Guía para empresas en materia de Protección de Datos Personales en el uso de Cómputo en la Nube (Cloud computing)

ÍNDICE DE CONTENIDO

I. ANÁLISIS DEL USO DEL CÓMPUTO EN LA NUBE EN MÉXICO 11
1. Introducción 11
2. Metodología de la encuesta 12
3. Análisis de las preguntas 13
3.1. Uso actual de la nube en la empresa 13
3.2. Servicios de cómputo en la nube que se utilizan actualmente 15
3.3. ¿Por qué motivo o motivos no hace uso del cómputo en la nube? 17
3.4. ¿Qué servicios tecnológicos utiliza en el cómputo en la nube? 18
3.5. ¿Sabe o ha calculado qué porcentaje de sus empleados utiliza dispositivos móviles para acceder a la información? 19
3.6. ¿Trata datos personales en la nube? 21
3.7. Si trata datos personales en la nube, ¿ha considerado aspectos para evitar riesgos o ha adoptado medidas para mitigarlos? 23
3.8. ¿Qué importancia tienen los aspectos que se indican para la adopción del cómputo en la nube? 24
3.9. ¿Qué confianza le ofrecen los siguientes prestadores de servicios de cómputo en la nube? 25
3.10. Si tuviera forma de asegurar o monitorizar su información en la nube, ¿haría más uso de ésta? 27
4. Conclusiones 28
Anexo A – Formulario de Encuesta 32
Anexo B – Tablas de Datos de Respuesta 39

II. CUESTIONES GENERALES SOBRE EL CÓMPUTO EN LA NUBE 47
1. Introducción, concepto y clasificaciones en el cómputo en la nube 47
1.1. Introducción y concepto 47
1.2. Las categorías de Ofertas de Servicios de "Cloud Computing" 51

1.2.1. Infraestructura como servicio ("*Infrastructure-as-a-service*". *IaaS*) 52
1.2.2. Plataforma como servicio ("*Platform-as-a-service*". *PaaS*)..... 52
1.2.3. Software como servicio ("*Software-as-a-service*". *SaaS*)..... 53
1.2.4. "Business Process as a Service" ("BPaaS")..... 53
1.3. Clases de nubes: las nubes públicas, privadas, híbridas y comunitarias..... 54
1.3.1. Las nubes públicas..... 54
1.3.2. Las nubes privadas..... 55
1.3.3. Las nubes comunitarias..... 56
1.3.4. Las nubes híbridas 57
2.- El cómputo en la nube como servicio de comunicaciones electrónicas y de la sociedad de la información..... 57
3. El artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares..... 65
4. El cómputo en la nube como oportunidad para que México aumente su competitividad internacional..... 85
5. Las estrategias y enfoques a nivel internacional sobre el cómputo en la nube..... 93
5.1. Estados Unidos..... 93
5.2. Unión Europea 100
5.3. Asia..... 117
5.3.1. China..... 118
5.3.2. India..... 120
5.3.3. Japón..... 124
5.4. Latinoamérica..... 126
5.4.1. Colombia 134
5.4.2. Argentina..... 135
5.4.3. Chile 137
5.4.4. Brasil 138
6. Las partes interesadas en las relaciones jurídicas de la computación en la nube. Especial referencia al prestador y al usuario de los servicios..... 141
6.1. Prestador de servicios de cómputo en la nube..... 141
6.2. Usuario: sector privado y público..... 146
7. La generación de confianza mediante el cómputo en la nube en todos los sectores..... 149

III. EL CÓMPUTO EN LA NUBE EN MÉXICO 155
1. Introducción a la Regulación de *cloud computing* en México 155
1.1. Mecanismos del Gobierno para impulsar el desarrollo de TIC 158
1.1.1. Secretaría de la Función Pública y la Agenda de Gobierno Digital 158
1.1.2. Esquema de Interoperabilidad de Datos Abiertos de la Administración Pública Federal 159
1.1.3. Secretaría de Comunicaciones y Transportes y la Agenda Digital del Sistema Nacional e-México 2010-2015 161
1.1.4. Estrategia Digital Nacional 162
1.1.5. Secretaría de Economía y PROSOFT 3.0 167
1.1.6. MEXICOIT 170
1.1.7. MexicoFIRST 170
1.2. Organizaciones no gubernamentales 171
1.2.1. CANIETI 171
1.2.2. AMITI 171
1.2.3. AMIPCI 172
1.3. Prácticas internacionales 173
1.3.1. ASPAN 173
1.3.2. APEC 174
1.3.3. UNCTAD- ALADI 174
2. Tipología de nubes y servicios 174
3. Oportunidades de negocio que ofrece el cómputo en la nube en México 176
3.1. De manera directa 177
3.2. De manera derivada 178
4. Aspectos a considerar sobre el cómputo en la nube desde un punto de vista tecnológico 180
4.1. Estandarización 180
4.2. Interoperabilidad 181
4.3. Análisis de las tendencias tecnológicas que requieren especial atención en la seguridad de la información y de datos personales 182
4.3.1. Internet de las cosas 182
4.3.2. Big data 184

4.3.3. Sistemas Operativos Urbanos (*smart cities*) 188
5. Necesidad de identificar riesgos legales y regulatorios para evitar incumplimientos 190
6. Protección de datos personales 194
6.1. Normatividad de protección de datos personales 194
6.1.1. Sector Privado 194
6.1.2. Sector Público 196
6.1.3. Regulaciones existentes a nivel mundial que contemplan requisitos de protección de datos personales para el cómputo en la nube 198
6.2. Principios de la protección de datos personales 203
6.2.1. Licitud 205
6.2.2. Consentimiento 206
6.2.3. Información 212
6.2.4. Calidad 217
6.2.5. Finalidad 220
6.2.6. Lealtad 222
6.2.7. Proporcionalidad 223
6.2.8. Responsabilidad 224
6.3. Roles de usuario como responsable del tratamiento y del prestador de servicios como encargado del tratamiento 227
6.4. El establecimiento del responsable y la ley aplicable al contrato 231
6.5. Necesidad de un contrato que regule el acceso a los datos personales 232
6.6. Subcontratación 235
6.7. Ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO) 238
6.8. Potestades de la autoridad garante y las autoridades 248
6.9. Cooperación internacional 252
6.10. Acceso de autoridades gubernamentales y judiciales a los datos 253
6.11. Principios mínimos con los que debe cumplir el proveedor de servicios en la nube 260
6.11.1. Sector privado 260
6.11.2. Sector Público 261
7. Propiedad intelectual 263

7.1. Cuestiones relativas a la protección de la propiedad intelectual 263
7.2. Licencias de *software* 265
7.2.1. Leyes que rigen las licencias de *software* 265
7.3. Una referencia específica al SaaS 274
7.4. Instituciones de gobierno 275
7.4.1. Instituto Nacional del Derecho de Autor (INDAUTOR) 275
7.4.2. Instituto Mexicano de la Propiedad Industrial (IMPI) 278
7.5. Jurisprudencia en materia de licencias de *software* 280
8. El documento electrónico y la firma electrónica 281
8.1. Firma electrónica 281
8.1.1. Tipos de firma electrónica 283
8.1.2. Instituciones de gobierno encargadas del manejo de la Firma Electrónica 285
8.1.3. Atribuciones y obligaciones de las autoridades certificadoras 286
8.1.4. Obtención de firma electrónica 287
8.1.5. Validez y eficacia probatoria 288
8.1.6. Instituciones de gobierno 291
8.1.7. Jurisprudencia 293
8.2. Documentos electrónicos 294
8.2.1. Validez y eficacia probatoria 295
9. Delitos informáticos 296
9.1. Notas sobre los delitos informáticos en el Código Penal Federal 297
9.2. La ciberseguridad y la ciberdelincuencia. 299
9.3. Protección penal de máquinas y servicios de comunicaciones electrónicas 304
9.4. Otros bienes jurídicos objeto de protección 306
10. Cuestiones contractuales 309
10.1. Acuerdo de nivel de servicio (SLA) entre el prestador de servicios y el usuario 309
10.2. Garantías legales y contractuales 310
10.3. Responsabilidad del prestador de servicios 313
10.4. Garantías de interoperabilidad, portabilidad de datos y reversibilidad: el usuario no cautivo 313

10.5. Cuestiones específicas de la contratación de cómputo en la nube en el sector público 316
11. Cuestiones de política pública a considerar sobre la computación en la nube 319
11.1. (Des)regulación y/o adecuación de la normatividad aplicable 320
11.2. Políticas públicas a considerar 322
11.2.1. Impulso de las Tecnologías de la Información (TI) en México 322
11.2.2. Cuestiones fiscales a considerar 324
11.2.3. Ancho de banda y otras cuestiones relativas a telecomunicaciones y comunicaciones electrónicas 326
11.2.4. Posibilidades de generar empleo 328
12. Posibilidad de que México sea referente para otros países 331
12.1. Recomendaciones para la Secretaría de Economía (SE) 332

IV. CONCLUSIONES 335

V. GUÍA PRÁCTICA EN MATERIA DE ADOPCIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE PARA EMPRESAS 357
1. Implicaciones de la contratación de servicios en la nube (cloud computing), sobre todo en lo relativo a protección de datos personales y seguridad de la información 357
2. Potenciales oportunidades de negocio que el *cloud computing* ofrece para las organizaciones 358
3. Guía práctica para empresas en la adopción de servicios de cómputo en la nube 361
3.1. Qué es el cómputo en la nube y qué sujetos participan 362
3.2. Legislación aplicable 364
3.3. Aspectos a considerar previo al contrato de los servicios 364
3.4. Aspectos a considerar al contratar el servicio 366
3.5. Recomendaciones prácticas para las PYMEs 373
4. *Checklist* para la revisión del cumplimiento 375
4.1. *Checklist* general sobre cómputo en la nube 376
4.2. *Checklist* específico sobre cómputo en la nube 385

VI. RESULTADOS DE LA APLICACIÓN DE LA "GUÍA PARA EMPRESAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL USO DEL CÓMPUTO EN LA NUBE" 389

1. Uso general del cómputo en la nube 390
2. Riesgos legales y regulatorios 390
3. Datos Personales 391
4. Medidas de seguridad 394
5. Propiedad intelectual 396
6. Acuerdos de nivel de servicio (SLA) y otras cuestiones contractuales 396
7. Ciberdelitos 397
8. Administraciones Públicas 398

I. ANÁLISIS DEL USO DEL CÓMPUTO EN LA NUBE EN MÉXICO

1. Introducción

A efectos de este entregable se ha procedido a realizar una encuesta sobre el uso actual del cómputo en la nube ("*cloud computing*") por empresas en México, de manera que la misma permita tener un insumo de la situación actual entre las MiPyMEs mexicanas por lo que se refiere a la adopción y uso del cómputo en la nube.

La encuesta y los resultados obtenidos permiten tener una visión extrapolable sobre el grado de conocimiento de las MiPyMEs mexicanas en cuanto a la nube y su uso.

Además, en la encuesta, a través de las preguntas planteadas a las MiPyMes, también se ha buscado obtener información relativa al grado de conocimiento de las mismas sobre determinadas cuestiones relativas al cómputo en la nube, tales como si antes de tratar datos personales en la nube se han adoptado medidas para evitar riesgos en protección de datos personales y cumplir con la normatividad sobre protección de datos personales.

También se han incluido preguntas generales sobre el uso que actualmente están haciendo las MiPyMeEs de la nube; qué aspectos de la nube o relacionados con la misma, tales como el cumplimiento de la normatividad sobre protección de datos personales, las medidas de seguridad o las certificaciones obtenidas por los prestadores de servicios de cómputo en la nube.

Otras preguntas tienen por objeto medir qué grado de confianza tienen los clientes en los servicios de cómputo en la nube y en los prestadores de los mismos, así como otros factores que podrían, en su caso, ser relevantes para acelerar la adopción del cómputo en la nube por las MiPyMEs mexicanas.

Por cada pregunta y conforme a las respuestas recibidas se incluyen gráficos que muestran los porcentajes correspondientes, así como las respuestas recibidas.

En particular, el objeto del presente entregable es presentar la metodología que se ha seguido para la realización de la encuesta, el análisis de las respuestas a la encuesta así como las correspondientes conclusiones a las que da lugar dicho análisis.

