos".

Complementando lo anterior, el artículo 52 del Reglamento señala que el responsable puede hacer uso de los servicios del encargado, siempre y cuando se cumpla con una serie de condiciones y se cuente con mecanismos específicos para

[40] Reglamento de la Ley Federal de Protección de Datos en Posesión de Particulares, Diario Oficial de la Federación, México, 21 de diciembre de 2011.

la contratación de estos servicios. Por ejemplo, respecto de las condiciones de seguridad de la información, en el Reglamento se exhorta la existencia de la transparencia en las subcontrataciones que involucren la información sobre la que se presta el servicio. Por otra parte, con respecto a los mecanismos, se impide el acceso a los datos personales a cualquier persona que no esté autorizada.

Finalmente, en torno a la autoridad competente que regula el cómputo en la nube, el Reglamento establece que serán las dependencias reguladoras en conjunto con el INAI los encargados de emitir los criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube.

2.4. Consideraciones para adecuar la normativa para la contratación pública del cómputo en la nube

Si bien, México cuenta con un marco regulatorio en protección de datos personales, la normativa no profundiza en las particularidades del cómputo en la nube. Esta insuficiencia propicia la pérdida del dinamismo y la flexibilidad para legislar este concepto jurídico en México. Así, en opinión de los expertos para hacer frente a los retos que demandan las TIC, es pertinente que en el ámbito legal exista una normativa transversal que considere los continuos cambios tecnológicos que se están generando en la industria.

De la misma forma, debido a que el desarrollo de tecnología en México no es el mismo que el de Estados Unidos o Europa, conjuntamente el retraso en esta materia se ha afectado, entre otros motivos, por la falta de proyectos de Ley que avalen el uso de tecnología emergente como es el caso del cómputo en la nube. En este sentido, el avance de la legislación es más pausado de lo que la industria necesita. Por este motivo, los expertos en la materia opinan que es inevitable que esos inhibidores evolucionen.[41]

A pesar de lo anterior, no todo está en contra de la normativa mexicana, ya que sería una tercera opción entre el enfoque apropiado que prevalece en Estados

[41] Expansión SA de CV, México, líder de cloud computing en AL, México, 2011. Disponible en: https://expansion.mx/tecnologia/2011/08/24/mexico-lider-de-cloud-computing-en-al. (Fecha de consulta: 25 de agosto de 2018).

Unidos y el enfoque prescriptivo que se estila en Europa. En tanto que la jurisdicción mexicana proporciona mayor flexibilidad en la transferencia internacional de datos y defiende el principio del consentimiento que puede ser obtenido tácticamente a través de una divulgación apropiada en un aviso de privacidad.[42]

Por ello, en un escenario ideal el marco jurídico tendría que evolucionar a la par del desarrollo tecnológico considerando tópicos tales como propiedad intelectual, fortalecimiento de la seguridad y/o virtualización, toda vez que, desde el momento en el que la autoridad decide contratar los servicios de la nube, se obliga a adoptar condiciones en función de sus necesidades, las cuales son diversas y se relacionan con el cumplimiento de las cláusulas contractuales.

De modo que, si las cláusulas no son claras y la normativa jurídica del cómputo en la nube no es robusta, se propicia que en el proceso de contratación ninguna de las partes tenga la certeza de sus obligaciones específicas a cumplir. En virtud de ello, la Administración Pública Federal ha externado que esas necesidades se pueden satisfacer con mejores contratos de cómputo en la nube si se atienden las siguientes recomendaciones:

Consideraciones	Evidencias	Propuesta
Aspectos básicos legales de la contratación pública y referente al cómputo en la nube.	La falta de claridad en los contratos y el desconocimiento legislativo en la materia conlleva a que las partes firmen sin tener plena conciencia.	No es funcional contar con la mejor de las Leyes, si ésta no puede ser aplicada en un contrato. Por lo tanto, es conveniente que la legislación mexicana exija algún requisito que otorgue la participación de los interesados en la

[42] Horacio E. Gutiérrez, Daniel Korn, Universidad Externado de Colombia, Facilitando “the cloud”: la regulación de la protección de datos como motor de la competitividad nacional en América Latina. Disponible en *https://revistas.uexternado.edu.co/index.php/propin/article/view/3908/4344* (Fecha de consulta: 25 de agosto de 2018).

		celebración de un contrato de cómputo en la nube.
Obstáculos de jurisdicción para regular un campo que está en constante evolución.	La incertidumbre en torno a la jurisdicción y la complejidad del marco jurídico que envuelve el contexto del cómputo en la nube en México.	Es pertinente que la normativa nacional legisle las tecnologías de la información y la comunicación, de modo que la regulación no llegue a ser obsoleta y se puedan minimizar las brechas entre el marco legal y su aplicación. Por ejemplo, la privacidad, el robo de datos y la propiedad intelectual. Asimismo, es posible alinear las cláusulas con la legislación para aplicarla a los proveedores pertenecientes a empresas radicadas en México.
Implementación de cláusulas específicas que no dejen espacio a la interpretación o duda.	Desde la perspectiva jurídica queda muy claro cuáles son los objetivos del contrato. Sin embargo, para las demás partes interesadas, no siempre se conciben las especificaciones de los servicios de cómputo en la nube que se contratan. De la misma forma, es importante evitar contratos que	Si bien los anexos pueden resolver las dudas respecto de cuestiones técnicas, es conveniente que los contratos hagan mención respecto de los términos clave. Es decir, aunque la justificación de las responsabilidades se encuentra expresa en la Ley, resulta útil que por tratarse

	contengan cláusulas que parezcan inapropiadas o imposibles de aplicar y, en algunos casos, ilegales.	de un tema técnico-jurídico se opte por ser un análisis detallado que respalda, en gran medida, los intereses e inquietudes expresados por las partes interesadas.
La efectividad del marco de protección de datos a nivel internacional.	Existen casos de contratos en los que las empresas transnacionales protegen los contratos de servicios de cómputo en la nube por la efectividad de sus cláusulas, las cuales se amparan bajo la adopción de un marco universal que otorga certeza jurídica en la materia.	Considerar la jurisdicción internacional como parte de la naturaleza transfronteriza del cómputo en la nube. La adopción de estándares internacionales en materia de tratamiento, seguridad y privacidad de la información, así como el cumplimiento de los derechos de propiedad intelectual.
Disconformidades antes y durante el proceso de contratación de servicios de cómputo en la nube.	Falta de compromiso por parte del encargado para consumar sus obligaciones, aun cuando puedan adquirir la protección en una jurisdicción distinta a la del responsable.	Establecer mecanismos para la solución de controversias de modo que no quede en segundo plano tan relevante aspecto, cuya importancia garantiza el compromiso entre las partes. Así, la solución de controversias y las herramientas para la gestión y solución de la misma manera constituye un elemento fundamental para garantizar el éxito de los

		servicios de cómputo en la nube.
Estado actual de la normativa mexicana respecto de la emisión de mejores reglas y disposiciones para asegurar la protección de datos personales.	La necesidad de ampliar la normativa referente al cómputo en la nube, como manuales, guías, certificaciones o estándares para contratar servicios de cómputo en la nube.	Emitir disposiciones para la portación de datos personales en la nube, como en el caso de Europa que cuenta con el Almacenamiento Cloud de Normas Europeas. Si bien el INAI es el organismo encargado de velar por el cumplimiento de la LFPDPPP, no obstante, es pertinente aumentar una función especializada para el tratamiento y protección de datos en la nube. Mediante este mecanismo se coadyuva a disminuir los riegos de transparencia y falta de control.

Cuadro 7. Cláusulas recomendadas.

Fuente: elaboración propia.

Además de lo que muestra el cuadro anterior, es importante evitar la sobrerregulación de la contratación pública, ya que ésta pudiera ser un freno para el desarrollo y la innovación tecnológica. Es decir, aun teniendo la mejor posición, como el caso de España que se encuentra entre los cuatro países del mundo más rigurosos en la protección de datos personales, el negocio de la nube pública está

en riesgo, ya que la contratación se facilita con empresas cuyos centros de procesos de datos no se encuentran en el propio país.[43]

2.5. Aspectos que los responsables del cómputo en la nube deben considerar para proteger los datos de sus clientes

De conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el responsable del tratamiento de los datos es quien generará el aviso de privacidad. El cual es un instrumento que describe de manera general las medidas de seguridad, técnicas, físicas y administrativas, adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee. En este sentido, la Ley establece que la figura del responsable incluye a todos los sujetos obligados que deciden sobre el tratamiento de los datos personales.

Además de lo que establece el principio, la figura del responsable tiene la obligación de informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que sean sometidos los datos personales, a fin de que pueda tomar decisiones informadas al respecto.

No obstante, específicamente en el tema de contratación de cómputo en la nube, el responsable de los datos debe considerar otros aspectos a fin de generar confianza entre los encargados del tratamiento de la información. En virtud de ello, se propone que los siguientes debieran ser los aspectos para considerar por parte de los responsables para proteger los datos de sus clientes:[44]

Resulta importante identificar qué tipo de datos serán objeto de tratamiento en el cómputo en la nube, ya que esta decisión delimita el control de los datos. Es decir, el hecho de emitir criterios para el debido tratamiento de los datos personales servirá también para fomentar el cumplimiento de la normatividad sobre los mismos,

---

[43] PalblaDigital S.L., revista transformación digital, La computación en la nube en Europa y en España: una oportunidad de negocio, Disponible en: *https://www.revistatransformaciondigital.com/2014/03/18/httpwww-revistagestiondocumental-* (Fecha de consulta: 25 de agosto de 2018).

[44] Superintendencia de industria y comercio, Bogotá, Protección de los datos personales en los servicios de computación en la nube (cloud computing) Disponible en: *https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf* (Fecha de consulta: 25 de agosto de 2018).

lo que, además, contribuye a desarrollar una cultura de protección de datos en México.

El encargado y el responsable deben comprender los términos y condiciones del contrato de servicios en la nube, de modo que se garantice el cumplimiento del contrato, así como garantizar la seguridad física en los centros de procesamiento de datos. Limitar la finalidad del tratamiento facilita aplicar la política de privacidad para datos personales, así como para datos personales sensibles que se refieren a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o represente riesgo grave para el titular.

Reporte de los incidentes de seguridad por parte del responsable en función del tipo de tratamiento que realice el encargado. Es decir, si los datos personales transmitidos por el responsable al encargado se viesen destruidos, perdidos, difundidos o alterados, ya sea accidentalmente o por medio de una actuación ilícita, como el caso de un ciberataque, toda vez que una brecha de seguridad de este tipo de datos es susceptible de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Establecer la manera en la que el encargado apoyará al responsable frente al ejercicio de los derechos de los titulares. En este caso el responsable del tratamiento puede facilitar al interesado información relativa a su solicitud en un determinado plazo, dependiendo de la complejidad del agravio. No obstante, en el supuesto en el que no se le conceda el ejercicio del derecho, deberá haber retroalimentación entre el responsable y el encargado para conocer el entorno y motivos de la negativa.

Disponer claramente si habrá subcontratación y, de ser así, las condiciones que la regirán. Esto debido a que el cómputo en la nube ha dado lugar a numerosas innovaciones, motivo por el cual se prioriza la adquisición de servicios superiores basados en la nube por medio de servicios informáticos subcontratados para aumentar la velocidad y la eficiencia de los procesos.

De ser posible, averiguar la localización de los servidores utilizados por el encargado, en el caso de que se requiera por cuestiones legales, derivado de

alguna inconsistencia de la relación entre el responsable y el titular; de modo que puedan acceder las entidades competentes.

Con base en estas propuestas y con lo que la Ley determina, se comprueba que el responsable debe mantener una postura constante respecto del uso y tratamiento de los datos de los titulares; no debe perder de vista que es responsable del tratamiento de la información y, por ello, debe establecer obligaciones específicas al encargado, de tal manera que no se presenten incidencias en los servicios de cómputo en la nube contratados.

Por esta razón, antes de que el responsable decida contratar cualquier clase de servicios en la nube, debe asegurarse que el proveedor cumpla, de acuerdo con sus necesidades, no sólo con la infraestructura sino con cuestiones de reputación. Para ello, es preciso que se establezca un estudio de factibilidad técnica, operativa, económica y legal, de modo que se tenga certeza del compromiso y calidad por parte del encargado contratado para ejecutar los servicios de nube. La finalidad de este estudio es determinar si los datos en posesión del encargado cumplen con la normatividad vigente, aplicable al tratamiento de los datos personales.

2.6. Propuesta de requisitos a observar en la contratación de cómputo en la nube

En el entendido de que el cómputo en la nube implica riesgos en la protección de la información, resulta pertinente que el responsable ejerza plenamente sus obligaciones respecto de las particularidades de la contratación de servicios de cómputo en la nube. En este sentido, el ente público deberá ser capaz de identificar la información a almacenar, los propósitos del almacenamiento, así como las medidas de seguridad que implementará para proteger dicha información.

Cabe precisar que el tema de medidas de seguridad abarca aspectos de acceso, códigos de encriptación, anonimato, privacidad y copias de seguridad, además del reconocimiento de estándares y normas de seguridad que obliguen al encargado a su cumplimiento, adopción de responsabilidades, así como solucionar controversias y control de servicios sin omitir la transparencia en los procesos para migrar a la nube.

2.7. Medidas de seguridad

A causa del desarrollo tecnológico, la contratación del cómputo en la nube implica mayor exigencia respecto del aumento de los estándares de seguridad, interoperabilidad y portabilidad. Por este motivo, es obligación del responsable:

- Implementar una estrategia de Fortalecer el sistema de seguridad al interior de la Administración Pública Federal (APF) a monitoreo de seguridad para prevenir y dar respuesta a los incidentes de ataque cibernético. En este sentido, la estrategia coadyuva a automatizar la respuesta a incidentes alineada a las soluciones de seguridad de la nube disponibles por el proveedor.
- Verificar los estándares para certificar la seguridad en el servicio contratado, a través de normas oficiales como la Norma Mexicana NMX-I-27018-NYCE-2016, Tecnologías de la Información-Técnicas de Seguridad-Código de Práctica para la Protección de Datos Personales (DP) para Proveedores de Servicios de Nubes Públicas.[45] O bien, por los estándares internacionales que establece la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés).
- Obtener el mayor provecho de los servicios que ofertan los proveedores de cómputo en la nube. De este modo, no sólo mejora la calidad en el servicio por parte del Gobierno, sino que se promueve la transparencia, la rendición de cuentas y la seguridad en la prestación de servicios.
- través de un sistema de interoperabilidad bien estructurado, equipado con aplicaciones y software funcionales que eviten la duplicidad de información, para garantizar a las organizaciones gubernamentales la seguridad en el intercambio de información, pero, sobre todo, para garantizar al titular la protección de sus datos.

[45] Norma Mexicana NMX-I-27018-NYCE-2016, Tecnologías de la información-técnicas de seguridad-código de práctica para la protección de datos personales (DP) para proveedores de servicios de nubes públicas. *Diario Oficial de la Federación*, 26 de agosto de 2016, disponible en: *https://www.dof.gob.mx/nota_detalle.php?codigo=5449891&fecha=26/08/2016*. Fecha de consulta: 25 de agosto de 2018).

En el entendido de que los servicios de la nube son provistos como servicios estándar, pueden ser gestionados en línea y no requieren de la adquisición de tecnologías, debido a que la nube provee el servicio de forma inmediata, el responsable debe cerciorarse de que el encargado cuenta con los certificados para el funcionamiento de los servicios previstos.

Los sujetos obligados en el ámbito federal, estatal y municipal -tales como autoridades, entidades, órganos y organismos- y los terceros que se encuentran vinculados o relacionados con aquéllos por virtud de la formalización de un contrato de prestación de servicios derivado de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás normativa aplicable en contrataciones públicas; o bien, que tengan o presenten alguna relación por cualquier acto jurídico plenamente válido, existente y legal, tienen la obligación, en términos de lo ordenado en los artículos 1, 2 y 3, fracción XXVIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de proteger la información y los datos personales de los titulares de dichos datos.

Lo anterior se logra, entre otros supuestos, con la celebración de contratos en materia de cómputo en la nube, pues este tipo de acuerdo de voluntades actualizan y mejoran el ejercicio, el actuar y la toma de decisiones de la APF, a efecto de lograr una eficiencia en los procesos, no sólo administrativos, legales, financieros y técnicos, sino también operativos y de interdependencia en sus diversas plataformas tecnológicas, de aplicaciones de software y componentes habilitadores, fortaleciendo el servicio público en beneficio de los gobernados y por tanto, del orden social.

En razón de ello, los diversos servidores y funcionarios públicos que son responsables de la administración y verificación del cumplimiento de los contratos en materia de tecnología y, en particular, de los acuerdos de voluntades de cómputo en la nube, así como los responsables de la recepción, validación y aceptación de los servicios de TIC, conjuntamente con los altos ejecutivos con poder de decisión y de determinación de las políticas públicas en materia de innovación tecnológica, deben estrechar sus vínculos y enriquecer la comunicación para retroalimentarse constantemente en las oportunidades y beneficios que presenta las diversas

modalidades de contratación de servicios de cómputo en la nube; o bien, hacerse saber los inconvenientes de dichos acuerdos.

Uno de los elementos clave para el funcionamiento efectivo del cómputo en la nube es generar, en las partes, la certeza sobre las garantías de privacidad y seguridad en el servicio a contratar. Por este motivo, en los contratos se debe considerar una cláusula que establezca la obligación de garantizar la seguridad de los datos personales, tal como lo establecido el artículo 3o. de la LGPDPPSO para proteger la información, y considerar el riesgo existente, las posibles consecuencias para los interesados, la sensibilidad de los datos y el desarrollo tecnológico.

2.8. Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales que emite el INAI

El servicio de la nube pública se efectúa por medio de redes globales, dispuestas en centros de datos, que el Gobierno contrata por medio de los proveedores cuyos recursos tecnológicos y financieros necesarios les permiten albergar los centros de datos y la conectividad global que se precisan. La principal característica de los proveedores de servicios en la nube es la especialización en *hardware* y *software* para proteger la ciberseguridad de los cada vez más constantes y sofisticados ataques cibernéticos.

En vista de sus características, el cómputo en la nube representa una gran oportunidad no sólo en términos económicos, traducidos en la reducción de costos, sino en el aspecto tecnológico, porque implica una herramienta de apoyo para transformar la Administración Pública Federal en términos de eficiencia y eficacia.

No obstante, la decisión de contratar la nube pública no es una cuestión accidental, ya que el responsable debe actuar cautelosamente para determinar qué proveedor ofrece el mejor servicio. Asimismo, es muy importante la congruencia del encargado para asegurar a los titulares el ejercicio de su derecho a la protección de datos personales, a través de la facilitación de procesos tales como el tratamiento de éstos.

Ante dichas circunstancias, el INAI emitió los “Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales”, los cuales consideran que, tratándose de servicios de cómputo en la nube, las dependencias reguladoras, en colaboración con el Instituto, son quienes emiten los criterios para el debido tratamiento de datos personales.

2.8.1. Estructura de los criterios

El documento hace referencia al artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, respecto de determinados aspectos que debe cumplir el proveedor, tales como aplicar las políticas de protección de datos y guardar confidencialidad respecto de los datos personales, así como transparentar la información y abstenerse de asumir la titularidad de esta, cuando se trate de subcontratación.

Asimismo, el documento hace referencia a los mecanismos mínimos con los que debe contar el encargado para garantizar la protección de los datos personales. En este sentido, se establece que debe dar a conocer los cambios en la política de privacidad, limitar el tipo de tratamiento de los datos personales, así como establecer medidas adecuadas de seguridad. Sin embargo, a pesar de estas menciones, el apartado no complementa más de lo que establece el artículo, es decir, podría ser más específico para definir cuáles son los tipos de tratamiento de datos, en qué consisten las medidas de seguridad o qué implica que las medidas sean “adecuadas”.

Posteriormente, en la primera sección se hace referencia a las generalidades de los Criterios; destaca, además del fundamento jurídico relativo al artículo 52 del Reglamento, el gráfico siguiente, que muestra el nivel del control que tienen el proveedor y el cliente respecto de los recursos de cómputo y la información.

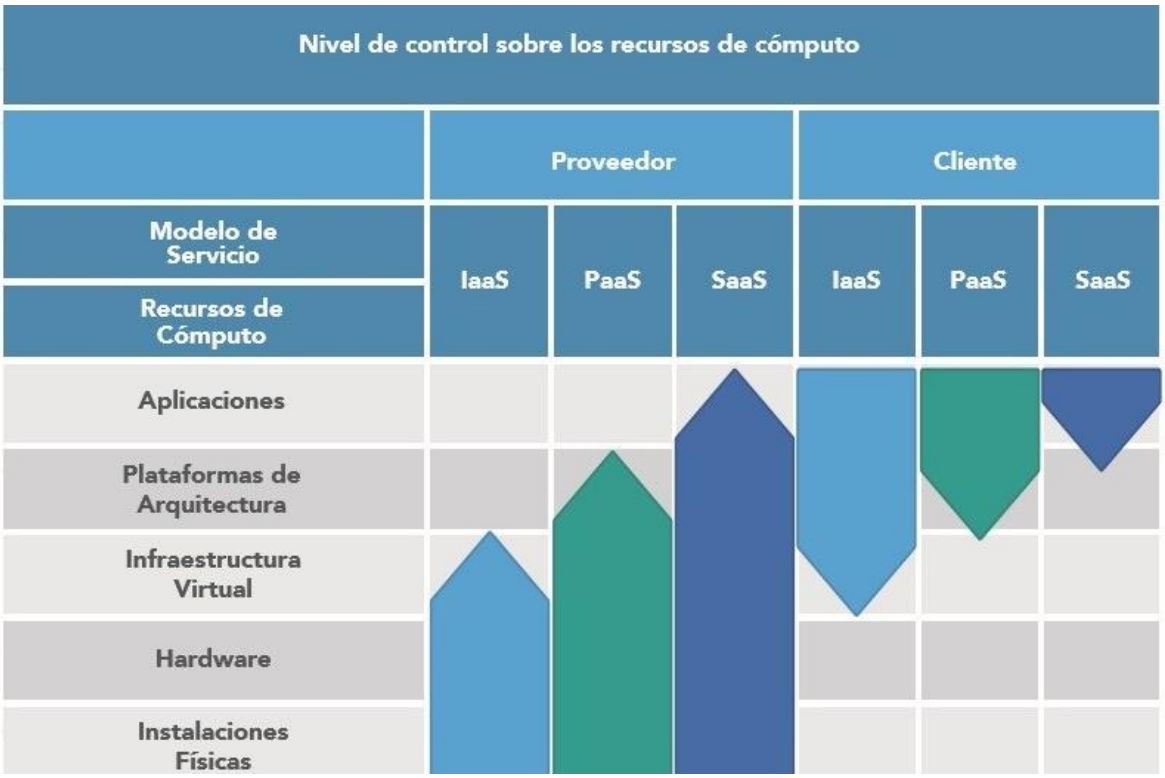

Figura 1 Nivel de Control sobre los recursos de cómputo[46]

En la imagen se puede observar que el nivel de control sobre la administración de los recursos de cómputo, por parte del encargado, aumenta de los servicios de infraestructura como servicio (IaaS, por sus siglas en inglés) a plataforma como servicio (PaaS), lo cual significa que el proveedor aumenta su intervención en el tratamiento de la información. Sin embargo, permitir que el proveedor intervenga en alguna fase del tratamiento de datos representa un riesgo paralelo al nivel de control sobre los recursos de cómputo.

Se sugiere consultar la *Guía para empresas en materia de protección de datos personales en el uso de cómputo en la nube*,[47] la cual es publicada por el

[46] Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, Secretaría de Economía, Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales, Disponible en *http://inicio.ifai.org.mx/nuevo/ComputoEnLaNube.pdf* (Fecha de consulta: 9 de noviembre de 2019).

[47] Secretaría de Economía, Prosoft industria 4.0 mx, Guía para empresas en materia de Protección de Datos Personales en el uso de Cómputo en la Nube. Disponible en https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_33.pdf. (Fecha de consulta: 9 de noviembre de 2019).

programa Prosoft de la Secretaría de Economía, y consta de 399 páginas en cuyo contenido se encuentra un *checklist* para la revisión del cumplimiento.