2. Metodología de la encuesta

Los resultados sobre el uso actual del cómputo en la nube por empresas en México se basan en una encuesta que fue preparada al efecto y que incluía un total de diez (10) preguntas que, tal y como se indicará a continuación, se refieren tanto a cuestiones generales como particulares en relación con el cómputo en la nube.

La base de la encuesta han sido MiPyMEs mexicanas, habiéndose puesto a disposición de un amplio número de empresas, principalmente a través de medios electrónicos y en otros casos contactando a algunas empresas, y recibiéndose un total de 250 respuestas.

Con las respuestas recibidas se han elaborado diferentes gráficos por cada una de las mismas en los que se muestran los porcentajes relativos a las diversas opciones de respuesta. Además, por cada pregunta se incluyen también el número de respuestas recibidas para cada opción así como el número total de respuestas recibidas y, en su caso, el número que no han respondido. Respecto a este último número, cabe señalar que en ocasiones puede deberse a que la empresa no sabía contestar o ha decidido no hacerlo.

Para facilitar la comprensión de la pregunta, por cada una de las mismas se ha incluido una breve explicación a través de la que se pone en contexto dicha pregunta y con la finalidad de que sirviera para que la empresa pudiera responder sin dificultad.

A continuación, se analizan las respuestas recibidas por cada una de las preguntas formuladas y al final se incluye, como anexo, la encuesta.

3. Análisis de las preguntas

Este apartado está dedicado a analizar la información obtenida en virtud de las respuestas recibidas a las preguntas planteadas en la encuesta.

Ya que en el Anexo se reproduce la encuesta realizada y por motivos expositivos, en este apartado se resume, en su caso, el enunciado de las preguntas.

Cabe señalar que el análisis combina gráficos, que se han podido elaborar con base en las respuestas obtenidas, así como una explicación que complementa tanto el enunciado de la pregunta correspondiente como las respuestas recibidas en su caso.

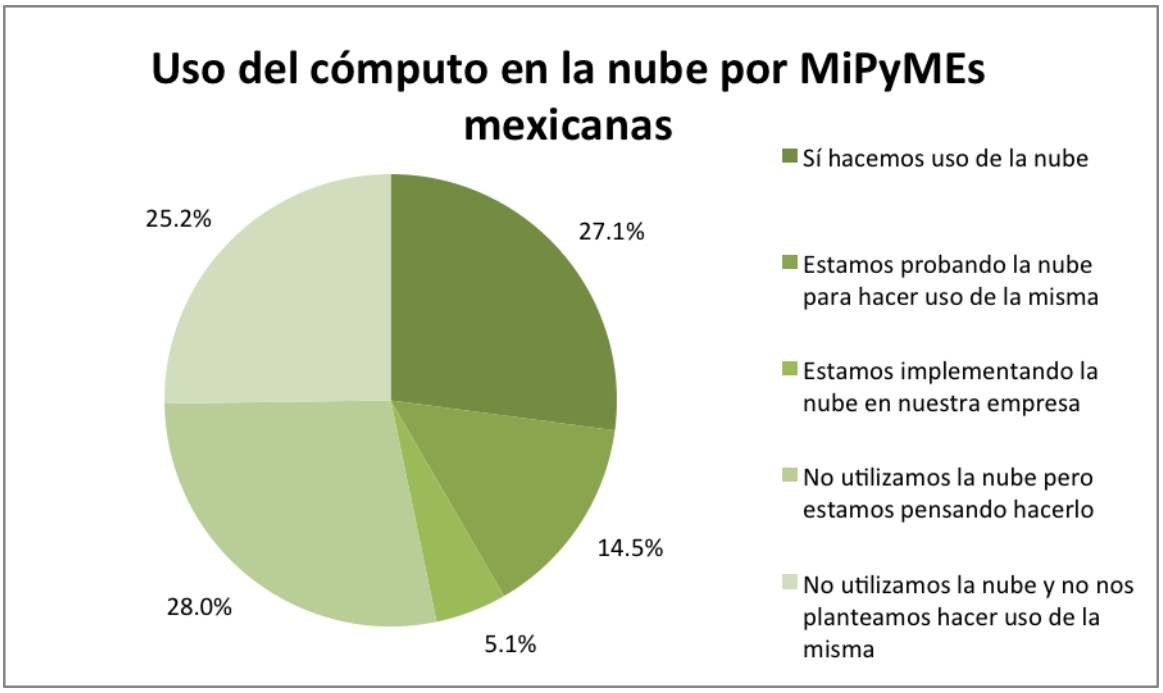
Por lo tanto, a continuación se incluyen las diez (10) preguntas con el análisis al que dan lugar las mismas.

3.1. Uso actual de la nube en la empresa

En esta primera pregunta, haciendo referencia a que según el Instituto Mexicano para la Competitividad (IMCO), en 2012 un 26% de las empresas mexicanas ya utilizaban cómputo en la nube[1], se planteaba si la empresa está haciendo actualmente uso de servicios de cómputo en la nube o si tiene intención o no de hacer uso de la misma en el futuro.

[1] El IMCO cita dicha cifra en relación con una encuesta realizada por ISACA en su IT Risk/Reward Barometer – Mexico Edition, 2011, en el white paper *"Cómputo en la nube": nuevo detonador para la competitividad de México*. Pág. 27. Disponible en el vínculo electrónico http://imco.org.mx/wp-content/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

Es así que las respuestas recibidas dan lugar a la siguiente gráfica:



Puede verse que el 27,1% de las MiPyMEs mexicanas está haciendo actualmente uso de la nube, lo que supone que cada vez sean más las que suman a la misma. Además, un 28% no está haciendo actualmente uso de servicios de cómputo en la nube, pero tiene pensado hacer en el futuro, lo cual determina que el futuro de las MiPyMEs esté en la nube y que sean relativamente pocas las que no están pensando en hacer uso de la misma.

Al respecto, un 25,2% de las empresas que han respondido a la encuesta han respondido que *"no utilizamos la nube y no nos planteamos hacer uso de la misma"*, cuestión que deberá ser tomada en consideración ya que plantea a su vez cuestiones tales si la respuesta se deba a la falta de concientización sobre las ventajas que pueden implicar los servicios de cómputo en la nube o si la nube no es vista como una opción para las mismas.

Es decir, la adopción de servicios de cómputo en la nube en México avanza, pero lo hace de manera moderada y todavía con un amplio porcentaje de empresas que todavía no lo han hecho o, incluso, no tienen pensado hacerlo.

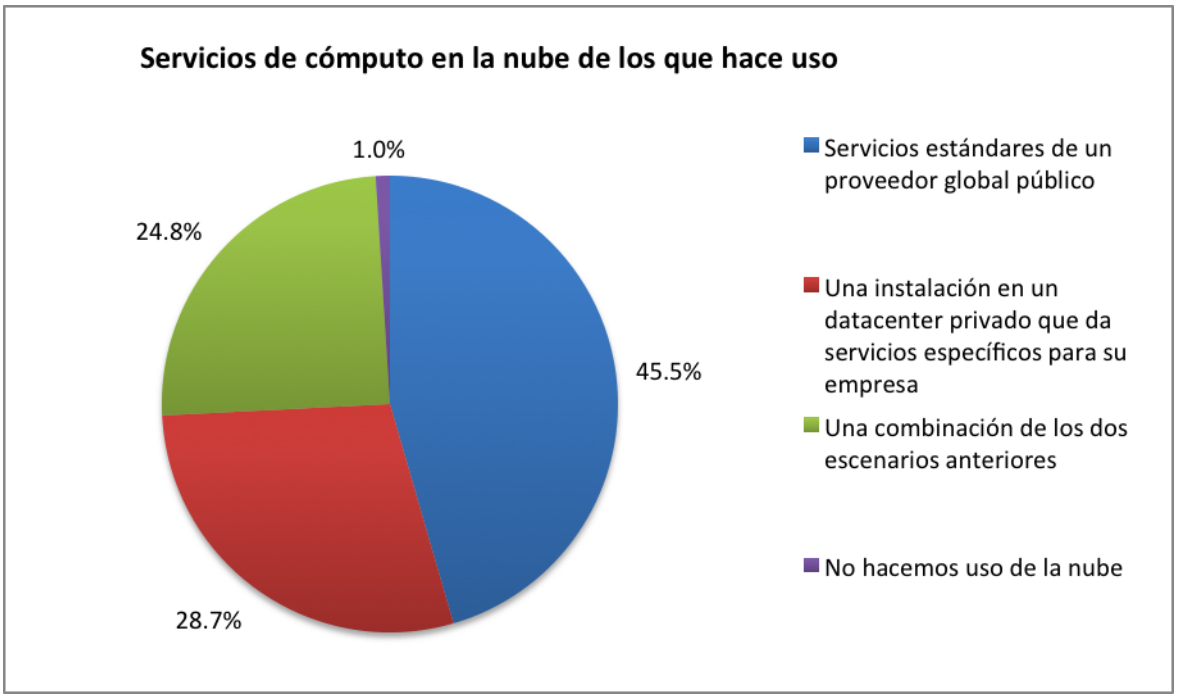
Como conclusión preliminar, es posible señalar que las MiPyMEs mexicanas siguen una evolución ascendente en cuanto a la adopción del cómputo en la nube, si bien más de la mitad todavía no lo han hecho, pero piensan hacerlo en el futuro 28%, y otro 25,2% no se plantean hacerlo.

3.2. Servicios de cómputo en la nube que se utilizan actualmente

Las respuestas a esta pregunta se reducen en buena medida debido a que no todas las empresas entrevistadas están haciendo uso de servicios de cómputo en la nube. Es así que del total de 214 empresas entrevistadas, respondieron a la misma 101, lo que supone casi un 50%.

En concreto, las opciones de respuesta sobre los servicios de cómputo en la nube eran las siguientes: servicios estándares de un proveedor global público; una instalación en un centro de datos (en inglés, datacenter) privado que da servicios específicos para su empresa, o una combinación de los dos escenarios anteriores.

El siguiente gráfico muestra los porcentajes a que da lugar, en cada caso, la pregunta a las empresas que han participado:



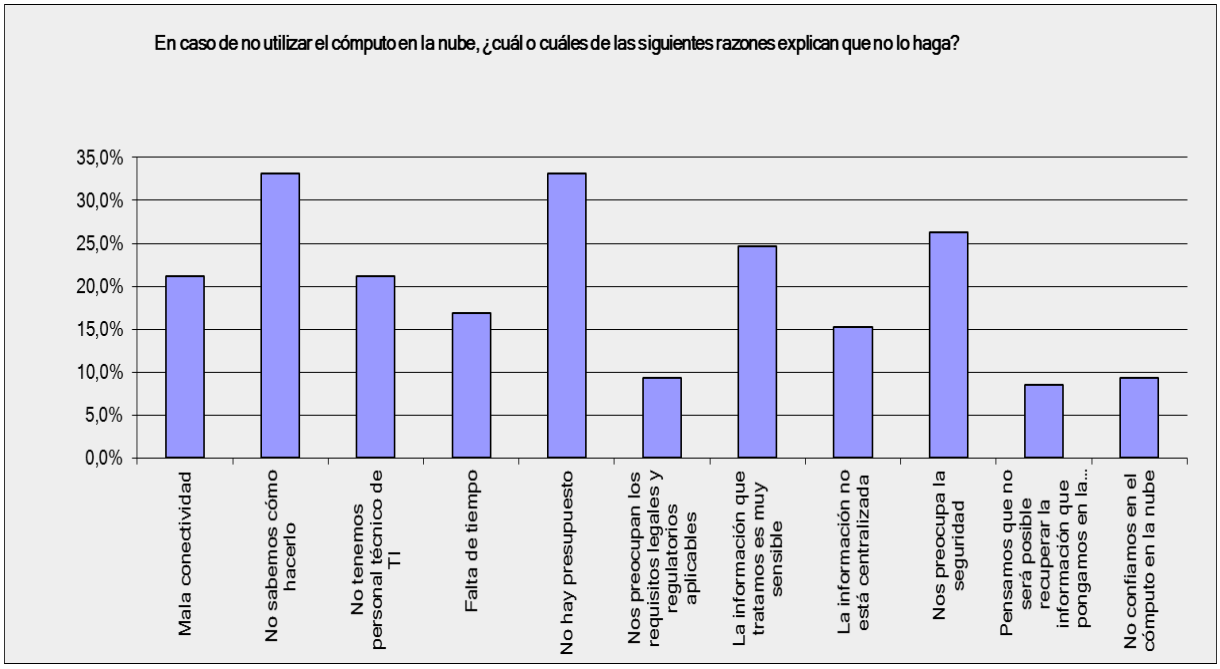
A la vista de las mismas es posible resaltar el hecho de que casi la mitad de las empresas haya respondido que utiliza servicios estandarizados de nube pública, mientras que el 24,8% han respondido que prefieren hacer uso de una combinación entre servicios de nube pública y privada.