Por una parte, los Criterios muestran una lista de verificación, la cual únicamente se presenta como un extracto que a su vez se divide en un *checklist* general sobre cómputo en la nube y un *checklist* específico sobre el mismo tema. Ambas se incluyen como parte de los anexos en los Criterios; la finalidad de incluirlas es que las empresas evalúen, por sí mismas, su nivel de conocimiento y aplicación de la normatividad en materia de protección de datos personales en el cómputo en la nube. Lo interesante de estos *checklist* incluyen diversos entornos que corresponden a bloques de temas como:

Riesgos legales y regulatorios. En este apartado del listado, el sentido de las preguntas es sondear si la empresa ha adoptado, contratado o verificado medidas de seguridad para la protección de datos personales. Del mismo modo, las preguntas confrontan a la empresa en el supuesto que se presente algún tipo de incumplimiento por parte del proveedor o si cuenta con el aviso de privacidad. Asimismo, respecto a la parte técnica se cuestiona qué tanto conoce la empresa a su proveedor en relación con la evaluación de su desempeño o si cuenta con suficiente ancho de banda para brindar el servicio.

Protección de datos personales. Las preguntas que corresponden a esta sección del listado están orientadas a que el cliente identifique, en el contrato, su participación, así como la del proveedor. Es decir, que se establezca quién es el responsable y quién el encargado del tratamiento de datos personales. Básicamente la orientación de este apartado es de índole legal para que la empresa reconozca las medidas normativas necesarias para asegurar la protección de los datos.

Seguridad. Al igual que la protección de datos, las preguntas relativas a la seguridad responden a la aplicación de la normatividad, de modo que la empresa aplica algún mecanismo para albergar copias de seguridad, mecanismos de protección de identidad o medidas disciplinarias en caso de vulneración de la información. De la misma forma, se cuestiona a la empresa si cuenta con medidas

de seguridad para prevenir fuga de datos, o procedimientos para el manejo de fuga de datos o para la reparación de vulnerabilidades.

Propiedad intelectual. En este apartado las preguntas están dirigidas a la parte legal, particularmente en lo que respecta a la contratación de servicios de cómputo en la nube, es decir, si en los contratos se estipula a quién pertenecen los datos del usuario para no causar conflicto o se adquiera algún derecho de propiedad intelectual.

Igualmente, se cuestiona respecto de la prevención en transferencia o derechos de propiedad intelectual, o si al momento de contratar servicios la empresa cuenta con la obtención de licencias necesarias. Lo mismo aplica para el cumplimiento de la normativa para la gestión de activos de *software* y el aseguramiento de que el proveedor de servicios garantiza la confidencialidad respecto a la información sujeta a derechos de propiedad intelectual.

Acuerdo de Nivel de Servicio (SLA) y otras cuestiones contractuales. Las preguntas, en este punto, son del tipo contractual mencionando las cláusulas relativas a la interoperabilidad. Además, se incluyen preguntas respecto del nivel de servicio y las cláusulas legales y contractuales que garanticen al cliente la sanción del proveedor en caso de incumplir con sus obligaciones. De igual forma, se considera lo que ocurre al término del contrato, por ejemplo, si éste contiene previsiones sobre la finalización del mismo o si en el contrato, se establece la recuperación de la información por parte del cliente, para llevarla a otro proveedor si así lo desea. Ciberdelitos. En este apartado la empresa puede ampliar el panorama respecto del manejo de situaciones que implican ataques informáticos; al respecto, tendrá un diagnóstico de la situación del proveedor en torno a las medidas que implementa para dar respuesta a este tipo de incidentes.

En la segunda sección, el documento únicamente describe algunos puntos que el cliente debe tener en cuenta, antes de la contratación o adhesión a un servicio de cómputo en la nube, entre los que se encuentran los siguientes: identificar datos, procesos o funciones que se pretendan migrar al servicio de cómputo en la nube; definir el modelo de aprovisionamiento que garantice de mejor manera el control sobre el tratamiento de datos personales; definir de manera interna las políticas y

medidas de seguridad para el uso del servicio de cómputo en la nube, y evaluar los términos y condiciones a los que se sujeta el servicio a contratar.

Si bien las recomendaciones son puntuales, pudieran complementarse agregando el propósito de cada recomendación y cómo éste coadyuva a cumplir el propósito. Por este motivo, a continuación, se presenta la propuesta para complementar las recomendaciones anteriores con un enfoque específico a la contratación en el sector público:

Recomendación de los Criterios	Propuesta
I. Identifique los datos, procesos o funciones que se pretendan migrar al servicio de cómputo en la nube.	El responsable de la información deberá implantar mejores prácticas durante todas las etapas de migración de la información. Es decir, se clarificará la información por medio de estándares y preguntas centrales para contratar los servicios, para migrar hacia la nube de un tercero. De igual forma, se considerarán algunos factores como: ✓ El tiempo para realizar la migración completa. ✓ La cantidad de tiempo de inactividad que se requerirá. ✓ El riesgo derivado de problemas técnicos de compatibilidad, corrupción de datos, problemas de rendimiento de aplicaciones y pérdida u omisión de datos.
II. Defina el modelo de aprovisionamiento que garantice de mejor manera el control sobre el tratamiento de datos personales, según los datos, procesos o funciones que se pretenden migrar a la nube.	…La entidad de la Administración Pública Federal habrá de disponer de una política de seguridad de la información, basada en controles de seguridad y procesos de gestión de riesgos para el tratamiento de datos personales con base en lo indicado en los Lineamientos de la LGPDPPSO.
III. Defina, de manera interna, las políticas y medidas de seguridad para	…Las dependencias de la Administración Pública Federal Centralizada y Órganos Autónomos,

el uso del servicio de cómputo en la nube.	deberán mantener confidencialidad en la información generada al interior, solicitando a los proveedores que se comprometan contractualmente a obedecer la normativa mexicana para la protección y el tratamiento de datos personales.
IV. Evalúe todos los aspectos del servicio, así como los términos y condiciones a los que se sujeta el servicio a contratar.	…Disponer de un acuerdo contractual que evalúe el nivel de servicio del proveedor en el que queden claramente definidas las responsabilidades y condiciones del encargado. Como parte de la evaluación la Administración Pública Federal solicitar al encargado certificaciones de seguridad de la información reconocidos y basados en estándares internacionales como las Norma ISO: ✓ ISO/IEC 27001 Seguridad de la información. ✓ ISO/IEC 27017 Controles de seguridad de la información ✓ ISO/IEC 27002 específicamente para los servicios en nube ✓ ISO/IEC 27018 Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud.

Cuadro 8. Recomendaciones para la protección de datos personales en la contratación de servicios de cómputo en la nube.
Fuente: Elaboración propia con información de la Superintendencia Industria y Comercio del Gobierno de Colombia.

En la segunda sección de los Criterios, se encuentran las recomendaciones respecto de los criterios mínimos previos a la contratación o adhesión, la reputación del proveedor, transparencia en el servicio y cambios en los términos de los servicios. De igual forma, se establecen los criterios mínimos a considerar para asegurar que el proveedor cuenta con medidas de seguridad, la evaluación de

riesgos para los datos personales, la interoperabilidad y portabilidad, así como la adhesión o contratación del servicio.

En general, el contenido de esta sección se confina a la descripción de las recomendaciones. Sin embargo, llama la atención la mención que se hace respecto de la Ley Federal del Consumidor, la cual también se refiere a la contratación del cómputo en la nube, al establecer que, en un contrato de adhesión es posible utilizar formatos uniformes de términos y condiciones aplicables a la adquisición de un producto o a la prestación de un servicio, aun cuando dicho documento no contenga todas las cláusulas ordinarias de un contrato.

2.8.2. Acciones por evitar en la contratación de servicios de cómputo en la nube

Por último, la tercera sección corresponde a las acciones a evitar en la contratación de adhesión a servicios de cómputo en la nube. Dichas acciones suponen ser un complemento de los Criterios, a saber: *a)* no dar por hecho que los servicios de cómputo en la nube son temas exclusivos de los expertos en informática, sino que requieren un análisis integral de los involucrados en la organización; *b)* aseverar que la popularidad en el servicio de cómputo en la nube otorga calidad predeterminada; *c)* asentir que, por el hecho de ser gratuito, un servicio de cómputo en la nube no es conveniente, en este sentido, la recomendación que se hace es que se evalúen las condiciones y políticas de privacidad para evaluar los riesgos que se mencionan en los Criterios, y por último *d)* asumir que el tratamiento de información y operaciones del cliente deben estar en su totalidad en la nube. Al respecto el cliente debe evaluar las operaciones o los procesos que conviene optimizar a través del cómputo en la nube.

De igual forma, considerando la adaptabilidad de los criterios al caso del cómputo en la nube en el sector público, los mismos principios y deberes se encuentran en los principios y deberes de la LGPDPPSO en sus artículos 16 y 31 respectivamente. Sin embargo, en el documento de los Criterios, tanto los principios como los deberes sólo son descritos tal como se encuentran en ambas Leyes. Por

este motivo, se considera conveniente agregar algunas aportaciones para poner en práctica los principios como se muestra en el siguiente apartado.

2.9. Establecimiento de principios y deberes para el uso de servicios de cómputo en la nube en el sector público de México[48]

Los Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales, no imponen obligaciones. Sin embargo, dan lugar al complemento del marco regulatorio que resulte aplicable de acuerdo con la interpretación de los principios[49] inherentes al tratamiento de datos como se muestra a continuación:

Principios	Aportación para el tratamiento de datos en el cómputo en la nube
Licitud. Significa que el tratamiento de los datos personales se hace de forma lícita y legítima o leal, con apego a la normativa aplicable y conforme lo acordado entre el responsable del tratamiento y el titular de los datos personales.	En el cómputo en la nube el tratamiento de datos es lícito, excepto en actividades de las dependencias cuyas disposiciones prohíban ubicar determinada información en la nube.
Lealtad. Se refiere a que el tratamiento de datos personales, a lo largo del ciclo de vida de los datos personales, en todas las fases de su tratamiento, cumpla con las condiciones aplicables.	El tratamiento de datos supone la privacidad de los titulares y la confianza de que los datos serán tratados con base en la Ley. Por lo tanto, en el cómputo en la nube aumenta el

[48] Plataforma digital única del Estado Peruano gob.pe, Secretaría de Gobierno Digital de la presidencia del Consejo de ministros, Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano. Disponible en: *https://www.gob.pe/institucion/pcm/informes-publicaciones/268665-lineamientos-para-el-uso-de-servicios-en-la-nube-para-entidades-de-la-administracion-publica-del-estado-peruano* (Fecha de consulta: 22 de noviembre de 2019)

[49] Miguel Recio Gayo, INAI, *Principios y deberes en materia de Protección de Datos Personales* Disponible en: h*ttp://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Principios%20y%20deberes%20en%20materia%20de%20Proteccio%CC%81n%20de%20Datos%20Personales.pdf?sequence=1*. (Fecha de consulta: 22 de noviembre de 2019)

	compromiso del cumplimiento del marco normativo o de cualesquiera otras normas de aplicación, así como del correcto tratamiento de los datos. Asimismo, el cumplimiento recae en la entidad pública propietaria de la información, independientemente de la existencia de acuerdos, seguros u otras medidas compensatorias.
Consentimiento. Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de estos.	En el cómputo en la nube el consentimiento del titular es parte del procedimiento para el tratamiento de los datos. Sin embargo, el responsable no requiere el consentimiento del titular de los datos personales para tratar su información en la nube.
Información. El responsable del tratamiento debe informar al titular de los datos personales, qué datos personales obtiene y para qué los va a tratar.	La información en el cómputo en la nube no es una finalidad específica para el tratamiento de datos personales. De igual forma, respecto del aviso de privacidad destaca que no es necesario informar si los datos serán colocados o tratados en la nube.
Calidad. Este principio implica que los datos personales tratados deben ser exactos, completos, pertinentes, actualizados y correctos.	Para el caso del cómputo en la nube en la Administración Pública, la calidad significa que, cuando los datos personales hayan cumplido con su finalidad, éstos deben ser eliminados por el responsable. Derivado de ello, en los criterios se establece que el responsable debe cumplir con dos

	obligaciones (i) tomar las medidas pertinentes para que los datos sean correctamente utilizados y (ii) eliminar o suprimir los datos de las bases de datos cuando éstos ya no sean necesarios.
Finalidad. Es la manifestación esencial de la protección de la privacidad en relación con el tratamiento de los datos personales. Se trata de un principio clave interrelacionado con otros principios, especialmente los de información, consentimiento y calidad.	En el cómputo en la nube, el principio de finalidad coadyuva a unificar la finalidad del tratamiento con lo que le fue informado al titular en el aviso de privacidad. Asimismo, el responsable y el encargado deben evitar cualquier desvío de finalidades.
Responsabilidad. La responsabilidad de quien trata los datos personales es fundamental para la protección efectiva de la privacidad y de los datos.	Para garantizar el debido tratamiento de datos en el cómputo en la nube, el responsable debe instrumentar un procedimiento para atender puntualmente el riesgo por la implementación de nuevas tecnologías. En este sentido, las dependencias que contraten servicios de cómputo en la nube deben apegarse a lo que establece la normatividad, en particular la LGPDPPSO.

Cuadro 10. Principios para el tratamiento de datos en el cómputo en la nube.
Fuente: elaboración propia con información del INAI[50]

De igual forma, resulta necesario considerar los deberes que señala la LGPDPPSO: Deber de confidencialidad. Por otra parte, los Criterios establecen que el deber de confidencialidad implica la obligación de guardar discreción respecto del

[50] Instituto Nacional de transparencia Acceso a la Información y Protección de Datos Personales, Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de datos personales, disponible en: http://inicio.ifai.org.mx/nuevo/ComputoEnLaNube.pdf (Fecha de consulta: 11 de diciembre de 2019)

tratamiento en los datos personales. En el caso del cómputo en la nube, el responsable debe adoptar las medidas necesarias para obligar al encargado, quien tiene acceso y lleva a cabo el tratamiento de datos personales, a observar la debida confidencialidad, aun terminada la relación jurídica. Por lo que resulta necesario adoptar medidas contractuales que establezcan derechos y obligaciones de las partes involucradas en el contrato de servicios de cómputo en la nube. Asimismo, en los Criterios se destaca la importancia de que, en el propio contrato, convenio o incluso en un anexo, se establezca una condición que prohíba al encargado asumir la propiedad de la información del titular o la que se genera en la nube.

Igual importancia requiere considerar que el nivel de compromiso de ambas partes dependerá del tipo de desarrollo entre la nube y la Administración Pública, y encontrar un punto medio para compartir la responsabilidad con el encargado. Adicionalmente, vale la pena resaltar que, si no se garantiza la confidencialidad de los servicios, datos e información soportada por servicios en la nube, en última instancia, podría resultar en mayores costos, afectación de la imagen y pérdida de los beneficios esperados.

Deber de Seguridad. Si bien la responsabilidad respecto de la seguridad en el tratamiento de la información es propia de cada una de las partes, las medidas de seguridad técnicas, físicas y administrativas deben ser ejercidas por ambas, de modo que se pueda proteger el daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado. En este sentido, la contratación de servicios de cómputo en la nube estará muy relacionada con las medidas de seguridad y éstas a su vez con la legislación y normativa vigente. De igual forma, los entes públicos deberán clasificar sus sistemas según las normas internacionales de seguridad de la información. Lo mismo para el caso de los requisitos o niveles de seguridad que deben especificar los términos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, ya sea que correspondan al ente público o al encargado.

2.9.1. Recomendaciones

El responsable debe considerar que, en la contratación de servicios en la nube, uno de los criterios más importantes es el relacionado al tipo de información o al contenido de los datos personales que el encargado de los servicios de la nube almacenará o procesará. Motivo por el cual, los encargados deberán proporcionar información detallada de cómo llevarán a cabo el tratamiento de datos.

Es necesario que la Administración Pública Federal mantenga el control total y la propiedad sobre sus datos. Asimismo, debe tener la posibilidad de elegir, de acuerdo con evaluaciones de riesgo e impacto, la ubicación geográfica en la que se puedan almacenar los mismos. Por otro lado, los proveedores de servicios en la nube deberán proporcionar controles de identidad y acceso para restringir el acceso a la infraestructura y los datos del cliente, atendiendo para tal efecto, los estándares de cumplimiento y observar las políticas de seguridad y cumplimiento de la nube, como visibilidad, control y auditoría.

Los entes de la Administración Pública Federal que opten por el servicio de cómputo en la nube deberán analizar con detalle qué tipo de datos personales son susceptibles de ser transferidos a dichos servicios, y antes de la contratación de servicios en la nube, tener claro el control necesario para el tratamiento de datos, dependiendo del tipo de servicios en la nube y de los tipos de datos que se procesen. En este sentido, podrán distinguir que la oferta del encargado incluya elementos relacionados a la información, ubicación del tratamiento de datos, existencia de subencargados, políticas de seguridad, derecho del usuario y obligaciones legales, de tal forma que coadyuven al tratamiento de los datos.

Con respecto a la etapa de contratación de servicios en la nube, la Administración Pública Federal debe conocer, por lo menos, los Acuerdos de Nivel de Servicio (ANS) con el objeto de establecer una serie de requisitos contractuales en la prestación del servicio, debiendo contemplar las características de este, las responsabilidades de ambas partes, los modelos de nube, los términos y condiciones, precios y seguridad, entre otros.

Responsabilidades. Es responsabilidad de la Administración Pública Federal observar las disposiciones legales vigentes de la contratación pública, así como

tomar las previsiones respecto de la celebración de contratos en donde el responsable se encargará de ejecutar la totalidad de sus obligaciones y responsabilidades; lo mismo para el encargado. El responsable deberá realizar el análisis de mercado, determinando y comparando de forma previa, de acuerdo con lo establecido en la Ley de Adquisiciones.

Resulta de vital importancia que la Administración Pública Federal determine si el servicio a contratarse será nube pública, nube privada, nube híbrida u otra modalidad previamente acordada, así como establecer la disponibilidad de la portabilidad de la información por parte del encargado, estableciendo los accesos y limitaciones respecto del tratamiento de datos.

Obligaciones*.* Entre las obligaciones se encuentran las siguientes: implementar el análisis y gestión de riesgos sobre el tratamiento de datos en el servicio de cómputo en la nube; coadyuvar a la protección de la información considerando el cifrado, tanto de los datos en tránsito como de los datos almacenados, garantizando de esta forma los ocho principios para el tratamiento de datos, así como los deberes que avalen su plena disponibilidad e integridad; implementar el análisis de seguridad del servicio para lo cual se puede adecuar la gestión de las incidencias de seguridad y mecanismos que garanticen la seguridad en el tratamiento de datos en caso de catástrofes o incidentes, y garantizar la realización de auditorías de seguridad ordinaria y extraordinaria, incluyendo destinatarios de las auditorias y conclusiones, a través de una auditoría de seguridad.

Ahora bien, los Criterios emitidos por el INAI son de gran utilidad para adaptarlos e implementarlos en la contratación de servicios de cómputo en la nube en el sector público. No obstante, sería conveniente que obtuvieran validez jurídica como parte integral de los Lineamientos de la LGPDPPSO, justamente para ayudar a disminuir la afectación en seguridad y a cumplir los objetivos del marco regulatorio en materia de protección de datos, los Criterios pueden llegar a ser un ejemplo de buenas prácticas para favorecer la disminución de contratiempos, a través de las siguientes acciones por parte de la Administración Pública:

1. Efectuar un análisis integral que incluya cumplimientos legales, buenas prácticas y la gestión de calidad en los servicios.
2. Evaluar los servicios de cómputo en la nube ya que por popularidad o tendencia no siempre son la mejor opción para otorgar el servicio en cierto tipo de datos o procesos.
3. Revisar cuidadosamente las condiciones del servicio a contratar, así como las cuestiones de seguridad y tratamiento de datos personales que ofrece el encargado.
4. Ponderar las operaciones o procesos que conviene optimizar a través del servicio de cómputo en la nube en el tratamiento de los datos personales.

Si bien, los criterios emitidos en la Guía son una extensión de los principios y deberes de protección de datos personales, así como los deberes de confidencialidad, seguridad, notificación de vulneraciones y el ejercicio de los derechos ARCO, el Estado actual del derecho a la protección de datos personales en México tiene la posibilidad de complementarse por el material elaborado por el INAI, ya que se trata del organismo garante más importante en este rubro.

Por tanto, la inclusión de temas tecnológicos, como es el caso del cómputo en la nube, no sólo debe ser parte de una guía, sino buscar la forma de integrarlos dentro de la normativa nacional aplicable a la protección de datos personales. Por otro lado, aunque el documento original está creado para orientar a los particulares en la contratación de cómputo en la nube, éste podría adaptarse a las necesidades de los responsables de la contratación en el sector público, entendiéndose como responsables quienes intervienen en la adopción y cumplimiento de prácticas, específicamente cuando el responsable del tratamiento de datos personales contrata servicios de cómputo en la nube. Valdría la pena retomar el caso de la Secretaría de Gobernación (SEGOB) “Implementación del Servicio Nacional de Identificación Personal y eventual Expedición de la Cédula de Identidad Ciudadana y Persona”, el cual fue difícil concretar toda vez que, en la verificación al cumplimiento de los principios de protección de datos personales, en la implementación del proyecto por parte del INAI, se detectaron vulnerabilidades, entre las que destacan: *lealtad*, al recabar los datos personales, la Secretaría no lo

hizo de manera engañosa, justificó que era necesario para cumplir con una de sus facultades; *consentimiento*, si bien, la Secretaría tenía previstos formatos para recabar el consentimiento de los titulares, el INAI se pronunció en el sentido de que la Secretaría debería incluir en dichos formatos que los datos personales recabados serán tratados y protegidos en términos de los principios de protección contenidos en la Ley y demás normatividad aplicable, así como los derechos conferidos al titular y los medios a través de los cuales pueden ejercerlos; *calidad*, es de llamar la atención el que, uno de los argumentos de la SEGOB para recabar datos biométricos fue que el registro del nacimiento de las personas no era exacto; *proporcionalidad*, el recabar catorce datos biométricos de los ciudadanos no estaba debidamente justificado por la SEGOB, con lo que no se cumplía con este principio, y por último, en cuanto al principio de *información*, la SEGOB no cumplía a cabalidad con el mismo, ya que el INAI recomendó incorporar en los formatos de solicitud, además de los elementos ya incluidos, el compromiso de que los datos personales recabados serían tratados y protegidos en términos de los principios de protección contenidos en la Ley y demás normatividad aplicable, así como los derechos conferidos al titular y los medios a través del cuales podrían ejercerlos.

Una de las principales preocupaciones del caso, fue que la SEGOB tenía planeado al 100% el proyecto del “sistema”, pero no así la contratación del proveedor que lo llevaría a cabo, razón por la cual en la presente investigación se hace énfasis en los aspectos a considerar cuando la Administración Pública Federal contrate servicios de cómputo en la nube.

Por ejemplo, entre los aspectos más relevantes que pueden ser considerados por los responsables está el elegir a aquellos proveedores que operan bajo normas mexicanas y que cumplan con estándares internacionales para proteger los datos personales en su posesión. Por tanto, se concluye que tanto los criterios para la protección de datos como los anexos y los *checklists* son herramientas útiles para optimizar el tratamiento de datos personales evitando el incumplimiento del principio de calidad o ser objeto de ataques cibernéticos.

2.10.Áreas de oportunidad en las dependencias y entidades en materia de contrataciones públicas

El Estado tradicionalmente realiza sus contrataciones a través de licitaciones públicas; siguiendo procedimientos estandarizados para la adquisición de bienes y contratación de servicios y obra pública, para lo cual, puede realizar sus contrataciones a través de licitación pública, invitación a cuando menos tres personas o adjudicación directa.

Aunque la estructura de las contrataciones muestra contundencia y simpleza, en la práctica no ocurre así, debido a que, en algunos casos, su ejecución se favorece de manera parcial. Por ejemplo, en el caso de la adjudicación directa cuyo procedimiento garantiza como regla general la obtención de las mejores condiciones de contratación con prontitud y eficacia, en seguimiento de la política general de contrataciones públicas, los expertos señalan que no es recomendable utilizar el procedimiento de adjudicación directa, particularmente cuando las condiciones de participación favorecen a un solo proveedor, contratista o incluso al propio Gobierno.

2.10.1.Normativa que rige las contrataciones públicas en México

Así, con todo y sus excepciones, la contratación pública en México se caracteriza por tener forma jurídica y una garantía de orden administrativo que coadyuva a que la sociedad crea en la honestidad de las autoridades responsables. Es decir, la principal encomienda de la licitación pública es generar la confianza en la correcta administración de los recursos de los que dispone el Estado.[51] Por lo tanto, es fundamental que las autoridades responsables conozcan la normativa en esta materia.