Por lo tanto, los servicios de nube pública en el caso de las MiPyMEs mexicanas son la opción preferida, lo que puede ser relevante desde el punto de vista de los clientes, a la hora de analizar el modelo de servicios preferido y, desde el punto de vista de los proveedores de servicios de cómputo en la nube, al ofrecer nuevos servicios. Dicha opción también tiene implicaciones a la hora de analizar el cumplimiento que resulte exigible a dichos clientes, en el sentido de que es necesario tomar en consideración la oferta de los prestadores de servicios de cómputo en la nube y el grado de cumplimiento que éstos ofrecen en relación con dicha nube pública.

3.3. ¿Por qué motivo o motivos no hace uso del cómputo en la nube?

Tomando en consideración que hay empresas que actualmente no hacen uso del cómputo en la nube, no piensan hacerlo o incluso no están aprovechando todas las oportunidades que ofrece aquélla, se preguntó a las empresas sobre la razón o razones ofreciendo una lista de opciones entre las que se incluían, por ejemplo, mala conectividad, falta de presupuesto, tratamiento de datos sensibles, preocupación por la seguridad o falta de confianza en el cómputo en la nube.

El siguiente gráfico muestra los porcentajes a que dan lugar las respuestas en atención a los diferentes motivos planteados para que las empresas no estén haciendo uso de los servicios de cómputo en la nube en México:



A la vista de las razones o motivos planteados por las empresas, en primer lugar, con un 33,1% de respuestas, se encuentra el hecho de no tener presupuesto así como no saber cómo hacerlo; seguido por el hecho de que a las empresas les preocupa la seguridad en el 26,3% de los casos y tratar información sensible en el 24,6% de casos.

Otras razones relevantes por las que las empresas no están haciendo uso del cómputo en la nube en México es por mala conectividad así como no tener personal técnico de TI (21,2%).

Cabe señalar que sólo un 9,3% de las empresas que han respondido señalan que no confían en la nube. También es relevante que un pequeño porcentaje (8,5%), haya respondido que le preocupa que no será posible recuperar la información que pongan en la nube, por lo que el conocido como *"vendor lock in"* no se convierte en un obstáculo, o al menos no es percibido así por los clientes de servicios de cómputo en la nube.

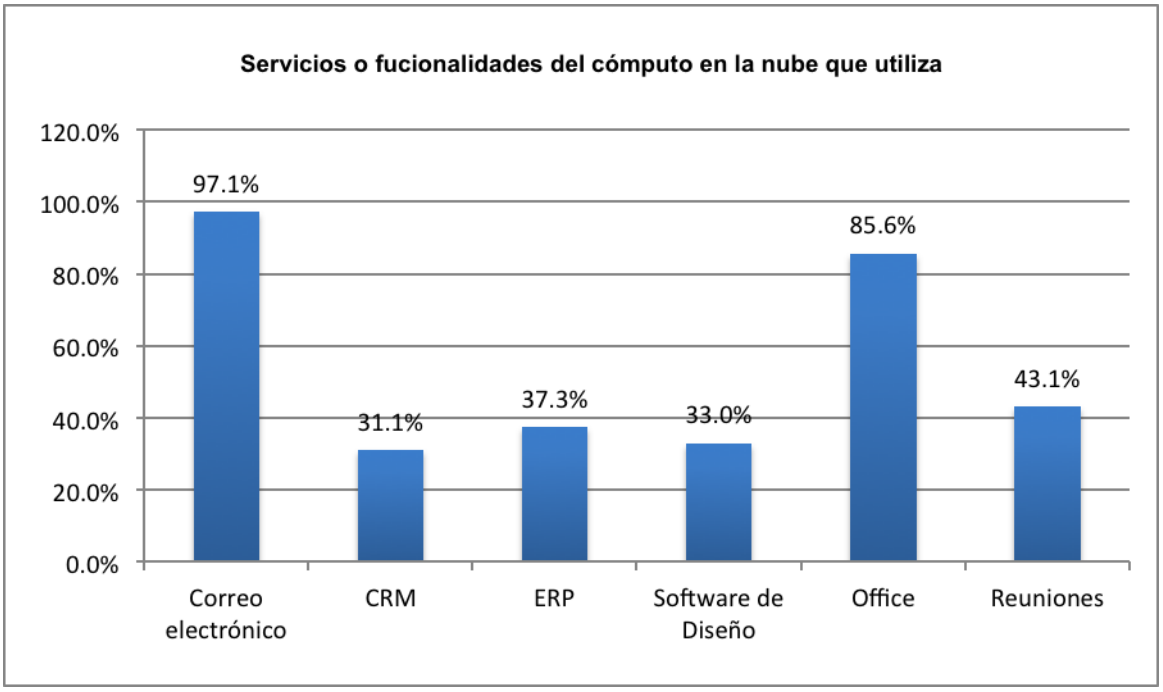
En definitiva, en el caso de las MiPyMEs mexicanas hay varios factores o razones que desincentivan el uso del cómputo en la nube, convirtiéndose en una barrera para la adopción de los mismos, entre los que destacan los relativos a falta de presupuesto, no saber cómo hacerlo, considerar que la información que tratan es muy sensible o preocupaciones relativas a la seguridad.

3.4. ¿Qué servicios tecnológicos utiliza en el cómputo en la nube?

Se trataba de preguntar a las empresas sobre los servicios tecnológicos que utilizan para el desarrollo de su negocio en atención a las necesidades que puedan tener en cada momento.

Al respecto, se daban varias opciones entre las que se encuentran el correo electrónico, la gestión de relaciones con los clientes (*Customer Relationship Management*, CRM), el software de diseño o las reuniones.

En relación con dichas funcionalidades, la siguiente gráfica muestra los porcentajes en cada caso en atención al número de respuestas recibidas:



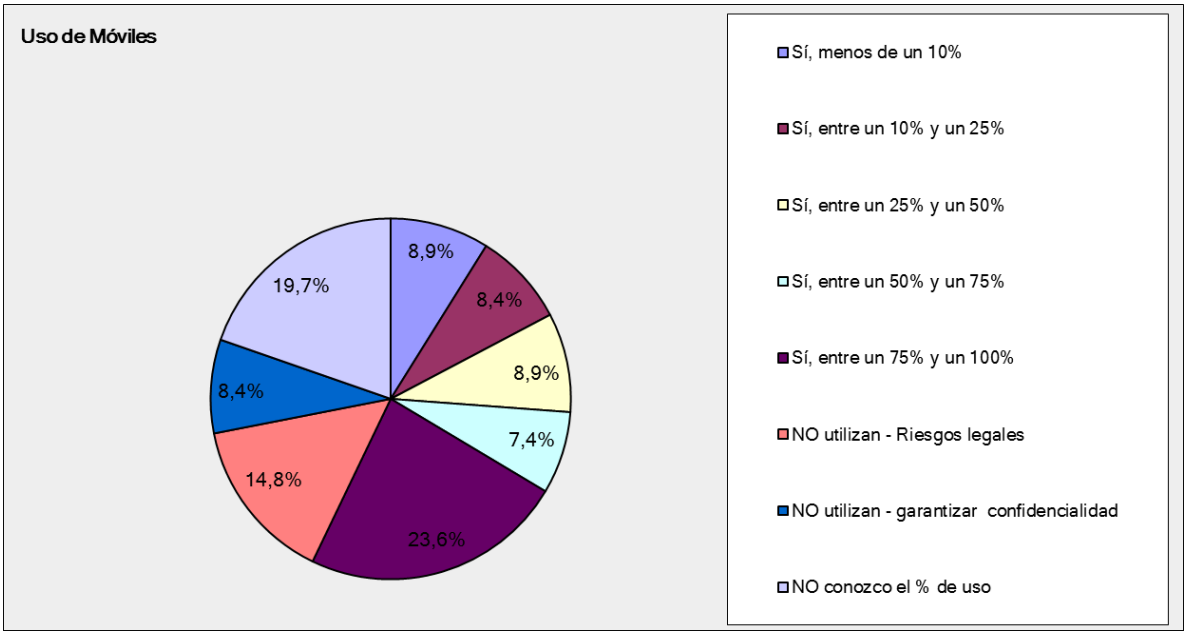
Cabe señalar que, con mucha diferencia, las principales funcionalidades utilizadas por las empresas son el correo electrónico (97,1%) y Office (85,6%), seguido por el software y/o aplicaciones de reuniones (43,1%) y por último el resto de servicios relativos a CRM, ERP y software de diseño.

3.5. ¿Sabe o ha calculado qué porcentaje de sus empleados utiliza dispositivos móviles para acceder a la información?

Siendo una de las ventajas del cómputo en la nube la movilidad, que se concreta en la posibilidad de poder acceder a la información en cualquier momento y desde cualquier lugar, se preguntó a las empresas sobre si sabía o había calculado qué porcentaje de sus empleados utiliza dispositivos móviles, tales como tabletas inteligentes

("tablets"), teléfonos inteligentes ("smartphones"), para acceder a la información.

Es así que el siguiente gráfico muestra los porcentajes correspondientes tanto en el caso de que se haya calculado por las empresas el porcentaje de empleados sí hace uso de dispositivos para el acceso a la información como aquellos otros en los que no se haya calculado dicho porcentaje o no se esté haciendo uso de dichos dispositivos por considerar que existen riesgos legales o riesgos para poder garantizar la confidencialidad y seguridad de los datos personales:



Respecto a los casos en los que no se hace uso de dispositivos, resulta relevante el hecho de que casi el 14,8% consideren que hay riesgos normativos y regulatorios en materia de protección de datos personales.

También resulta relevante que un 19,7% desconozca el uso que sus empleados están haciendo en su caso de dispositivos móviles para acceder a la información, lo que supone que haya empresas que pueden estar, por una parte, en riesgo de incumplimiento y, por otra

parte, perdiendo oportunidades que ofrece el uso de los mismos y las ventajas que ofrece el cómputo en la nube.

3.6. ¿Trata datos personales en la nube?

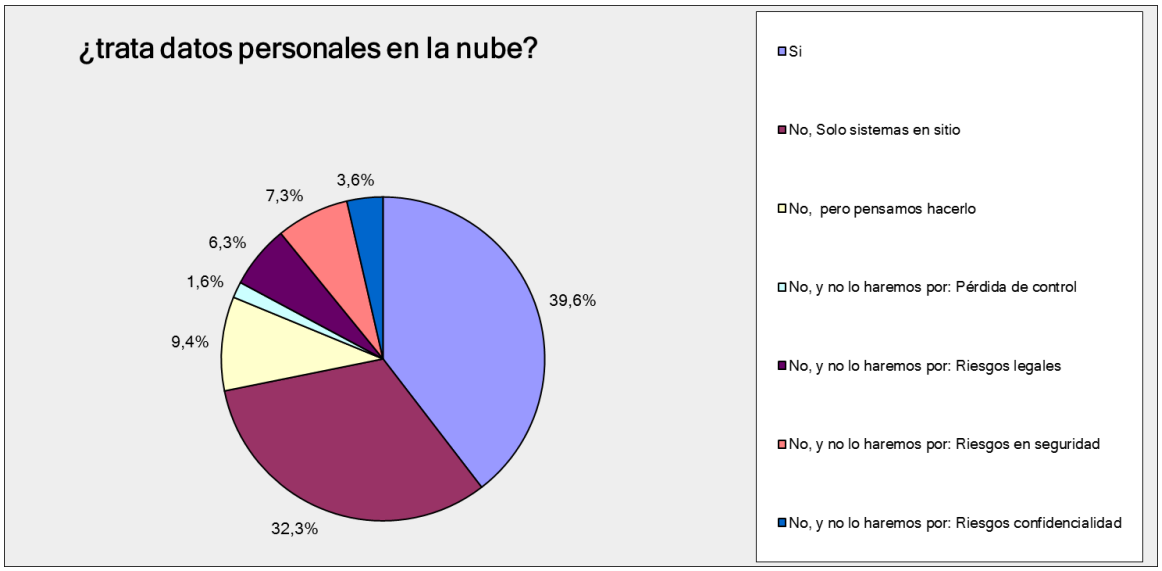
Siguiendo con la pregunta anterior, en esta se planteaba si la información a la que acceden los empleados o colaboradores a través de la nube son datos personales, en el sentido de la normatividad sobre protección de datos personales, que los define en la fracción V, del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[2] (LFPDPPP), se entiende *"cualquier información concerniente a una persona física identificada o identificable."*[3]

Las opciones de respuesta se dividían en primer lugar en sí o no, habiendo a su vez varias opciones en el caso de que se respondiera que no se tratan datos personales en la nube.