En efecto, jurídicamente las contrataciones son de suma importancia debido a que éstas constituyen una de las principales actividades económicas del Gobierno y son un elemento fundamental para la ejecución del gasto público. En este sentido,

[51]Carlos Matute González, El Universal, Compañía periodística Nacional, S.A. de C.V., *¿Para qué sirven las licitaciones públicas?* Disponible en: https://www.eluniversal.com.mx/articulo/carlos-f-matute-gonzalez/nacion/para-que-sirven-las-licitaciones-publicas. (Fecha de consulta:22 de noviembre de 2019)

en el Estado mexicano, se identifican seis etapas comunes en el procedimiento administrativo de licitación: suficiencia presupuestal, preparación de la convocatoria, publicación de la convocatoria, presentación de ofertas, apertura de ofertas y fallo.

2.10.2.Problemática en las contrataciones

A pesar del establecimiento de etapas para la contratación y de su funcionamiento mecanizado, suelen suceder contratiempos, particularmente cuando la contratación implica temas nuevos como es el caso del cómputo en la nube. Así, en las distintas etapas de los procesos de contratación se presenta algún tipo de problemática que altera los objetivos en los distintos tipos de contrataciones públicas cambiando el panorama por actos de fraude y corrupción, por ejemplo:

- Solicitud de bienes y servicios innecesarios o excesivos.
- Requerimientos y especificaciones direccionadas a un proveedor o vendedor específico.
- División de proyectos grandes competitivos en diversos proyectos pequeños no competitivos.
- Contratación directa con pocos días para que otros proveedores o contratistas no tengan tiempo de participar.
- Manipulación de la licitación (direccionada a empresas favoritas).
- Fuga de información.
- Colusión entre contratistas para dejar fuera a la competencia.
- Colusión entre empleados y proveedores para obtener beneficios.
- La existencia de funcionarios cuya honestidad es dudosa.
- Servidores públicos con poco o nulo conocimiento de la normativa aplicable a la materia.

No obstante, las malas prácticas en las contrataciones públicas, además de la corrupción, generan consecuencias que, en otros ámbitos,[52] como el sistema de

[52] Delia Ferreira Rubio, Transparencia Internacional, *Percepción de transparencia 2018*, Disponible en: https://www.transparency.org/cpi2018. (Fecha de consulta:22 de noviembre de 2019)

compras, merma la economía, eficiencia y eficacia del quehacer público; por lo que ha sido necesario fortalecer dichos sistemas con el objetivo de generar un mejor valor en el proceso y por consiguiente, mayor eficacia, eficiencia y transparencia en materia de contrataciones públicas.

Al respecto, la Organización de los Estados Americanos considera que, al implementar buenas prácticas en el proceso de contratación, se generan múltiples beneficios tales como, la reducción de costos en los convenios, el avance del comercio electrónico, el aumento en el empleo, disminución de la corrupción y fortalecimiento de la gobernabilidad democrática para hacer funcionar plenamente el, todavía, novedoso Sistema Nacional Anticorrupción.

2.10.3.Recomendaciones

Dada la problemática en el sistema de contrataciones públicas, la Secretaría de Hacienda y Crédito Público (SHCP), a través de sus unidades administrativas y normativa en materia de contrataciones, ha propuesto implementar una política de contrataciones públicas orientada a asegurar las mejores condiciones para el Estado, así como en el desarrollo de un sistema de contratación pública dinámico, simplificado y moderno. Es decir, el objetivo de la Administración Pública Federal es el de contribuir en la aplicación de mejoras en materia de contrataciones públicas de manera íntegra, participativa, transparente y con apego a la legalidad[53] a través de la c*orrecta planeación de las contrataciones públicas*. La falta de planeación en materia de contrataciones públicas es la causa tanto de subejercicios en el gasto como de dispendios de dinero y retrasos en la prestación de servicios públicos. Del mismo modo, frecuentemente aparece como una de las causas de proyectos fallidos, principalmente en materia de obras públicas. De modo que, para generar una correcta planeación de las contrataciones públicas, es pertinente poner en marcha las siguientes acciones:

[53]Secretaría de la Función Pública, *Contrataciones públicas que garanticen las mejores condiciones para el Estado*. Disponible en: https://www.gob.mx/sfp/acciones-y-programas/contrataciones-publicas-que-garanticen-las-mejores-condiciones-para-el-estado. (fecha de consulta: 29 de noviembre de 2019)

- Identificar adecuadamente las necesidades en el área que se pretende satisfacer.
- Determinar el satisfactor idóneo de la necesidad detectada.
- Planear la estrategia de contratación.
- Promover la competencia en los procedimientos mediante su puesta en concurrencia.
- Asignación de servidores públicos capacitados y con visión de servicio en la toma de decisiones y liderazgo de proyectos.

Para formalizar un contrato seguro de cómputo en la nube con la Administración Pública, tal como lo menciona la Secretaría de la Función Pública, n la licitación pública no garantiza que el Estado obtenga las mejores condiciones de contratación existentes en el mercado, sino que, es necesario crear las condiciones que favorezcan la mayor participación de interesados en la licitación[54], implementar medidas de seguridad de la información y garantizar el tratamiento seguro de datos personales, involucrando a todos los sectores; además, claro de la capacitación constante y de alto nivel a los servidores públicos involucrados en las contrataciones públicas, comenzando por aquellos que actúan como áreas requirentes y técnicas, ya que son los primeros actores en la definición de necesidades, establecimiento de condiciones y evaluación de proposiciones; sin lugar a dudas, las áreas contratantes que son quienes llevan a cabo los procedimientos de contratación, sin olvidar a los asesores al interior de las dependencias y entidades, quienes juegan un papel fundamental en la prevención y fortalecimiento de los procedimientos de contratación.

La educación debe ser una constante en todas las actividades de la vida humana, sin que las contrataciones puedan ser excluidas de ello. Por esta razón, el Consejo de la Organización para la Cooperación y el Desarrollo Económicos Sobre Contratación Pública en su numeral IX inciso i) sugiere a los Estados miembros, como buena práctica, asegurarse que los profesionales de la contratación pública

[54] Secretaría de la Función Pública, Fomento a la competencia en los procedimientos mediante puesta en concurrencia, Disponible en *https://www.gob.mx/sfp/acciones-y-programas/2-fomento-a-la-competencia-en-los-procedimientos-mediante-puesta-en-concurrencia* (fecha de consulta: 29 de noviembre de 2019)

cuenten con un alto nivel de integridad, capacitación teórica y aptitud, que adquieran a través de cursos presenciales y en línea que imparten las diferentes unidades administrativas de la SFP (ahora SHCP) cuyo contenido debe estar acorde con la política general de contrataciones públicas que se promueve, así como alinearse con la normativa en materia de combate a la corrupción y responsabilidades de los servidores públicos.

2.11.Conclusiones

Una vez que tenemos claro que un contrato administrativo es un acuerdo de voluntades que contiene derechos y obligaciones, que éstos son el instrumento jurídico que celebra el Estado con particulares para obtener bienes y servicios que resultan necesarios para cumplir con su obligación de brindar servicios a sus gobernados, los contratos administrativos solamente pueden ser formalizados por aquellos servidores públicos con facultades conferidas en ordenamiento legal, exprofeso para ello, es decir, si bien los contratos administrativos los celebra el Estado en ejercicio de sus facultades, no cualquier servidor público puede formalizarlos, resaltamos los principios del contrato administrativo: legalidad, en el que la Administración Pública Federal solamente puede hacer aquello que contempla la Ley; continuidad, que significa que sus efectos no pueden interrumpirse. Es decir, una vez celebrado el contrato, las obligaciones deben cumplimentarse y no puede interrumpirse por simple voluntad del particular; principio de mutabilidad, al igual que el anterior, solo interviene la voluntad del Estado para su modificación y; el principio de equilibrio financiero, es decir, se debe evitar un perjuicio financiero al Estado y, en caso de esto ser inevitable, procurar que se reduzca al mínimo indispensable, considerando, en todo momento, el interés público y beneficio social.

Identificamos que para la celebración de un contrato administrativo, el Estado requiere previo a su formalización, llevar a cabo un procedimiento de contratación, ya sea licitación pública, nacional o internacional, en la que libremente puede participar cualquier persona física o moral que no esté inhabilitado por resolución de la Secretaría de la Función Pública y que su actividad esté directamente

relacionada con el bien o servicio objeto de la contratación; invitación a cuando menos tres personas, en el que el Estado invita a determinadas personas físicas o morales cuya actividad comercial esté directamente relacionada con el objeto de contratación y que cuenten con capacidad de respuesta inmediata, garantizando al Estado las mejores condiciones en cuanto oportunidad, eficiencia y eficacia y; por último, la adjudicación directa, procedimiento mediante el cual, el Estado adjudica a aquella persona física o moral que oferte el mejor precio, precisamos que para que opere la adjudicación directa, el importe adjudicado, no debe rebasar el monto máximo de actuación que conforme al Presupuesto de Egresos de la Federación para el ejercicio fiscal que corresponda autorice el Comité de Adquisiciones, Arrendamientos y Servicios, Arrendamientos y Servicios de la Dependencia o Entidad correspondiente

Tal como se mencionó en uno de los objetivos del presente capítulo, una vez identificados los diferentes tipos de contratos administrativos, los procedimientos de contratación que debe implementar el Estado, las principales cláusulas que debe contener un contrato de servicios de cómputo en la nube, las diversas consideraciones jurídicas a observar en los contratos de cómputo en la nube, así como la importancia que reviste el anexo técnico que utiliza el Estado como base fundamental para la contratación de servicios, la interacción que debe existir entre las áreas técnicas y contratantes en este tipo de servicios, destaca el control de la información, el aprovechamiento de las herramientas tecnológicas, garantizando la continuidad de la operación al interior de la dependencia o entidad, cuidando la interoperabilidad, portabilidad, seguridad, confiabilidad e integridad de la información.

Esto último se logra considerando, en la contratación de los servicios de cómputo en la nube, el cifrado de la información para evitar robo, perdida o violación a la misma, implementando políticas de seguridad y monitoreo constante con información medible y cuantificable de ataques y disponibilidad, así como desempeño y disponibilidad, niveles de servicio y mantenimiento y, actualización de infraestructura, entendiéndose ésta el software, licenciamiento y parches necesarios para el adecuado funcionamiento del servicio.

Con relación al objetivo de conocer la normativa relacionada con la protección de datos personales aplicable en México para robustecer y brindar seguridad jurídica a la Administración Pública Federal en la contratación de cómputo en la nube, pudimos observar que si bien, los primeros intentos mundiales por proteger los datos personales datan de la década de los 60, en México fue cuatro décadas después cuando se legisló al respecto, legislación que preveía las obligaciones para los sujetos obligados (gobierno) y; fue en 2010, cuando emite la normativa aplicable a particulares. Aun con esa distancia, México fue pionero en América Latina en cuanto a la protección de datos personales en posesión de sujetos obligados. Dicha protección requirió no solo de la emisión de normatividad específica para ambos sectores -público y privado- sino modificaciones constitucionales, por un lado, para reconocer como derecho fundamental la vida privada de los ciudadanos y; por otro, facultar al congreso para legislar al respecto.

Por lo que respecta al objetivo de resaltar los aspectos básicos a considerar en la contratación de servicios de cómputo en la nube, el hecho de que México haya sido pionero en el tema, en américa latina y que sea Parte del acuerdo de la Unión Europea, lo ha obligado a poner especial atención a la protección de datos, a adoptar mecanismos que permitan responsabilidad compartida de todos los involucrados en los servicios de cómputo en la nube. Uno de estos mecanismos, por sencillo que parezca es el implementar el aviso de privacidad, el cual, contempla medidas de seguridad, técnicas, físicas y administrativas, adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que recaba.

Por lo que respecta al objetivo de señalar las responsabilidades y obligaciones al contratar servicios de cómputo en la nube, consideramos importante el limitar la finalidad del tratamiento buscando facilitar la aplicación de la política de privacidad para datos personales, dependiendo de si los datos solamente son datos personales o se trata de datos personales sensibles. De igual forma, resulta importante la delimitación de responsabilidades de los involucrados, llámese responsable o encargado, identificando la información a almacenar, los propósitos

del almacenamiento, así como las medidas de seguridad que implementará para su protección.