El siguiente gráfico resume y muestra los porcentajes correspondientes:

[2] Publicada en el Diario Oficial de la Federación de 5 de julio de 2010 y disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

[3] Por lo que se refiere al concepto de persona física identificable, ésta es definida en la fracción VIII del artículo 2 del Reglamento de la LFPDPPP como *"Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas."* Disponible en el vínculo electrónico http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011



De entre las empresas que respondieron, cabe señalar que el 39,6% señaló que sí trata datos personales en la nube, siendo llamativo ya que la cifra representa casi el 40% de las empresas encuestadas.

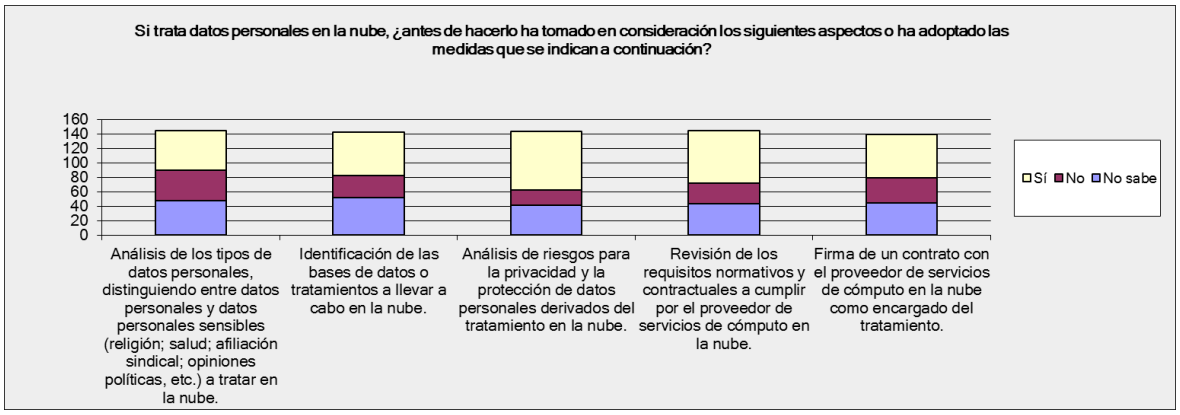
Por su parte, el resto respondió que no trababa datos personales en la nube. Entre los motivos que indicaron estas empresas, un 32,3% respondió que los datos personales solo se manejan en los sistemas en sitio. Cabe señalar que el total de empresas que respondió no tratar datos personales en la nube por la existencia de riesgos legales (6,3%); en materia de medidas de seguridad (7,3%) y de confidencialidad (3,6%).

En definitiva, los riesgos normativos y regulatorios en materia de protección de datos personales, medidas de seguridad y confidencialidad son percibidos por la mayoría de las MiPyMEs mexicanas como un problema a la hora de tratar datos personales en la nube.

3.7. Si trata datos personales en la nube, ¿ha considerado aspectos para evitar riesgos o ha adoptado medidas para mitigarlos?

Dirigida a las empresas que tratan datos personales en la nube, la pregunta tiene por objeto obtener información sobre si las mismas han tomado en consideración cuestiones que inciden en la identificación de riesgos así como en el cumplimiento, y también si se han adoptado en su caso medidas que permitan reducir estos riesgos.

El siguiente gráfico muestra las opciones y las respuestas dadas por las empresas:



Entre las respuestas dadas por las empresas cabe destacar que en todos los casos hay un alto número de empresas no ha adoptado medidas o no sabe al respecto. Por ejemplo, un 42% no ha realizado un análisis que le permita distinguir entre datos personales y datos personales sensibles[4] y un porcentaje similar (48%) no sabe al respecto. De igual manera, un 29% no ha procedido a revisar los requisitos normativos y contractuales que tiene cumplir con el proveedor de servicios de cómputo en la nube, lo que supone que

[4] Definidos éstos por la fracción VI del artículo 3 de la LFPDPPP como *"Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual."*

podrían estar incumpliendo la normatividad sobre protección de datos personales si se tratan datos personales entre el responsable y el encargado del tratamiento, a menos que este último les haya hecho firmar un contrato que cumpla con dichos requisitos. Y también un 43% dice no saber nada al respecto.

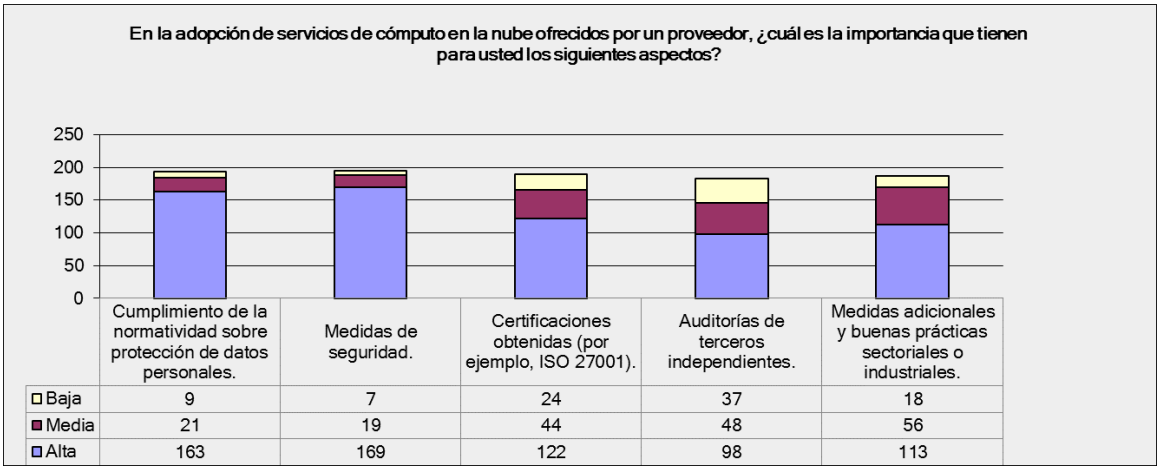
Por lo tanto, la pregunta sirve para demostrar que específicamente en materia de protección de datos personales en el cómputo en la nube pueden darse porcentajes relevantes de incumplimiento bien por falta de adopción de medidas o bien por desconocimiento de las empresas.

3.8. ¿Qué importancia tienen los aspectos que se indican para la adopción del cómputo en la nube?

Se preguntaba específicamente por cuestiones relativas al cumplimiento y otras cuestiones que ofrece, en su caso, el prestador de servicios de cómputo en la nube.

Es así que, entre dichas cuestiones, se hacía referencia al cumplimiento de la normativa sobre protección de datos personales, las medidas de seguridad, certificaciones obtenidas u otras medidas adicionales.

El gráfico al que dan lugar las respuestas dadas por las empresas encuestadas es como sigue:



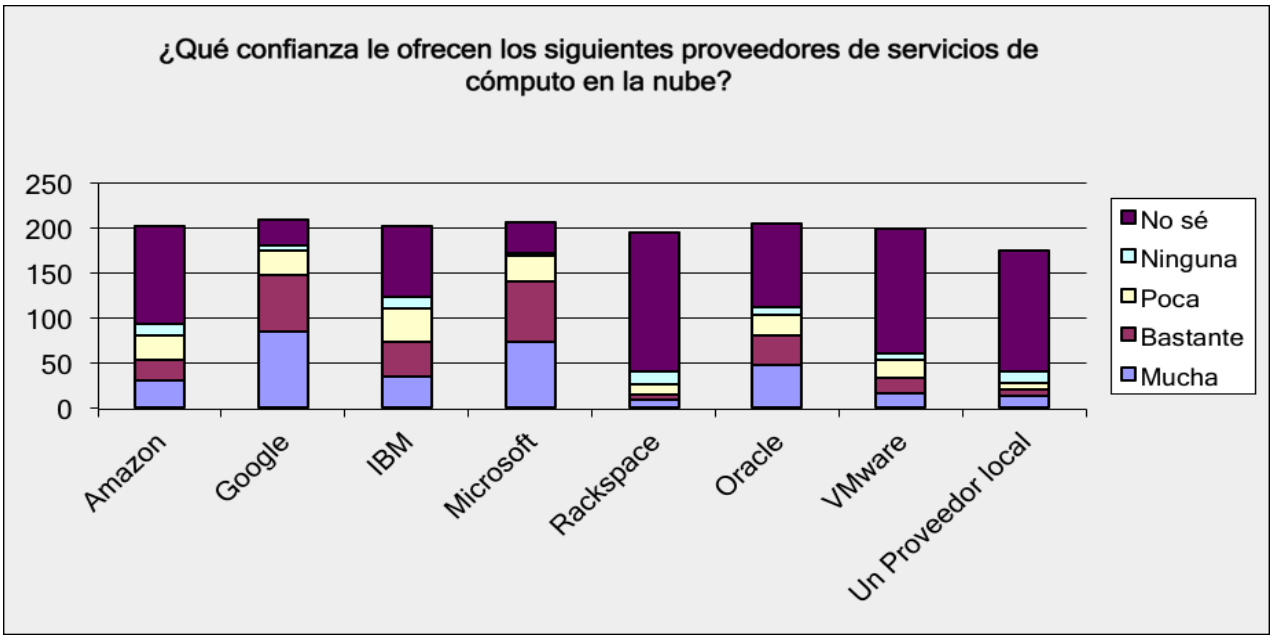
	Cumplimiento de la normatividad sobre protección de datos personales.	Medidas de seguridad.	Certificaciones obtenidas (por ejemplo, ISO 27001).	Auditorías de terceros independientes.	Medidas adicionales y buenas prácticas sectoriales o industriales.
Baja	9	7	24	37	18
Media	21	19	44	48	56
Alta	163	169	122	98	113

A la vista de las respuestas, cabe señalar que los porcentajes más altos y, por lo tanto, los aspectos más relevantes que los clientes de servicios de cómputo en la nube toman en consideración son los relativos a cumplimiento de la normatividad sobre protección de datos personales (84,46%) y medidas de seguridad (86,67%), seguidas por las certificaciones obtenidas por los prestadores de servicios de cómputo en la nube (64,21%) y, en último lugar, las auditorías de terceros independientes (53,55%).

En definitiva, las respuestas dadas por las empresas encuestadas permiten concluir que los clientes de servicios de cómputo en la nube buscan un alto de grado de cumplimiento por los prestadores de servicios de cómputo en la nube, siendo el cumplimiento normativo en materia de protección de datos personales y la seguridad los aspectos más relevantes para ellos.

3.9. ¿Qué confianza le ofrecen los siguientes prestadores de servicios de cómputo en la nube?

Con esta pregunta se trataba de obtener información sobre el grado de conocimiento de las empresas encuestadas sobre los diferentes prestadores de servicios de cómputo en la nube que actualmente ofrecen servicios, así como en su caso la confianza que les transmiten a la hora de prestar servicios de cómputo en la nube.



De entre la lista de prestadores de servicios de cómputo en la nube, y atendiendo a las respuestas proporcionadas, destaca el hecho de que la mayoría desconoce la existencia de prestadores locales, seguido por Rackspace y VMare.

En cuanto a los más conocidos y el mayor grado de confianza que ofrecen a los clientes, hay dos prestadores de servicios de cómputo en la nube que destacan con respecto al resto. Éstos son, Google (40,87%) seguido muy de cerca por Microsoft (35,92%) A cierta distancia les siguen Oracle (22,93%) e IBM (17,33%).

En definitiva, las empresas mexicanas encuestadas conocen una variada lista de prestadores de servicios de cómputo en la nube, si bien indican mostrar más confianza en dos, que son Google y Microsoft. No obstante, hay prestadores de servicios de cómputo en la nube que sí son conocidos por otras empresas y que encabezan los rankings en otras áreas geográficas, tales como Amazon o VMare, pero que son en gran medida desconocidos para las MiPyMEs mexicanas.

3.10. Si tuviera forma de asegurar o monitorizar su información en la nube, ¿haría más uso de ésta?

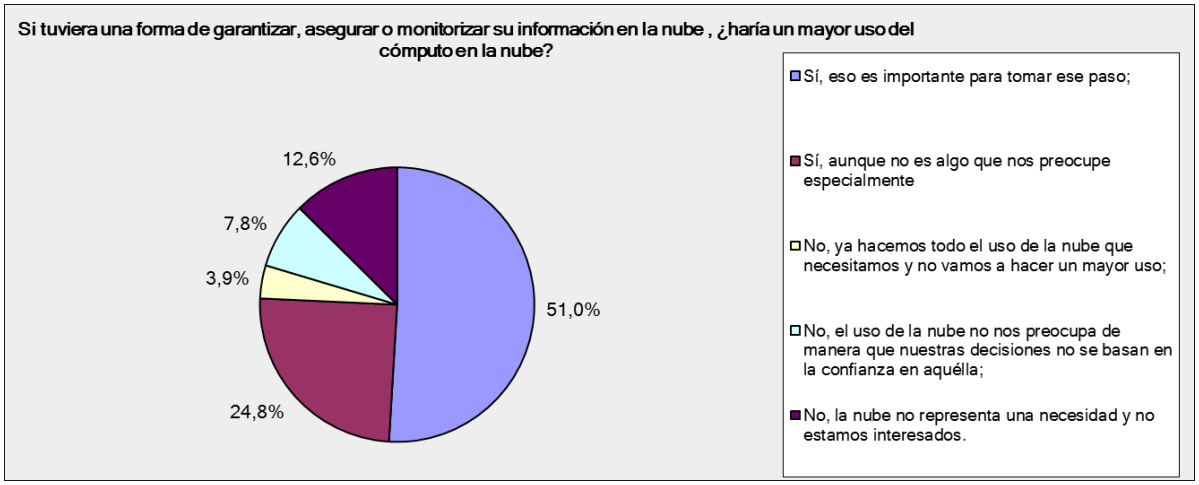
La última pregunta tenía por objeto obtener la opinión de las empresas sobre si garantizar, asegurar o monitorizar su información en la nube y pudiese cumplir con las regulaciones y requisitos que le atañen es un detonante o no para la adopción del cómputo en la nube.

Al respecto, para poco más de la mitad de las empresas (50,97%) que han respondido a la pregunta, sí es una cuestión importante, lo cual es llamativo ya que para gran parte del resto no es algo relevante a la hora de hacer uso de servicios de cómputo de cómputo en la nube.

En concreto, para un (24,76%) tener la posibilidad de garantizar, asegurar o monitorizar su información en la nube sería un factor a considerar para hacer mayor uso de la nube, si bien no es algo que les preocupe especialmente.

Por último, destaca también el hecho de que para un (12,62%) la nube no sea una necesidad y por lo tanto no estén interesados en esta cuestión.

El siguiente gráfico incluye las respuestas obtenidas a la pregunta:



En definitiva, cabe señalar que garantizar, asegurar o monitorizar la información en la nube y poder cumplir con las regulaciones y requisitos es un factor relevante para más de la mitad de servicios de cómputo en la nube, si bien casi otra mitad podrían no estar valorando esta posibilidad correctamente al no entender las implicaciones de incumplir dichas regulaciones o los requisitos que son exigibles a la hora de contratar servicios de cómputo en la nube

4. Conclusiones

En virtud del análisis efectuado sobre la encuesta relativa al uso actual del cómputo en la nube por empresas mexicanas, es posible presentar las siguientes conclusiones:

- La adopción del cómputo en la nube entre las MiPyMEs mexicanas sigue avanzando, aunque no de manera acelerada, pudiendo ser factores relevantes para explicar esta lenta progresión la falta de presupuesto o de personal de Tecnologías de la Información (TI) que les ayuden a realizar el proceso de migración a la misma, así como el desconocimiento de la nube en sí misma. Las empresas que no adoptan el cómputo en la nube, pudiendo hacerlo, pierden oportunidades con respecto a otras, incluso grandes empresas, porque se ven privadas del acceso a tecnología que les permitiría ser más competitivas.

- De las respuestas a la pregunta sobre el uso del cómputo en la nube por las empresas mexicanas, cabe concluir que el futuro pasa por la nube, ya que actualmente un 27,10% hacen uso de la misma y un 28% se plantea hacerlo en el futuro. Al respecto, la adopción de la nube puede convertirse en un diferencial competitivo para las mismas, ya que gracias a la posibilidad de acceder a tecnología que de otra manera no sería posible, las MiPyMEs mexicanas pueden competir con grandes empresas. No obstante, es necesario tomar en consideración que un 25,2% no

se plantea hacer uso de la nube, pudiendo perder oportunidades y ser menos competitivas al no hacer un uso eficiente de las TIC.

- Por lo que se refiere a los servicios de los que las empresas hacen uso en la nube actualmente, casi la mitad de las empresas que han participado en la encuesta utiliza servicios estandarizados de nube pública mientras que un 24,75% prefieren hacer uso de una combinación entre servicios de nube pública y privada.

- Entre las razones para no hacer uso de la nube, los principales motivos son no tener presupuesto o no saber cómo hacer uso del cómputo en la nube en el (33,05%) y la mala conectividad o falta de personal técnico de TI (21,19%). Además, otra razón relevante planteada por las empresas para no hacer uso de la nube es el hecho de tratar información que consideran como muy sensible. Por lo tanto, sería aconsejable tomar en consideración dichos factores con la finalidad de que no se conviertan en barreras para las empresas a la hora de adoptar servicios de cómputo en la nube.

- En cuanto al uso de dispositivos para que empleados y colaboradores accedan a la información desde cualquier lugar y en cualquier momento, cabe destacar que, por una parte, un 15,78% ha manifestado que no hace uso de dispositivos porque considera que existen riesgos normativos y regulatorios en protección de datos personales y, por otra parte, un 19,70% desconoce el uso que sus empleados están haciendo en su caso de dispositivos móviles para acceder a la información, lo que supone que haya empresas que pueden estar en riesgo de incumplimiento y/o perdiendo oportunidades de beneficiarse del uso del cómputo en la nube.

- Un 39,58% de las empresas que han participado en la encuesta ha señalado que trata datos personales en la nube. Por el contrario, hay un alto porcentaje de empresas que ha respondido que no trata datos personales en la nube, siendo los principales motivos el hecho de que los datos personales solo se manejan en los sistemas en sitio (32,29%); la existencia de riesgos legales (6,25%); o riesgos en materia de medidas de seguridad (7,29%) y de confidencialidad (3,65%).

- Es relevante señalar que en respuesta a la pregunta sobre si se han considerado aspectos para evitar riesgos en cuanto al tratamiento de datos personales en la nube, tales como realizar un análisis que permita distinguir entre datos personales y datos personales sensibles o revisar los requisitos normativos y contractuales que tiene cumplir con el proveedor de servicios de cómputo en la nube, un elevado porcentaje de empresas haya respondido que no o que no sabe al respecto, lo que podría ser indicativo de incumplimientos en materia de la normatividad sobre protección de datos personales.

- Cabe señalar que a la hora de adoptar servicios de cómputo en la nube, los clientes buscan un alto de grado de cumplimiento por los prestadores de servicios de cómputo en la nube, siendo el cumplimiento normativo en materia de protección de datos personales (84,46%) y la seguridad (86,67%) los aspectos más relevantes para ellos. Adicionalmente, las certificaciones obtenidas por los prestadores de servicios de cómputo en la nube (64,21%) son también uno de los principales aspectos que los clientes valoran a la hora de usar la nube.

- Por lo que se refiere al grado de conocimiento y confianza de los prestadores de servicios de cómputo en la nube, hay dos que centran la atención de la mayoría de las empresas que han participado en la encuesta y que son Google (40,87%) y Microsoft (35,92%).

- Por último, la posibilidad de garantizar, asegurar o monitorizar la información en la nube y poder cumplir con las regulaciones y requisitos es un factor relevante para más de la mitad de servicios de cómputo en la nube, si bien casi otra mitad podrían no estar valorando esta posibilidad. En este último caso, cabe pensar que las empresas pueden no estar entendiendo la importancia de instrumentos que garanticen el cumplimiento a lo largo del periodo de prestación de servicios de cómputo en la nube.

- Como conclusión final y a la vista de las respuestas recibidas, cabría señalar que son necesarias acciones que tengan por objeto concientizar a las MiPyMEs mexicanas sobre las implicaciones del uso de servicios de cómputo en la nube, tanto por lo que se refiere al cumplimiento legal y regulatorio como a los beneficios que puede tener dicho uso, permitiéndoles acceder a una mejor tecnología que puede ayudarles a ser más competitivas.

Anexo A – Formulario de Encuesta

ENCUESTA SOBRE EL USO ACTUAL DEL CÓMPUTO EN LA NUBE (´CLOUD COMPUTING´) POR EMPRESAS MEXICANAS

Como sabe, el cómputo en la nube permite a las organizaciones obtener servicios de cómputo (software, infraestructura o plataforma) bajo demanda. Es decir, se trata, tal y como lo define el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de un *"modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente."*

El cómputo en la nube está suponiendo una auténtica revolución para las empresas, con independencia de cuál sea su tamaño y sector de actividad, ya que la forma tradicional de gestionar las Tecnologías de Información (TI) no permite ajustarse elásticamente a las necesidades cambiantes del negocio y por lo tanto ser competitivo.

Para las organizaciones mexicanas el cómputo en la nube sigue siendo un reto y una oportunidad. Es por ello que la Secretaría de Economía, con el patrocinio del Banco Mundial, está llevando a cabo un estudio en virtud del que pueda fomentar mejores prácticas que ayuden al sector de TI y a dichas organizaciones mexicanas. El **Estudio Jurídico PIÑAR MAÑAS & ASOCIADOS MEXICO, S.C.** ha recibido el encargo de la Secretaría de Economía para realizar dicho estudio, de manera que la información que usted proporcione será tratada por dicha firma con la finalidad de que la Secretaría de Economía pueda conocer la situación actual del cómputo en la nube en México.

Es por ello que le pedimos y agradecemos de antemano si pudiera dedicar unos minutos de su valioso tiempo a responder a las preguntas que se presentan a continuación. Su aportación ayudará a

muchas empresas mexicanas a comprender el significado e implicaciones del cómputo en la nube.

NOMBRE O RAZÓN SOCIAL DE LA EMPRESA: _____

ÁREA DE ACTIVIDAD O NEGOCIO: _____

NÚMERO DE EMPLEADOS: ☐ 1-10 ☐ 11-50 ☐ 51-250 ☐ Más de 251

1. Conforme a los datos manejados por el Instituto Mexicano para la Competitividad (IMCO), en 2012 un 26% de las empresas mexicanas ya utilizaban cómputo en la nube, pudiendo tratarse de:

a. Uso de Software como servicio (en inglés, Software as a Service, SaaS), como por ejemplo Office 365

b. Infraestructura como servicio (Infraestructure as a Service, IaaS), como por ejemplo Amazon Web Services

c. Plataforma como servicio (Platform as a Service, PaaS) como por ejemplo Windows Azure o Google Apps Engine.

En este momento ¿cuál es la situación de uso de computación en la nube en su empresa?

☐ Sí hacemos uso de la nube;
☐ Estamos probando la nube para hacer uso de la misma;
☐ Estamos implementando la nube en nuestra empresa;
☐ No utilizamos la nube pero estamos pensando hacerlo;
☐ No utilizamos la nube y no nos planteamos hacer uso de la misma.

2. En caso de utilizar actualmente la nube, indique de cuál o cuáles hace uso:

☐ Servicios estándares de un proveedor global público;
☐ Una instalación en un datacenter privado que da servicios específicos para su empresa;
☐ Una combinación de los dos escenarios anteriores.