Por último, en cuanto a las áreas de oportunidad al contratar servicios de cómputo en la nube, consideramos importante el analizar las opciones de interoperabilidad y adecuación de procesos, en busca del beneficio tanto al interior como al exterior de las dependencias y entidades, contratando centros de datos certificados, exigiendo el cumplimiento de normas tanto nacionales como internacionales y sistemas de gestión de calidad, confidencialidad y medidas de seguridad, pasando por supuesto, por los aplicativos, infraestructura tanto física como virtual, hardware y licenciamiento; sin olvidar, la propiedad intelectual y los niveles de servicio, observando en todo momento que cuando un ente público, llámese dependencia o entidad, debe observar los principios de *Licitud*: que estos se recaben en apego a la norma específica; *Lealtad*: que garantice a su titular la protección de los mismos; *Consentimiento*: obtener autorización del titular para el tratamiento de sus datos; *Información*: que el titular siempre sepa qué tratamiento se dará a sus datos; *Calidad*: que los datos siempre se mantengan actualizados, correctos y completos; *Finalidad*: el fin para el cual se recaban los datos y; *Responsabilidad*: garantizando que el tratamiento cumpla con la norma; así como los deberes de confidencialidad y seguridad.

Capítulo 3

Los procedimientos de contratación en particular en INFOTEC

Capítulo 3. Los procedimientos de contratación en particular en INFOTEC

3.1. Resumen

Al ser, INFOTEC, uno de los pocos centros especializados del Gobierno Federal en Tecnologías de la Información y Comunicación y, principal proveedor de este servicio al interior de la Administración Pública, en el presente capítulo se pretende abordar los procedimientos de contratación que con mayor frecuencia se instrumentan en INFOTEC para la contratación de bienes y/o servicios relacionados con las Tecnologías de la Información y Comunicación, ya que INFOTEC es un centro público de investigación especializado en el área y que, además de contratar este tipo de bienes o servicios para sí, para el cumplimiento de su objeto social, también actúa como proveedor de estos bienes y servicios con diversas dependencias y entidades y, la mayoría de los servicios que proporciona como proveedor tales como centro de datos, resguardo de información, correo electrónico, respaldo y recuperación de información, por mencionar algunos, involucran el tratamiento de datos personales, situación que, se torna importante ya que, INFOTEC no solamente es un sujeto obligado, sino un proveedor que debe aplicar, en todo momento la normatividad que aplica tanto al Gobierno como a los particulares.

3.2. objetivo

En el capítulo primero, identificamos los procedimientos de contratación que realiza la administración pública federal; en el presente capítulo, señalaremos los requisitos específicos para la contratación del servicio de cómputo en la nube en INFOTEC a través del procedimiento de adjudicación directa y cómo contribuye al ejercicio oportuno de los recursos en apego a los criterios de eficiencia, eficacia, transparencia y economía consagrados en la Constitución Política de los Estados Unidos Mexicanos.

3.3. La licitación pública en INFOTEC

De conformidad con lo establecido por el tercer párrafo del artículo 134 de la Constitución Política de los Estados Unidos Mexicanos, para llevar a cabo la contratación de bienes, arrendamientos o servicios necesarios para que INFOTEC cumpla con su misión y objeto social, así como con su programa de trabajo y compromisos derivados de la celebración de convenios, contratos y/o acuerdos con sus clientes, se privilegia la realización de dichas contrataciones a través del procedimiento de licitación pública, basado principalmente en los montos de actuación autorizados en cada ejercicio, de conformidad con el Presupuesto de Egresos de la Federación del ejercicio fiscal que corresponda y aprobados por el Comité de Adquisiciones, Arrendamientos y Servicios, Arrendamientos y Servicios. Cuidando, en todo momento la normatividad aplicable en cuanto a excepciones a la licitación y los requisitos para llevar a cabo el procedimiento de contratación correspondiente.

Uno de los desafíos a superar por parte de INFOTEC es el cumplimiento irrestricto de la normativa aplicable en materia de contrataciones públicas, por su naturaleza jurídica; esto es, a nivel federal la normativa en materia de contracciones públicas se traduce en al menos 50 ordenamientos jurídicos, sin considerar las políticas al interior de las dependencias y entidades; por lo que el exceso de regulación pudiera ser un contratiempo en los procedimientos que sigue el Gobierno federal para allegarse de bienes y servicios para satisfacer las necesidades de la sociedad.

Si bien INFOTEC es considerada una entidad paraestatal, con naturaleza jurídica y patrimonio propios, su naturaleza es la de un fideicomiso público; se le da tratamiento de entidad, es coordinada por el Consejo Nacional de Ciencia y Tecnología y funciona con recursos autogenerados, es decir, sólo está agrupada en un sector para efectos de control y rendición de cuentas; no obstante, no tiene asignado un presupuesto del erario público. A pesar de lo anterior, debe observar

la normatividad federal aplicable en materia de contrataciones; razón por la cual, las contrataciones que realice deben ser preferentemente mediante licitación pública.

Es importante resaltar que INFOTEC, además de actuar como convocante en un proceso de contratación, en ocasiones también lo hace como licitante y proveedor; ya que, al tratarse de un centro público de investigación especializado en tecnologías de la información y comunicación, es uno de los pocos organismos de la Administración Pública Federal especializados en la materia; por tanto, provee de diversos servicios a otros entes públicos de los tres órdenes de Gobierno. Servicios que pueden incluir o no el tratamiento de datos personales.

Así que, además de establecer requisitos y condiciones a cumplir por parte de los licitantes en un procedimiento de contratación para brindar servicios a la sociedad en cumplimiento de su objeto social, también debe cumplir con los requisitos y condiciones que otros entes públicos establecen a quienes pretendan contratar con ellos.

Debido a lo anterior, resulta indispensable fortalecer a la Administración Pública Federal en el tema de protección de datos personales al contratar servicios de cómputo en la nube. Servicio que INFOTEC ofrece, en calidad de proveedor, tanto a dependencias y entidades de la Administración Pública Federal, como a particulares.

INFOTEC cuenta con un centro de datos con certificación en Tier III (diseño) otorgada por el UpTime Intitute, entidad certificadora a nivel mundial; cuenta además con certificación ISO/IEC 20000-1:2011, SO/IEC20000-1:2011, NMX20000-1_2012, CMMI Nivel 5 y ofrece servicios de infraestructura, coubicación y bóveda de medios, centro de datos, seguridad de la información, administración de servidores, procesamiento y almacenamiento, virtualización, telecomunicaciones, bases de datos y servidores de aplicaciones, monitoreo de infraestructura, central de mesas de servicio, correo electrónico, análisis de riesgos, análisis de vulnerabilidades, respaldo y resguardo de información, respaldo y recuperación de información, gestión de almacenamiento, gestión de procesamiento e implementación de servidores de bases de datos y servidores de aplicaciones, con lo que se afinan parámetros y configuración avanzada para los

mismos servicios que, como puede observarse, involucran, en su gran mayoría, el tratamiento de datos personales; razón adicional para fortalecer y blindar las contrataciones que realiza la Administración Pública.

3.3.1. Documentación necesaria

El siguiente cuadro señala los requisitos básicos que, documentalmente debe soportar los procedimientos de contratación:

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
Oficio de solicitud, área requirente	4.2.1.1.6 Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓
Requisición (FO-CON-03)	4.2.1.1.9 Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
Suficiencia presupuestal	Artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público **4.2.1.1.8** Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓
Anexo Técnico	**4.2.1.1.8** Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓
Resultado de la Investigación de	4.2.1.1.10	✓	✓	✓

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
Mercado (FO-CON-05) Debe incluir peticiones de oferta (FO-CON-04), cotizaciones, resultado de consulta en CompraNet	Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público			
Programa Anual de Adquisiciones, Arrendamientos y Servicios	**4.2.1.1.8** Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓
Normas aplicables al bien o servicio a contratar	Artículo 51 de la Ley Federal sobre Metrología y Normalización **4.2.1.1.8** Manual Administrativo de	✓	✓	✓

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
	Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público			
Constancia de no existencias en almacén (FO-CON-02)	Numeral 4.2.1.1.5 Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓		
Oficio de solicitud y autorización del criterio de evaluación BINARIO	Artículo 36 segundo párrafo, LAAASSP 51 del RLAASSP Numeral 4.2.1.1.18 MAAGAAS	✓	✓	✓
Tabla de puntos para evaluación (es de precisar que tratándose de bienes o servicios	Artículo 36 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público	✓	✓	✓

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
relacionados con TIC la evaluación de las proposiciones debe realizarse a través de este método)	Acuerdo por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las mismas, publicado en el *Diario Oficial de la Federación* el 9 de septiembre de 2010			
Oficio de solicitud y autorización de Reducción de plazos, en su caso.	Artículo 32 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 42 de su Reglamento	✓	✓	✓
Autorización para el ejercicio de recurso de partida restringida	Acuerdo relativo al establecimiento de los lineamientos generales para las campañas de comunicación social		✓	✓

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
	de las dependencias y entidades de la Administración Pública Federal			
Autorización del titular de la Entidad para ejercer recursos en más de un ejercicio fiscal (plurianualidad)	Artículo 25 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 50 de la Ley Federal de Presupuesto y Responsabilidad Hacendaria y, 148 de su Reglamento.			
Constancia de no existencia de servicios similares Dictamen de no contar con personal capacitado o disponible para su realización	Art. 19 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 15 y 72, fracc. VIII de su Reglamento			✓
Estudio de factibilidad	Lineamiento 32 a 34 de los			

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
(debe contarse con el visto bueno de la UTIC, OIC, UGD y, tratándose de bienes TIC, de la UPCP)	LINEAMIENTOS para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal55			
Cartas de Ausencia de no conflicto de interés	Acuerdo por el que se expide el protocolo de actuación en materia de contrataciones	✓	✓	✓

55 Secretaría de Hacienda y Crédito Público, Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, Diario Oficial de la Federación, México, 30 de enero de 2013.

Documento	Fundamento legal	Bienes	Servicios	Consultorías, asesorías, estudios e investigaciones
	públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones			

Cuadro 8. Requisitos para la contratación de servicios

Fuente: elaboración propia con información de POBALINES.

3.4. La adjudicación directa en el INFOTEC en el supuesto normativo del artículo 41, fracción III, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público

Como se planteó en el apartado 6 del capítulo primero, la adjudicación directa es un supuesto de excepción a la licitación pública que, de conformidad con lo establecido por los artículos 41 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 71 y 72 fracción III de su Reglamento, deben configurarse una serie de requisitos para poder contratar bajo dicho supuesto, a saber:

"Existan circunstancias que puedan provocar pérdidas o costos adicionales importantes, cuantificados y justificados". Para acreditar este supuesto la Administración Pública Federal debe acreditar, con la investigación de mercado, que se obtienen las mejores condiciones para el Estado y, por tanto, se evitan pérdidas o costos adicionales, al contratar con algún proveedor que tenga contrato vigente previamente adjudicado mediante licitación pública y éste acepte otorgar los mismos bienes o servicios en iguales condiciones en cuanto a precio, características y calidad de los bienes o servicios materia del contrato celebrado con la misma u otra dependencia o entidad.

Es decir, además de la documentación necesaria señalada en el apartado anterior, las áreas requirentes deben incluir una justificación de las razones por las cuales considera que, a diferencia de la licitación pública, con una adjudicación directa se obtienen los bienes y/o servicios (en el caso que nos ocupa, servicios) indispensables para cumplir con el fin propuesto, generando un ahorro o evitando costos adicionales, cuantificando éstos ya sea porque se trata de cuestiones económicas, sociales, humanas, administrativas o políticas; pero siempre demostrando dicha circunstancia. Resulta transcendental resaltar que la justificación debe acreditar los siguientes supuestos como resultado de la investigación de mercado:

- Que se eviten pérdidas o costos adicionales.
- Que la contratación se realice con un proveedor que tenga contrato vigente, previamente adjudicado mediante licitación pública.
- Que el proveedor en cuestión acepte proporcionar los servicios en iguales condiciones en cuanto a precio, características y calidad.
- El contrato puede estar celebrado, incluso, con la misma dependencia o entidad.