3. En caso de no utilizar el cómputo en la nube, ¿cuál o cuáles de las siguientes razones explican que no lo haga?

☐ Mala conectividad;
☐ No sabemos cómo hacerlo;
☐ No tenemos personal técnico de TI;
☐ Falta de tiempo;
☐ No hay presupuesto;
☐ Nos preocupan los requisitos legales y regulatorios aplicables;
☐ La información que tratamos es muy sensible;
☐ La información no está centralizada;
☐ Nos preocupa la seguridad;
☐ Pensamos que no será posible recuperar la información que pongamos en la nube;
☐ No confiamos en el cómputo en la nube;
☐ Otro (indicar cuál): _____

4. Como sabrá, hay diferentes posibilidades que pueden facilitar el desarrollo de su negocio, ya que permiten el uso de recursos tecnológicos según las necesidades que pueda tener en cada momento. Al respecto, por favor, responda si actualmente hace uso de alguno de los siguientes:

☐ Correo electrónico
☐ CRM
☐ ERP
☐ Software de Diseño
☐ Office
☐ Reuniones
☐ Otro: _____

5. La nube ofrece a las empresas la posibilidad de hacer uso de recursos tecnológicos en cada momento en atención a las necesidades que pueda tener y, además, facilita que empleados o colaboradores puedan acceder a la información que necesitan desde cualquier lugar en cualquier momento. En este sentido, ¿sabe o ha calculado qué porcentaje de sus empleados o colaboradores utilizan dispositivos móviles (smartphones, tablets, etc.) para acceder a la información?

☐ Sí, un ____ por cien utiliza dispositivos móviles para acceder a la información;

☐ No, mis empleados no utilizan dispositivos móviles para acceder a la información empresarial por las siguientes razones (marque la(s) que corresponda(n)):

○ Riesgos legales en cuanto al uso de dispositivos móviles conforme a la normatividad sobre protección de datos personales;

○ Riesgos para poder garantizar la confidencialidad y seguridad de los datos personales;

○ Otros riesgos (indicar cuáles): _____

☐ No conozco el porcentaje o la forma en que mis empleados utilizan la información en sus dispositivos móviles.

6. La información a la que acceden sus empleados o colaboradores a través de la nube, ¿hace referencia a sus clientes, prospectos, empleados u otras personas físicas? Es decir, ¿trata datos personales en la nube?

☐ Sí;
☐ No.

En caso negativo explique:

☐ Los datos personales solo se manejan en los sistemas en sitio;

☐ Mi empresa no trata datos personales en la nube, pero pensamos hacerlo;

☐ No tratamos datos personales en la nube y no tenemos pensado hacerlo, por la siguiente o siguientes razones (marque la(s) que corresponda(n)):

○ Pérdida de control sobre el tratamiento de los datos personales;

○ Riesgos legales derivados de la normatividad sobre protección de datos personales;

○ Riesgos en materia de medidas de seguridad;

○ Riesgos en materia de confidencialidad;

○ Otros riesgos (indicar cuáles): _____

7. Si trata datos personales en la nube, ¿antes de hacerlo ha tomado en consideración los siguientes aspectos o ha adoptado las medidas que se indican a continuación?

Aspectos o medidas	Sí	No	No sabe
Análisis de los tipos de datos personales, distinguiendo entre datos personales y datos personales sensibles (religión; salud; afiliación sindical; opiniones políticas, etc.) a tratar en la nube.	○	○	○
Identificación de las bases de datos o tratamientos a llevar a cabo en la nube.	○	○	○
Análisis de riesgos para la privacidad y la protección de datos personales derivados del tratamiento en la nube.	○	○	○
Revisión de los requisitos normativos y contractuales a cumplir por el proveedor de servicios de cómputo en la nube.	○	○	○
Firma de un contrato con el proveedor de servicios de cómputo en la nube como encargado del tratamiento.	○	○	○

8. En la adopción de servicios de cómputo en la nube ofrecidos por un proveedor, ¿cuál es la importancia que tienen para usted los siguientes aspectos?

Aspecto a tomar en consideración en relación con el proveedor	Baja	Media	Alta
Cumplimiento de la normatividad sobre protección de datos personales.	○	○	○
Medidas de seguridad.	○	○	○
Certificaciones obtenidas (por ejemplo, ISO 27001).	○	○	○
Auditorías de terceros independientes.	○	○	○
Medidas adicionales y buenas prácticas sectoriales o industriales.	○	○	○

9. ¿Qué confianza le ofrecen los siguientes proveedores de servicios de cómputo en la nube? Si no conoce al proveedor, por favor, marque: No sé.

Proveedor de cómputo en la nube	No sé	Ninguna	Poca	Bastante	Mucha
Amazon	○	○	○	○	○
Google	○	○	○	○	○
IBM	○	○	○	○	○
Microsoft	○	○	○	○	○
Rackspace	○	○	○	○	○
Oracle	○	○	○	○	○
VMware	○	○	○	○	○
Un Proveedor local	○	○	○	○	○

10. Si tuviera una forma de garantizar, asegurar o monitorizar su información en la nube y pudiese cumplir con las regulaciones y requisitos que le atañen, ¿haría un mayor uso del cómputo en la nube?

☐ Sí, eso es importante para tomar ese paso;
☐ Sí, aunque no es algo que nos preocupe especialmente

☐ No, ya hacemos todo el uso de la nube que necesitamos y no vamos a hacer un mayor uso;
☐ No, el uso de la nube no nos preocupa de manera que nuestras decisiones no se basan en la confianza en aquélla;
☐ No, la nube no representa una necesidad y no estamos interesados.

De nuevo, le agradecemos su tiempo y las respuestas dadas a las preguntas anteriores. En caso de que usted tenga cuestiones adicionales sobre el uso del cómputo en la nube, por favor, díganos si desea que nos pongamos en contacto con usted para brindarle más información a través del teléfono o e-mail que nos indique.

Aviso legal de su interés

La presente encuesta está dirigida a su empresa, de manera que en virtud la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el DOF de 5 de julio de 2010, y del artículo 5 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el DOF de 21 de diciembre de 2011, la información relativa a empresas y/o los datos de contacto utilizados únicamente para comunicarse con una empresa quedan excluidos de la protección conferida por dicha normatividad para las personas físicas cuyos datos personales sean tratados por un responsable del tratamiento. La información obtenida en virtud de las respuestas que nos proporcione será utilizada finalmente y únicamente por **PIÑAR MAÑAS & ASOCIADOS MEXICO, S.C.** para la elaboración de un estudio sobre cómputo en la nube que le ha sido encargado, de manera que cualquier información obtenida no será utilizada con otros fines.

©PIÑAR MAÑAS&ASOCIADOS, MEXICO, S.C., 2014. Todos los derechos reservados. Prohibida la reproducción total o parcial de esta encuesta sin autorización expresa de **PIÑAR MAÑAS&ASOCIADOS, MEXICO, S.C.**

Anexo B – Tablas de Datos de Respuesta

1. Uso de Cloud computing en México

Conforme a los datos manejados por el Instituto Mexicano para la Competitividad (IMCO), en 2012 un 26% de las empresas mexicanas ya utilizaban cómputo en la nube, pudiendo tratarse de: a. Uso de Software como servicio (en inglés, *Software as a Service*, SaaS), como por ejemplo Office 365 b. Infraestructura como servicio (*Infraestructure as a Service*, IaaS), como por ejemplo Amazon Web Services c. Plataforma como servicio (*Platform as a Service*, PaaS) como por ejemplo Windows Azure o Google Apps Engine. En este momento ¿cuál es la situación de uso de computación en la nube en su empresa?		
Opciones	**Porcentaje**	**Cuenta**
Sí hacemos uso de la nube	27,1%	58
Estamos probando la nube para hacer uso de la misma	14,5%	31
Estamos implementando la nube en nuestra empresa	5,1%	11
No utilizamos la nube pero estamos pensando hacerlo	28,0%	60
No utilizamos la nube y no nos planteamos hacer uso de la misma	25,2%	54
Preguntas respondidas		**214**
Preguntas no respondidas		**0**

2. Servicios de cómputo en la nube que se utilizan actualmente

En caso de utilizar actualmente la nube, indique de cuál o cuáles hace uso:		
Opciones	**Porcentaje**	**Cuenta**
Servicios estándares de un proveedor global público	45,5%	46

Una instalación en un datacenter privado que da servicios específicos para su empresa	28,7%	29
Una combinación de los dos escenarios anteriores	24,8%	25
No hacemos uso de la nube	1,0%	1
Respondidas		**101**
No respondidas		**113**

3. ¿Por qué motivo o motivos no hace uso del cómputo en la nube?

En caso de no utilizar el cómputo en la nube, ¿cuál o cuáles de las siguientes razones explican que no lo haga?		
Opciones	**Porcentaje**	**Cuenta**
Mala conectividad	21,2%	25
No sabemos cómo hacerlo	33,1%	39
No tenemos personal técnico de TI	21,2%	25
Falta de tiempo	16,9%	20
No hay presupuesto	33,1%	39
Nos preocupan los requisitos legales y regulatorios aplicables	9,3%	11
La información que tratamos es muy sensible	24,6%	29
La información no está centralizada	15,3%	18
Nos preocupa la seguridad	26,3%	31
Pensamos que no será posible recuperar la información que pongamos en la nube	8,5%	10
No confiamos en el cómputo en la nube	9,3%	11
Otro (por favor especifique)		32
Preguntas respondidas		**118**
Preguntas no respondidas		**96**

4. ¿Qué servicios tecnológicos utiliza en el cómputo en la nube?

Como sabrá, hay diferentes posibilidades que pueden facilitar el desarrollo de su negocio, ya que permiten el uso de recursos tecnológicos según las necesidades que pueda tener en cada momento. Al respecto, por favor, responda si actualmente hace uso de alguno de los siguientes:

Opciones	Porcentaje	Cuenta
Correo electrónico	97,1%	203
CRM	31,1%	65
ERP	37,3%	78
Software de Diseño	33,0%	69
Office	85,6%	179
Reuniones	43,1%	90
Otros (por favor especificar)		9
	Respondidas	**209**
	No respondidas	**5**

5. ¿Sabe o ha calculado qué porcentaje de sus empleados utiliza dispositivos móviles para acceder a la información?

La nube ofrece a las empresas la posibilidad de hacer uso de recursos tecnológicos en cada momento en atención a las necesidades que pueda tener y, además, facilita que empleados o colaboradores puedan acceder a la información que necesitan desde cualquier lugar en cualquier momento. En este sentido, ¿sabe o ha calculado qué porcentaje de sus empleados o colaboradores utilizan dispositivos móviles (smartphones, tablets, etc.) para acceder a la información?

Opciones	**Porcentaje**	**Cuenta**
Sí, menos de un 10% utiliza dispositivos móviles para acceder a la información	8,9%	18
Sí, entre un 10% y un 25% utilizan dispositivos móviles para acceder a la información	8,4%	17
Sí, entre un 25% y un 50% utilizan dispositivos móviles para acceder a la información	8,9%	18
Sí, entre un 50% y un 75% utilizan dispositivos móviles para acceder a la información	7,4%	15
Sí, entre un 75% y un 100% utilizan dispositivos móviles para acceder a la información	23,6%	48
NO utilizan dispositivos móviles para acceder a la información empresarial por Riesgos legales en cuanto al uso de dispositivos móviles conforme a la normatividad sobre protección de datos personales	14,8%	30
NO utilizan dispositivos móviles para acceder a la información empresarial por Riesgos para poder garantizar la confidencialidad y seguridad de los datos personales	8,4%	17
NO conozco el porcentaje de uso	19,7%	40
NO usamos por la siguiente razón:		4
	Respondidas	**203**
	No respondidas	**11**

6. ¿Trata datos personales en la nube?

La información a la que acceden sus empleados o colaboradores a través de la nube, ¿hace referencia a sus clientes, prospectos, empleados u otras personas físicas? Es decir, ¿trata datos personales en la nube?

Opciones	Porcentaje	Cuenta
Si	39,6%	76
No, Los datos personales solo se manejan en los sistemas en sitio	32,3%	62
No, Mi empresa no trata datos personales en la nube, pero pensamos hacerlo	9,4%	18
No tratamos datos personales en la nube y no tenemos pensado hacerlo, porque: Pérdida de control sobre el tratamiento de los datos personales	1,6%	3
No tratamos datos personales en la nube y no tenemos pensado hacerlo, porque: Riesgos legales derivados de la normatividad sobre protección de datos personales	6,3%	12
No tratamos datos personales en la nube y no tenemos pensado hacerlo, porque: Riesgos en materia de medidas de seguridad	7,3%	14
No tratamos datos personales en la nube y no tenemos pensado hacerlo, porque: Riesgos en materia de confidencialidad	3,6%	7
No tratamos datos personales en la nube por la siguiente razón:		12
Respondidas		**192**
No respondidas		**22**

7. Si trata datos personales en la nube, ¿ha considerado aspectos para evitar riesgos o ha adoptado medidas para mitigarlos?

Si trata datos personales en la nube, ¿antes de hacerlo ha tomado en consideración los siguientes aspectos o ha adoptado las medidas que se indican a continuación?				
Opciones	**Sí**	**No**	**No sabe**	**Cuenta**
Análisis de los tipos de datos personales, distinguiendo entre datos personales y datos personales sensibles (religión; salud; afiliación sindical; opiniones políticas, etc.) a tratar en la nube.	55	42	48	145
Identificación de las bases de datos o tratamientos a llevar a cabo en la nube.	60	31	52	143
Análisis de riesgos para la privacidad y la protección de datos personales derivados del tratamiento en la nube.	82	21	41	144
Revisión de los requisitos normativos y contractuales a cumplir por el proveedor de servicios de cómputo en la nube.	73	29	43	145
Firma de un contrato con el proveedor de servicios de cómputo en la nube como encargado del tratamiento.	61	35	44	140
			Respondidas	**146**
			No respondidas	**68**

8. ¿Qué importancia tienen los aspectos que se indican para la adopción del cómputo en la nube?

En la adopción de servicios de cómputo en la nube ofrecidos por un proveedor, ¿cuál es la importancia que tienen para usted los siguientes aspectos?				
Opciones	**Baja**	**Media**	**Alta**	**Cuenta**
Cumplimiento de la normatividad sobre protección de datos personales.	9	21	163	193
Medidas de seguridad.	7	19	169	195
Certificaciones obtenidas (por ejemplo, ISO 27001).	24	44	122	190
Auditorías de terceros independientes.	37	48	98	183
Medidas adicionales y buenas prácticas sectoriales o industriales.	18	56	113	187
			Respondidas	**197**
			No respondidas	**17**

9. ¿Qué confianza le ofrecen los siguientes prestadores de servicios de cómputo en la nube?

¿Qué confianza le ofrecen los siguientes proveedores de servicios de cómputo en la nube? Si no conoce al proveedor, por favor, marque: No sé.						
Opciones	**No sé**	**Ninguna**	**Poca**	**Bastante**	**Mucha**	**Cuenta**
Amazon	107	13	28	23	30	201
Google	28	5	28	62	85	208
IBM	79	13	36	39	35	202
Microsoft	34	3	28	67	74	206
Rackspace	155	14	11	6	9	195
Oracle	93	9	22	34	47	205
VMware	139	7	19	17	17	199

Un Proveedor local	134	13	8	6	14	175
					Respondidas	**209**
					No respondidas	**5**

10. Si tuviera forma de asegurar o monitorizar su información en la nube, ¿haría más uso de ésta?

Si tuviera una forma de garantizar, asegurar o monitorizar su información en la nube y pudiese cumplir con las regulaciones y requisitos que le atañen, ¿haría un mayor uso del cómputo en la nube?

Opciones	**Porcentaje**	**Cuenta**
Sí, eso es importante para tomar ese paso;	51,0%	105
Sí, aunque no es algo que nos preocupe especialmente	24,8%	51
No, ya hacemos todo el uso de la nube que necesitamos y no vamos a hacer un mayor uso;	3,9%	8
No, el uso de la nube no nos preocupa de manera que nuestras decisiones no se basan en la confianza en aquélla;	7,8%	16
No, la nube no representa una necesidad y no estamos interesados.	12,6%	26
	Respondidas	**206**
	No respondidas	**8**

II. CUESTIONES GENERALES SOBRE EL CÓMPUTO EN LA NUBE

1. Introducción, concepto y clasificaciones en el cómputo en la nube

1.1. Introducción y concepto

Según el BSA (*Business Software Alliance*) *Global Cloud computing Scorecard* de 2012[5], México es el país de América Latina mejor posicionado para el desarrollo del *Cloud computing,* por delante de Argentina y Brasil. Para llegar a esa conclusión BSA analiza los siguientes parámetros[6]:

Privacidad: El éxito del cómputo en la nube depende en la fe que tienen los usuarios de que su información no será usada o divulgada, a pesar de que los proveedores estén en libertad para mover los datos a través de internet para maximizar los beneficios y ser más eficientes.

Seguridad: Los usuarios conocen a los proveedores de *cloud computing* y entienden los riesgos inherentes de gestionar, almacenar y ejecutar aplicaciones en la nube. Los proveedores de *cloud* están en capacidad de implementar soluciones de vanguardia en seguridad cibernética, sin necesidad de utilizar tecnologías específicas.

Ciberdelincuencia: Las leyes disuaden de forma significativa y toman medidas contra acciones ilegales. Los sistemas jurídicos deben proporcionar un mecanismo eficaz de aplicación de la ley, para luchar contra el acceso no autorizado a los datos almacenados en la nube.

Propiedad intelectual: Las leyes de propiedad intelectual prevén una protección clara y una aplicación estricta contra la apropiación indebida y violación de los acontecimientos que son la base de la nube.

---

[5] http://cloudscorecard.bsa.org/2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf

[6] Asi se expone en el documento citado en nota anterior. El resumen de tales criterios se ha tomado de http://empresas.it/2013/03/estos-son-los-mejores-y-los-peores-paises-para-el-computo-en-la-nube/#sthash.rjIo6VCg.dpuf

Portabilidad de los datos y la armonización de las normas internacionales: La fluidez de los datos en todo el mundo – como entre diferentes proveedores de la nube – requiere los esfuerzos para promover la apertura y la interoperabilidad. Los gobiernos trabajan con la industria para desarrollar estándares, así como para minimizar conflictos y obligaciones legales para los proveedores de la nube.

Libre comercio: Por su propia naturaleza, las tecnologías de cloud operan sin tener en cuenta fronteras nacionales. La capacidad de la nube para promover el crecimiento económico depende de un mercado mundial que trasciende las barreras al libre comercio, incluyendo las preferencias por determinados productos o proveedores.

Infraestructura de IT: Cloud computing requiere acceso ubicuo y robusto a banda ancha asequible. Esto se logra con políticas que incentiven la inversión privada en infraestructura de banda ancha y de leyes que promuevan el acceso universal a la banda ancha.

El “cómputo en la nube” es una forma de obtener servicios de cómputo por demanda. Cabe describirlo como un modelo de tecnología que mueve los servicios de computación (software, plataformas o infraestructura) de un medio tradicional (computadora personal) a Internet.

Su importancia es cada vez más notable en el marco de la economía global en que nos movemos y puede representar una oportunidad excepcional para el desarrollo de las empresas mexicanas a nivel nacional e internacional. Según un informe reciente de CISCO, el tráfico en la nube en Internet se va a multiplicar por 4 ó 5 entre 2012 y 2017. En general, se prevé que el tráfico en la nube crecerá en torno a un 35% anual hasta 2017. Y en ese año casi dos tercios de todos los datos serán procesados en centros de datos en la nube[7]

[7] *Cisco Global Cloud Index: Forecast and Methodology, 2012-2017*, 2013. Puede consultarse en http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.

La crisis económica ha despertado el interés de las empresas y los Gobiernos por la nube como un medio para reducir costes, pero éste no es su único atractivo, puesto que también ofrece un amplio abanico de posibilidades, algo de lo que los usuarios se están dando cuenta poco a poco[8].

La nube es cada vez más utilizada por grandes empresas, pero también resulta especialmente atractiva para las pymes y *start-ups*[9]. El principal motivo para ello es la reducción de costes, pero se prevé que los motivos cambien una vez superada la crisis[10].

Sin embargo, el *Cloud computing* no está limitado a las empresas. El gran tamaño, la complejidad y la gran expansión de los servicios de tecnología de los gobiernos hace que cada vez recurran más al cómputo en la nube, si bien la naturaleza de la información gestionada por las Administraciones es sin duda un obstáculo para su desarrollo.

En el ámbito de la protección de datos las cuestiones que plantea el cómputo en la nube son de una extraordinaria importancia, y de su observancia depende en gran medida su desarrollo futuro. La trascendencia de las cuestiones relacionadas con la protección de datos y el cómputo en la nube se ha puesto de manifiesto en el hecho de que ha merecido la atención de los más importantes actores de la protección de datos en México y a nivel internacional. Merece destacar, a título de ejemplo, la referencia expresa que le dedica el artículo 52 del Reglamento de desarrollo de la Ley Federal de Protección de Datos

---

[8] Cfr.: RAVENTOS, Laia. "El 21% de las pymes con web usa el Cloud computing". Diario El Pais. Tecnología 28 de mayo de 2012.
http://tecnologia.elpais.com/tecnologia/2012/05/28/actualidad/1338202811_741760.html

[9] El Cloud computing es la base de lo que The New York Times, llama "DIY (do it yourself). En septiembre de 2011, el Cloud computing ya permitió a los emprendedores e innovadores poner en marcha nuevas empresas con requerimientos mínimos de capital en Estados Unidos "El Cloud computing impulsará las próximas starups". Nubeit http://www.nubeit.es/el-cloud-computing-impulsara-la-proxima-generacion-de-startups/

[10] Cfr.: Cloud computing ofrece ventajas a las empresas pequeñas y medianas en términos de reducción de costos. "Usted paga por lo que usa". Así se determina en "10 Beneficios Clave de Cloud computing". En GBM Cloud. http://www.gbmcloud.com/blog/10-beneficios-clave-de-cloud-computing/

Personales en posesión de los Particulares, publicado en el Diario Oficial de 21 de diciembre de 2011 (RLFPDPPP).

En Europa está en fase de elaboración un nuevo Reglamento Europeo de Protección de Datos y el Parlamento Europeo ha propuesto la inclusión en su texto de una referencia expresa al hecho de que "*Amongst other technologies, cloud computing has the potential to transform the European economy, provided, that appropriate data safety and data protection measures are put in place. In order to ensure the highest level of safety of personal data, it is essential to understand rights and obligations of data controllers and data processors within this Regulation*[11]*".* El Grupo de Autoridades de Protección de Datos, llamado Grupo de Trabajo del Artículo 29, ha elaborado un interesante documento sobre *Cloud computing*[12], al que haremos referencia.

El citado artículo 52 del RLFPDPPP incluye una definición de cómputo en la nube: "*Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente".*

Es importante destacar que el Reglamento que acabamos de citar y en particular el art. 52, es pionero en la regulación del *cloud computing* y acierta a recoger las más importantes previsiones sobre el tema desde la perspectiva de la protección de datos de carácter personal.

La nube hace más eficiente el uso de tecnologías existentes y permite que quienes no podían utilizarlas, ahora tengan acceso a ellas. La gran ventaja de esta tecnología es que elimina las rigideces de los

[11] REPORT on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs, de 21 de noviembre de 2013, pág. 227.

[12] *Opinion 05/2012 on Cloud computing*, de 1 de julio de 2012, WP 196.

sistemas tradicionales de Tecnologías de Información (TI) al permitir aumentar los servicios contratados conforme a la demanda[13].

Según *The NIST Definition of Cloud computing*[14], las cinco características esenciales del "cómputo en la nube" son:

1. Autoservicio *on-demand* o pago por evento. Los servicios pueden ser solicitados por el usuario o el cliente a través de Internet o directamente, pagando únicamente por el tiempo de uso del servicio.
2. Acceso ubicuo a la red (uso de los servicios cuando sea y donde sea). Los servicios en la nube son accesibles desde cualquier medio (computadora, teléfono, etc.) con acceso a la red.
3. Fondo común de recursos. Los servicios en la nube pueden ser usados por distintos usuarios en diferentes lugares del mundo. Esto crea una independencia de la ubicación de los recursos al aprovechar el Internet.
4. Rápida elasticidad. La cantidad o calidad de los servicios ofrecidos en la nube puede aumentar o disminuir como le convenga al usuario sin necesidad de hacer colas o trámites para solicitarlos.
5. Servicio medido. Cada recurso que consume el usuario y que es facturable debe ser medido, no sólo para fines de tarificación, sino también de control. Este servicio puede ser vendido al mismo usuario o cliente dentro de su contexto y/o ambiente.