En este orden de ideas, si bien puede señalarse un ahorro monetario, podría darse el caso de que el no contar con el servicio con la oportunidad y prontitud solicitada por el área requirente, se pusiera en riesgo un servicio que el Gobierno, por ministerio de Ley, brinde a la sociedad.

La justificación mencionada, además de la documentación necesaria arriba listada, debe presentarse a los integrantes del Comité de Adquisiciones, Arrendamientos y Servicios, de la entidad, para que éste, con base en la documentación que se le presente, emita su opinión sobre la procedencia o no de la contratación.

Como en cualquier procedimiento de contratación, podría decirse que el documento “base de la acción” es el resultado de la investigación de mercado; por lo que cabe resaltar la importancia que reviste en la Administración Pública, pero particularmente para INFOTEC; en primer lugar, identificar y determinar las características técnicas, alcances, niveles de servicio, plazo, lugar y condiciones

para la entrega de los bienes o prestación de servicios, requisitos que deben cumplir los licitantes, pruebas de funcionamiento, periodicidad de informes, forma y términos para calcular y aplicar penalizaciones y/o deductivas, niveles de servicio, seguridad de la información y, en general, prever en el anexo técnico todos y cada uno de los requisitos que deben cumplir los licitantes, particularmente cuando los servicios involucran datos personales, así como certificaciones que se solicitarán para garantizar la seguridad de la información, ya sea que INFOTEC actúe como responsable o no.

Lo anterior se traduce en una razón más del por qué es importante el anexo técnico y las condiciones a las que se sujetará la contratación, ya que, si bien existen "necesidades" comunes en la Administración Pública, también es cierto que el volumen, uso y destino que se da a la información debe tener un tratamiento "hecho a la medida", sobre todo, tratándose de servicios que involucren datos personales.

3.4.1. Documentación necesaria

De conformidad con lo establecido por el Manual administrativo de aplicación general en materia de adquisiciones, arrendamientos y servicios del sector público, la documentación que debe presentar el área requirente al área contratante para solicitar la contratación de un bien o servicio al amparo del artículo 41 fracción III de la Ley, es la siguiente:

- Oficio de solicitud del área requirente
- Justificación/dictamen del área requirente
- Requisición (FO-CON-03)
- Suficiencia presupuestal
- Anexo técnico
- Resultado de la investigación de mercado (FO-CON-05)
- Debe incluir peticiones de oferta (FO-CON-04), cotizaciones, resultado de consulta en CompraNet
- Programa Anual de Adquisiciones, Arrendamientos y Servicios
- Normas aplicables al bien o servicio a contratar

- Asignación de puntos o porcentajes para calificar la capacidad de los licitantes
- Autorización para el ejercicio de recursos de partida restringida
- Autorización para ejercer Autorización para ejercer recursos de más de un ejercicio fiscal, en su caso
- Constancia de no existencia de servicios similares (tratándose de asesorías, consultorías o investigaciones)
- Dictamen de no contar con personal capacitado o disponible para su realización (tratándose de asesorías, consultorías o investigaciones)
- Dictamen de factibilidad, visto bueno de la UTIC, OIC y UGDy; en caso de bienes relacionados con TIC, dictamen de la UPCP
- Resultado de la consulta en CompraNet de no inhabilitación o sanción del proveedor propuesto
- Cartas de ausencia de no conflicto de interés

3.4.2. Requisitos que establece el Manual administrativo de aplicación general para la contratación de servicios relacionadas con TIC

- Planeación: Deberán sujetarse a las estrategias y líneas de acción de la estrategia digital nacional (EDN).
- Investigación de mercado: Verificar si existe algún ente público que, conforme a su objeto y niveles de servicio, esté en posibilidad de suministrar los bienes o prestar los servicios que se requieran.
- Estudio de factibilidad: Registro en herramienta HGPTIC, visto bueno del OIC, Dictamen UGD y, en su caso, Dictamen de la UPCP (tratándose de bienes).
- En caso de contratación de hospedaje de infraestructura y aplicaciones en un centro de datos: Solicitar la autorización de la UGD, anexando el estudio costo-beneficio, incluyendo los niveles de disponibilidad del

servicio a contratar, así como los requerimientos de seguridad de la información asociados56.

- Tratándose de prestación de servicios: Incluir precios unitarios del servicio, así como el desglose de los componentes que integren el servicio.
- Tratándose contrataciones relacionadas con los servicios de desarrollo, implementación, soporte a la operación y mantenimiento de aplicativos de cómputo: Acreditaciones de Normas Oficiales Mexicanas, Normas Mexicanas y Normas Internacionales en términos de la Ley Federal sobre Metrología y Normalización, así como la certificación de otros estándares o modelos reconocidos por la industria como las mejores prácticas, diseño detallado del aplicativo a desarrollar (requerimientos del negocio, de seguridad de la información, de privacidad y protección de datos personales, técnicos, casos de uso, módulos, matriz de trazabilidad y protocolos de pruebas; así como el uso de la Identidad digital).

Especificar el conjunto de aplicativos de cómputo, debiendo incluir como entregables las bitácoras de actividades del personal que se asigne a tales aplicativos, ya sea desarrollos, implementaciones, soportes a la operación o mantenimientos; señalar, además, que los aplicativos quedarán bajo la titularidad de la institución contratante; prever el uso de canales seguros para la integridad de los datos; mantener una arquitectura que permita la portabilidad, de forma tal que las aplicaciones de cómputo puedan migrar entre distintos centros de datos y sean interoperables.

De igual forma, establecer los requisitos que debe cubrir el personal asignado a los proyectos, académicos y de experiencia, sobre todo si éstos están relacionados con el tratamiento de datos personales; determinar los niveles de

[56] Secretaría de Gobernación, Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, México, Diario Oficial de la Federación, 4 de febrero de 2016

acceso, seguridad, bitácoras, medidas de seguridad, tanto físicas como administrativas y de infraestructura.

3.5. conclusiones

Como consecuencia del abanico de servicios que ofrece INFOTEC, los cuales en su mayoría, tiene, el respaldo de realizarse bajo certificaciones tanto nacionales como internacionales, tiene contacto con datos personales, lo que no necesariamente se traduce en su tratamiento; es decir, si el servicio que proporciona es de gestión de almacenamiento, solo interviene en el resguardo de la información sin conocer a detalle qué información está resguardando; lo mismo sucede con la administración de servidores y monitoreo de infraestructura y; en los casos en que por alguna razón, por ejemplo, fábricas de software, borrado seguro, seguridad perimetral, SOC y pruebas de intrusión, tiene acceso a datos personales, resulta necesario establecer niveles de acceso, que el personal que interviene firme cartas de confidencialidad, y se establezcan niveles de acceso, que permiten, por una parte, proponer al cliente medidas de seguridad de su información y/o fortalecer los mecanismo y medidas existentes.

Como pudimos apreciar, los requisitos para solicitar la contratación de servicios en INFOTEC se realiza con apego al Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público y el de Estrategia Digital y Seguridad de la información, tanto para licitación pública como para adjudicación directa son prácticamente los mismos; las diferencias entre un procedimiento y otro, se resumen en que mientras el procedimiento de licitación se realiza, en promedio, en 25 días naturales, el de adjudicación directa podría realizarse en una semana; mientras la convocatoria de licitación (bases del concurso) es autorizada por un Subcomité y la participación es abierta a cualquier interesado; la adjudicación directa debe estar acompañada de una justificación mediante la cual el titular del área requirente acredita los criterios por los cuales considera que es factible realizar el procedimiento de adjudicación directa y, en ésta propone al proveedor que proporcionará el servicio, cuya dictaminación

corresponde al Comité de Adquisiciones, Arrendamientos y Servicios y; diferencia sustancial es la forma de evaluar las proposiciones de los licitantes; ya que por tratarse de servicios relacionados con tecnologías de la información, la ley obliga a evaluar a través del mecanismo de puntos o porcentajes -mecanismo aplicable solamente a procedimientos de licitación e invitación a cuando menos tres personas- mientras que, en la adjudicación directa, la selección del proveedor es consecuencia ya sea del cumplimiento de requisitos establecidos en el anexo técnico, incluido el cumplimiento de contratos, experiencia, especialidad, equipo de trabajo, cumplimento de normas y de contratos, contar con sistemas de gestión, y la acreditación de criterios de eficiencia, eficacia, economía, transparencia honradez o del ahorro sustancial de recursos ya sea humanos, materiales, económicos, de infraestructura, al contratar con un proveedor que haya resultado adjudicado mediante licitación pública por otra dependencia o entidad, en el entendido de que ésta contrató servicios similares y de la misma naturaleza, evaluando las proposiciones mediante el mecanismo de puntos o porcentajes.

Capítulo 4

Derecho y tecnologías de la información

Capítulo 4 Derecho y tecnologías de la información

4.1. Resumen

Por último, retomaremos los principales aspectos de protección de datos personales en la contratación de servicios de cómputo en la nube, las deficiencias que, en la práctica, hemos detectado cuando la Administración Pública Federal formaliza contratos de servicios relacionados con las tecnologías de la información.

4.2. Objetivos

1) Identificar las causas que al interior de la administración pública vulneran la seguridad de los datos personales, para proponer soluciones que garanticen a los gobernados el cumplimiento de la norma por parte de los sujetos obligados.
2) Demostrar la importancia de la capacitación de los servidores públicos en materia de protección de datos personales.

4.3. Violación de datos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Hoy por hoy, el Gobierno mexicano está más comprometido en con el tema de la protección de datos personales, principalmente a partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ahora, Ley General de Transparencia y Acceso a la Información Pública. Las dependencias, organismos y entidades gubernamentales se han adherido al cumplimiento de la protección de datos personales para y bajo la vigilancia del INAI.

Así, por mencionar un caso en particular, dependencias como la Secretaría de la Función Pública refrendan su compromiso con la protección de datos personales y con el cumplimiento de la LGPDPPSO. En ese sentido, la SFP

promueve entre los servidores públicos de la Administración Pública Federal la obligación de cumplir con dicha Ley.[57]

De este modo, la Administración Pública Federal se obliga a proporcionar aspectos clave de la protección de datos como es el caso del aviso de privacidad, así como el fundamento para el tratamiento de los mismos; se difunden los mecanismos, medios y procedimientos para ejercer derechos ARCO en el tratamiento de datos personales. No obstante, dado que los datos personales por su naturaleza son vulnerables y las consecuencias de las vulneraciones afectan a los involucrados directos (titular, responsable y encargado), se concluye que las principales causas de vulnerabilidad, además de la tecnología, son la falta de cultura o de conocimiento en el tema al interior de las dependencias y entidades, aunado a las deficiencias de la regulación normativa.

Para demostrarlo, en las siguientes líneas se establecen los elementos que intervienen en el crecimiento de la brecha entre el conocimiento de protección de datos personales, en el caso específico del cómputo en la nube, ya que comúnmente la protección de datos personales se ve como una obligación normativa con poco compromiso del sector público, lejos de verse como un derecho humano consagrado en la Constitución.

4.3.1. Deficiencias en la protección de datos en el cómputo en la nube

- Falta de responsabilidad por parte de quienes son encomendados para ejecutar un contrato de cómputo en la nube, en el sentido de no estar actualizados en materia tecnológica y jurídica.
- Falta de iniciativa por parte del servidor público para estudiar los aspectos básicos de la protección de datos personales en el cómputo en la nube.
- Poca sinergia entre encargado, responsable y administrador respecto del manejo y establecimiento de cláusulas contractuales y elaboración de los anexos técnicos.

[57] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Diario Oficial de la Federación, México, 26 de enero de 2017, Disponible en: *https://www.gob.mx/sfp/articulos/sfp-comprometida-con-la-proteccion-de-datos-personales-144568*. Fecha de consulta (29 de noviembre de 2019

- Especulación respecto de la emisión de cláusulas que garantizan el correcto resguardo de los datos personales que se recaban.
- Desconocimiento o evasión del riesgo existente y las posibles consecuencias para los interesados; responsable, titular y encargado.
- Vulnerabilidad de los datos ante el atraso tecnológico.
- Poca seguridad en los datos y aumento en la violación de los mismos a causa de los ataques cibernéticos y del ciberdelito.
- Incertidumbre respecto de las medidas de seguridad para el tratamiento de datos, afectando de manera significativa los derechos de los interesados en la contratación de cómputo en la nube.
- Insolvencia por parte del responsable o encargado para identificar delitos mayores relacionados con el uso incorrecto de datos personales en las etapas de recopilación, almacenamiento, uso y tratamiento.
- Violación de datos debido a la vulnerabilidad tecnológica al interior de las dependencias por amenazas de robo de datos.

La guía que emite el INAI para contratar cómputo en la nube se basa en lo establecido en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

4.4. Conclusiones

Con la entrada en vigor, en enero de 2017, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el marco jurídico existente incluyó deberes y obligaciones para el tratamiento de datos personales, considerando el desarrollo tecnológico para recabar, procesar, tratar o transmitir grandes volúmenes de información y es aquí donde el responsable juega un papel importante ya que se requiere que éste tenga pleno conocimiento de las políticas de protección de datos personales aunado a la importancia que representa la confidencialidad en la protección de datos.

Si bien mediante los avisos de privacidad, INFOTEC informa a los titulares de la información qué datos recaba, el uso y fin que se les dará y, con ello recaba el consentimiento de los titulares, resulta fundamental que no sólo se guarde la

confidencialidad, sino que se recomienda que, mediante un acuerdo de confidencialidad, integrado como anexo dentro del contrato, se implementen las medidas técnicas y organizativas necesarias para garantizar la confidencialidad.

Como vimos a lo largo, del presente trabajo, en la contratación de servicios de cómputo en la nube, intervienen diversos actores y diversas áreas al interior de la Institución: área requirente, técnica, contratante, comité o subcomité y usuarios finales; razón por la cual, se recomienda capacitar a todos los involucrados en la comprensión de la normativa en materia de protección de datos personales tanto en posesión de sujetos obligados como particulares, recordemos que INOFTEC juega ambos papeles, reforzar la contratación del servicio con el establecimiento de cláusulas que obliguen a los proveedores a incluir medidas de seguridad estrictas ya sea de infraestructura o accesos en la recopilación almacenamiento y uso de la información.

En apego al Manual Administrativo de Aplicación General en Materia de Tecnologías de la información y Seguridad de la Información, designar administradores de contrato que no solamente vigilen los aspectos técnicos, sino que también, conozcan la normatividad aplicable en la materia para garantizar que los servicios que proporciona INFOTEC ya sea servicios de infraestructura, coubicación y bóveda de medios, centro de datos, seguridad de la información, administración de servidores, procesamiento y almacenamiento, virtualización, telecomunicaciones, bases de datos y servidores de aplicaciones, monitoreo de infraestructura, central de mesas de servicio, correo electrónico, análisis de riesgos, análisis de vulnerabilidades, respaldo y resguardo de información, respaldo y recuperación de información, gestión de almacenamiento, gestión de procesamiento e implementación de servidores de bases de datos y servidores de aplicaciones, garanticen a sus clientes, en todo momento, el cumplimiento de la normatividad aplicable y sobre todo, la seguridad de la información.

Conclusiones

Conclusiones

Como pudimos apreciar a lo largo de cuatro capítulos, los actores que intervienen en un contrato administrativo de prestación de servicios de cómputo en la nube, son diversos y de diversas áreas, técnica, jurídica, administrativa, personal de apoyo, usuarios, proveedores, administradores, incluso, fiscalizadores; por lo que, dado que la protección de los datos personales es un derecho contemplado en nuestra carta magna, máximo instrumento jurídico, es que se debe prestar especial atención a su tratamiento, implementando medidas de seguridad ya sea físicas, administrativas o de infraestructura, capacitar a los actores que intervienen en los procesos, concientizando e incentivando la protección de los datos. Lo que podría convertirse en una ardua labor, ya que los procesos desde la elaboración de las necesidades, plasmarlo en el anexo técnico, pasando por el proceso de contratación, elaboración de contrato y administración es éste, exigen el conocimiento de normatividad de diversas disciplinas, expertos en derecho, en tecnologías de la información e involucran distintas disciplinas.

Labor que no es imposible si se comienza con una lista de verificación o *check list* de los puntos básicos, medulares y necesarios para contar con un contrato de servicios de cómputo en la nube seguro, práctico y funcional y continuar con capacitación constante al interior de la administración púbica e implementando controles de vigilancia, que si bien, en materia de tecnologías de la información y seguridad de la información, existe un manual administrativo de aplicación general con procesos, tareas y responsables perfectamente definidos; resulta necesario, involucrar a todos los actores en todas la tareas, lo que tendría como resultad confianza en las instituciones y la certeza de que los datos personales que se proporcionen al realizar un trámite o solicitar un servicio al gobierno, este cuenta con los filtros, personal y recursos técnicos idóneos para su protección.

Bibliografía

Agencia española de Protección de datos, ¿Qué es el derecho a la portabilidad?, 2018, *https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad*

Amazon Web Services, Seguridad en la nube, Infraestructura y servicios que elevan su seguridad en la nube, *https://aws.amazon.com/es/security/introduction-to-cloud-security*

Carlos Matute González, El Universal, Compañía periodística Nacional, S.A. de C.V., ¿Para qué sirven las licitaciones públicas? *https://www.eluniversal.com.mx/articulo/carlos-f-matute-gonzalez/nacion/para-que-sirven-las-licitaciones-publicas*

Criterios Técnicos para la Contratación, por parte de los sujetos obligados, de adquisiciones y arrendamiento de bienes muebles, prestación de servicios, de obras públicas y servicios relacionados con las mismas", Diario Oficial de la Federación, 27 de septiembre de 2017.

Delia Ferreira Rubio, Transparencia Internacional, Percepción de transparencia 2018, *https://www.transparency.org/cpi2018.*

European Union Agency For Cibersecurity, *Beneficios, riesgos y recomendaciones para la seguridad de la información*, 2019, *https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish*.

Expansión SA de CV, México, líder de cloud computing en AL, México, 2011. *https://expansion.mx/tecnologia/2011/08/24/mexico-lider-de-cloud-computing-en-al*

Emiliano Nieto, Facultad de Informática, Universidad de la Plata, Diseño de aplicaciones SaaS sobre plataformas de cloud computing, 2018, *http://sedici.unlp.edu.ar/bitstream/handle/10915/46834/Documento_completo.pdf?sequence=1*

Fernández Ruiz, Jorge, Derecho administrativo, 2016, México, UNAM, Instituto de Investigaciones Jurídicas.

Gómez de Lara, Fernando y Huacuja Betancourt, Sergio, 2016, *La contratación de bienes, arrendamientos y servicios en la administración pública federal*", México, Universidad Panamericana.

González Sandoval, Rodrigo, 2008, *La licitación pública y el contrato administrativo*, México, Porrúa.

Herrera Somellera, José Luis,1997, *Apunte sobre contratos administrativos*, México, UNAM, Instituto de Investigaciones Jurídicas.

Horacio E. Gutiérrez, Daniel Korn, Universidad Externado de Colombia, Facilitando "the cloud": la regulación de la protección de datos como motor de la competitividad nacional en América Latina. https://revistas.uexternado.edu.co/index.php/propin/article/view/3908/4344

Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales Guía para el aviso de privacidad, *http://inicio.ifai.org.mx/SitePages/Guia-para-el-Aviso-de-Privacidad.aspx*.

Instituto Mexicano para la Competitividad, Guía práctica de compras públicas, 2018, https://imco.org.mx/wp-content/uploads/2013/7/Guia_de_compras_publicas_011012.pdf

Leiza Zunino, Pablo "Contratos de la administración pública", Fondo de Cultura Universitaria, disponible en: https://derechopublicoadministrativo.blogspot.com/2012/03/teoria-de-las-clausulas-exorbitantes.html

Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Diario Oficial de la Federación México Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, 2017, México. 10 de noviembre de 2014.

Lineamientos Generales de Protección de Datos Personales para el Sector Público, Diario Oficial de la Federación, México, 26 de enero de 2018

Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. Diario Oficial de la Federación, México, 2018.

Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina

presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal, 2013, México.

López Elías, José Pedro, 1999, *Aspectos jurídicos de la licitación pública en México*, México, Instituto de Investigaciones Jurídicas UNAM.

Lucero Espinosa, Manuel, 2009, *La licitación pública*, 4a. ed., México, Porrúa.

Miguel Ángel Zamora y Valencia,1989, Contratos civiles, primera edición, México, Porrúa.

Miguel Recio Gayo, INAI, Principios y deberes en materia de Protección de Datos Personales, http://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Principios%20y%20deberes%20en%20materia%20de%20Proteccio%CC%81n%20de%20Datos%20Personales.pdf?sequence=1.

Municipio de Zapopan, Jalisco, Gobierno de Zapopan, 2015, contrato de servicios en la nube administrados y servicios de actualización de licencias de software y soporte. *https://www.zapopan.gob.mx/wp-content/uploads/2015/05/173.pdf*

Norma Mexicana NMX-I-27018-NYCE-2016, *Tecnologías de la información-técnicas de seguridad-código de práctica para la protección de datos personales (DP) para proveedores de servicios de nubes públicas*. Diario Oficial de la Federación, 2016, México.

Oracle Corporation, Protección de datos, 2019, https://www.oracle.com/es/database/security/

PalblaDigital S.L., Revista transformación digital, La computación en la nube en Europa y en España: una oportunidad de negocio, https://www.revistatransformaciondigital.com/2014/03/18/httpwww-revistagestiondocumental

Paloma Aviles,2013, ContadorMX, Ejemplos de aviso de privacidad y para la protección de datos personales en México. *https*://contadormx.com/2013/05/06/ejemplos-de-aviso-de-privacidad-y-para-la-proteccion-de-datos-personales-en-mexico

Plataforma digital única del Estado Peruano gob.pe, Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros,

https://www.gob.pe/institucion/pcm/informes-publicaciones/268665-lineamientos-para-el-uso-de-servicios-en-la-nube-para-entidades-de-la-administracion-publica-del-estado-peruano.

Privacy Driver, Responsabilidad del tratamiento en la mediación de seguros, Ley Orgánica 15/1999, de 13 de diciembre 1999, de Protección de Datos de Carácter Personal, *https://www.privacydriver.com/es/responsabilidad-del-tratamiento-mediacion-seguros-c356*

Reglamento de la Ley Federal de Protección de Datos en Posesión de Particulares, Diario Oficial de la Federación, 2011, México.

Rabindranath Guadarrama Martínez, Secretaría de Gobernación, Orden jurídico Nacional, Antecedentes de la Ley federal de Transparencia y acceso a la información pública gubernamental, http://www.ordenjuridico.gob.mx/Congreso/pdf/39.pdf.

Ricard Martínez "LOPD y Seguridad", Cloud en el nuevo reglamento mexicano de protección de datos, España, 2011. *http://lopdyseguridad.es/11*

Sala, Vicente, 1873, Diccionario latino-español, París, Librería de Garnier Hermanos.

Sarabia Miramontes, Grecia, 2003, *Gestión de obra pública en México: contratos de obra pública y Pidiregas*, México, Universidad de las Américas Puebla.

Secretaría de Economía, Prosoft industria 4.0 mx, Guía para empresas en materia de Protección de Datos Personales en el uso de Cómputo en la Nube, *https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_33.pdf*

Secretaría de Gobernación, Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias, México, Diario Oficial de la Federación, 4 de febrero de 2016.

Secretaría de Hacienda y Crédito Público, Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio

del gasto público, así como para la modernización de la Administración Pública Federal, Diario Oficial de la Federación, México, 30 de enero de 2013.

Secretaría de la Función Pública, Criterios Técnicos para la Contratación, por parte de los sujetos obligados, de adquisiciones y arrendamiento de bienes muebles, prestación de servicios, de obras públicas y servicios relacionados con las mismas, Diario Oficial de la Federación, 27 de septiembre de 2017, *http://dof.gob.mx/nota_detalle.php?codigo=5498762&fecha=27/09/2017*.

Secretaría de la Función Pública, *https://www.gob.mx.*

Serrano Rodríguez, Carlos Eduardo, 1991, *La contratación administrativa*, San José, Universidad de Costa Rica.

Superintendencia de industria y comercio, Protección de los datos personales en los servicios de computación en la nube (cloud computing), Bogotá, *https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf.*

Tesauro Jurídico de la Suprema Corte de Justicia de la Nación, 2014, *Derecho administrativo.* SCJN

Tesis aislada. Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XV, abril de 2002.

Tesis s/n aislada, *Semanario Judicial de la Federación*, Quinta Época, t CVIII, p. 17.

Tesis: P. IX/2001, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XIII, abril de 2001.