1.2. Las categorías de Ofertas de Servicios de "Cloud Computing"

Las ofertas principales de "Cloud Computing" se pueden agrupar de acuerdo con las siguientes categorías:

---

[13] Cfr.: "Computo en la nube: Nuevo detonador para la competitividad en México". Microsoft. IMC e Instituto Mexicano para la Competitividad A.C. http://imco.org.mx/wpcontent/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

[14] Peter Mell & Timothy Grance, *The NIST Definition of Cloud computing*, NIST Special Publication 800-145, septiembre 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

1.2.1. Infraestructura como servicio ("*Infrastructure-as-a-service*". *IaaS*)

Nos referimos a los servicios de "Cloud Computing" por los que se ponen a disposición de los usuarios los recursos informáticos de carácter básico -tales como almacenamiento, espacio en disco y servidores- como servicios bajo demanda. En lugar de proceder a la utilización de máquinas físicas los clientes, en este caso, tienen la posibilidad de acceder a los servidores virtuales donde despliegan su propio software, generalmente a partir del sistema operativo.

Esta categoría ofrece ahorros de costes y reducción de riesgos, eliminando los sustanciales gastos de capital necesarios para desplegar una infraestructura o aplicaciones a gran escala de forma interna. Los proveedores de "Cloud Computing" generalmente ofrecen un modelo de negocio de pago por uso que permite a las compañías escalar según sus necesidades en tiempo real, en lugar de pagar por adelantado una infraestructura que puede no ser utilizada, o tener un exceso recursos para hacer frente a picos ocasionales de la demanda.

1.2.2. Plataforma como servicio ("*Platform-as-a-service*". *PaaS*)

Esta categoría ha encontrado un rápido crecimiento entre las ofertas que se producen de "Cloud Computing", ya que permite un fácil desarrollo y despliegue de aplicaciones Web escalables, sin necesidad de proceder a invertir, o gestionar, una infraestructura subyacente.

Las principales características asociadas al "*Platform as a Service"* son:

a) Facilita el despliegue de las aplicaciones del cliente, sin el coste y la complejidad derivados de la compra y gestión del hardware y de las capas de software asociadas.

b) Ofrece a través de redes de servicio IP todos los requisitos necesarios para crear y entregar servicios y aplicaciones web.

1.2.3. Software como servicio ("*Software-as-a-service*". *SaaS*)

Se trata de las ofertas de "Cloud Computing" más adaptadas a las necesidades de la empresa, ya permiten desplegar, gestionar y entregar aplicaciones completas de usuario final en la Web.

Los proveedores de los servicios "SaaS" pueden tener instalada la aplicación en sus propios servidores web (permitiendo a los clientes acceder, por ejemplo, mediante un navegador web), o descargar el software en los sistemas del contratante del servicio.

Esta categoría sigue el paradigma propio de "Cloud Computing" de sistemas de bajo coste, que se ajusta plenamente a las necesidades de cada empresa, y determina los modelos a seguir bajo demanda. La velocidad y facilidad con la que se pueden adquirir y consumir las aplicaciones han convertido a esta categoría de ofertas de "Cloud Computing" en la más solicitada y adoptada en la actualidad.

1.2.4. "Business Process as a Service" ("BPaaS")

Se trata de una categoría relativamente reciente que consiste primordialmente en la provisión como servicio de procesos de negocio "*end-to-end"* altamente estandarizados a través de su entrega dinámica, la modalidad de pago por uso y los modelos de consumo de autoservicio bajo demanda. Su característica principal es que los recursos utilizados mediante esta solución que sirven para ejecutar los procesos de negocio son compartidos entre los diferentes clientes del proveedor. En muchos casos, este hecho proporciona un aporte de valor al negocio; sin embargo, la solución "BPaaS" se encuentra en una fase incipiente, siendo todavía un modelo de negocio en el que los proveedores tan solo operan en la actualidad en nichos concretos, y que obviamente queda condicionado a su ulterior desarrollo.

1.3. Clases de nubes: las nubes públicas, privadas, híbridas y comunitarias

1.3.1. Las nubes públicas

En este caso, como señala *The NIST Definition of Cloud computing*, la infraestructura en la nube está preparada para el uso abierto al público en general. Puede ser en propiedad, administrado y operado por una empresa, organización académica, o el gobierno. Permite que múltiples usuarios puedan utilizar servicios procesados en el mismo servidor.

Como características[15] inherentes a esta forma de implementación, podemos citar:

a) Reducido plazo de tiempo para la disponibilidad del servicio.
b) No se requiere llevar a cabo inversión monetaria para su implementación.
c) Permite la externalización a un proveedor de servicios Cloud de todas las funciones básicas de la empresa.
d) Posibilita el aprovechamiento de la infraestructura de los proveedores de servicios, permitiendo adicionalmente una alta escalabilidad y flexibilidad en la modificación del dimensionamiento del servicio.
e) Favorece la utilización de conjuntos de software estándar.
f) Lleva asociadas unas cuotas iniciales de pago más bajas que el resto de implementaciones. Adicionalmente los costes del Cloud público son variables, cumpliendo el principio de pago por uso.
g) La información corporativa se encuentra alojada en la nube pública junto a la del resto de clientes del proveedor, lo que implica, además de no poder tener localizada físicamente dicha información, imponer al proveedor una serie de requisitos de alta exigencia en temas de seguridad y protección de datos.

[15] Vid. "Principales formas de implementación del Cloud Computing", en *"Cloud Computing. Retos y Oportunidades"*. Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información. Ministerio de Industria, Energía y Turismo. Gobierno de España. Mayo de 2.012.

El mayor reto sobre seguridad surge a la hora de usar *Clouds* públicos, ya que los datos y las aplicaciones se encuentran en un entorno controlado por un tercero, y compartido con otras empresas. En estos casos, como en otras muchas situaciones, la clave está en la solvencia que ofrezca el proveedor ya que los *Clouds* públicos actúan como una prolongación de la plataforma tecnológica que la que opera la empresa. En este aspecto, resulta necesario evaluar las credenciales de seguridad del proveedor de servicios de "Cloud Computing", y conocer qué estándares sigue, y a que revisiones externas se somete.

Es importante contar con un proveedor que no sólo cumpla con el entorno legislativo vigente en materia de protección de datos de carácter personal, sino que cuente con controles rigurosos para salvaguardar la confidencialidad y la seguridad de la información[16].

1.3.2. Las nubes privadas

En este caso la infraestructura en la nube está preparada para el uso exclusivo de una sola organización que comprende varios consumidores (por ejemplo, unidades de negocio)[17]. Puede ser de propiedad, administrado y operado por la organización, un tercero, o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

Como características propias de la nube privada cabe citar[18]:

a) Reducido plazo de tiempo para la puesta en servicio y una alta flexibilidad en la asignación de recursos.
b) Al contrario que el Cloud Público, requiere de inversión económica para la implementación de la solución contratada.
c) Lleva asociados sistemas y bases de datos locales.

---

[16]Vid. http://itcio.es/Cloud -computing/análisis/1005069022902/ seguridad-entornos-Cloud -computing/

[17] *The NIST Definition of Cloud computing*

[18] Vid. "Principales formas de implementación del Cloud Computing", en "Cloud Computing. Retos y Oportunidades". Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información. Ministerio de Industria, Energía y Turismo. Gobierno de España. Mayo de 2.012.

d) Ofrece la posibilidad de aprovechar el personal existente, y las inversiones en sistemas de información realizadas con anterioridad.
e) Implica más especificidad en la solución adquirida, ya que está diseñada para ajustarse a las necesidades propias de la empresa contratante.
f) Permite disponer de un control total de la infraestructura, de los sistemas y de la información corporativa tratada por éstos.
g) Facilita el control y la supervisión de los requisitos de seguridad y protección de la información almacenada

Las nubes privadas requieren grandes costes iniciales de desarrollo, mantenimiento continuo y conocimiento interno, y en consecuencia, ofrece un perfil de beneficio muy distinto en comparación con las nubes de carácter público. Esta tipología de nube, puede constituir el primer paso lógico para muchas organizaciones, que realizan un desembolso en hardware y quieren aprovecharlo.

Las nubes privadas son muy adecuadas para flujos de trabajo de misión crítica que requieren altos niveles de seguridad y disponibilidad, así como para aplicaciones que por razón de cumplimento normativo exigen un mayor grado de control de la propiedad de los datos.

1.3.3. Las nubes comunitarias

Se caracterizan por estar compartidas entre varias organizaciones que forman una comunidad con principios similares, entre los que se suele mencionar: la visión, los requerimientos de seguridad, las políticas y cumplimientos normativos, etc. Se trata de Clouds utilizados por distintas organizaciones cuyas funciones y servicios sean comunes, permitiendo con ello la colaboración entre grupos de interés.

En general, el conjunto de recursos disponibles en una nube comunitaria es mayor que en la privado, con las ventajas evidentes que ello conlleva en términos de elasticidad. Sin embargo, la cantidad de recursos es menor que los existentes en una solución de Cloud público.

Por otra parte, el número de usuarios de este tipo de nube es menor que los de la nube pública, lo que la dota de mayores prestaciones en cuestiones de seguridad y privacidad. La nube comunitaria se caracteriza por poder estar gestionada por la propia comunidad que la integra, o bien, por un tercero designado de común acuerdo por los partícipes[19]. Estaría constituida, por tanto, por un conjunto de servicios ofrecidos por un proveedor a un grupo de clientes que presenten afinidades entre sí. Por ello, se puede considerar que la nube comunitaria constituye básicamente una variante más de la nube de carácter privado a la que ya se ha hecho referencia con anterioridad en estas notas.

1.3.4. Las nubes híbridas

Se caracterizan por aunar dos o más formas de Clouds (privado, comunitario o público), los cuáles continúan siendo entidades únicas interconectadas mediante tecnología estandarizada o propietaria, tecnología que permite la portabilidad de datos y aplicaciones (ej. el rebalanceo de cargas entre nubes). Debe tenerse presente que una entidad que emplee esta forma de implementación se podría beneficiar de las ventajas asociadas a cada tipo de Cloud, (público, privado, etc.), con lo que dicho modelo podría salir reforzado.

2.- El cómputo en la nube como servicio de comunicaciones electrónicas y de la sociedad de la información

Los datos son un activo empresarial. De hecho, los objetivos estratégicos que tienen las empresas son cada vez más complicados y necesitan más datos para ser alcanzados. Esta realidad tiene su reflejo en el crecimiento exponencial del volumen de información con que se cuenta, lo que supone que cada vez sea más complicado gestionar esos datos. Hasta ahora era posible llevar a cabo esta gestión de

[19] Vid. INTECO. Instituto Nacional de Tecnologías de la Comunicación. Observatorio de la Seguridad de la Información. Ministerio de Industria, Energía y Turismo. Gobierno de España. "Guía para empresas: seguridad y privacidad del 'Cloud Computing'". Octubre de 2011.

manera sencilla, pero ahora las organizaciones empresariales se ven obligadas a prestar especial atención a los datos por si mismos para poder dar respuesta a las necesidades del negocio[20].

En el marco de la revolución tecnológica las empresas y los mercados, independientemente del sector en el que actúen, se han convertido, en gran medida, en procesadores de información y generadores de nuevo conocimiento.

En este sentido, los avances en las Tecnologías de la Información y la Comunicación (TIC) han sido capaces de reestructurar las relaciones existentes hasta la fecha entre el tiempo y el espacio, y se han convertido en el centro neurálgico del proceso de globalización. El ejemplo paradigmático de este proceso es la red Internet. Su expansión vertiginosa ha permitido a la economía funcionar como una unidad en tiempo real, y ha conformada una economía global que viene definida, principalmente, por los flujos de capitales, personas e información, en los cuales las fronteras espaciales han dejado de tener la importancia de antaño.

Construir una estructura Cloud requiere inversión (CAPEX)[21]. Hardware, software, servicios, aplicaciones, licencias, procesos, redes, conectividad; todo ello necesita de planificación e inversión. El suministro de servicios Cloud[22] requiere de una conectividad fiable y de

---

[20] Cfr.: "Data Management. La gestión de datos eficaz", en *PowerData*. http://www.powerdata.es/index.php/cl/

[21]Vid.: INTERXION. "Ninguna nube es una isla. Las nubes híbridas ofrecen nuevas oportunidades de negocio". Cfr.:http://www.interxion.com/es/sectores/Cloud /no-Cloud -is-an-island/

[22] Ya en 1960 se introdujeron conceptos de Cloud Computing por John McCarthy, quien dijo en un discurso que "Algún día la computación podrá ser organizada como un servicio público" y haciendo una comparación con lo ocurrido en la distribución eléctrica a comienzos del siglo XX donde las grandes empresas tenían su propio generador de energía, ahora las empresas grandes constan de sus servidores, clúster o supercomputadoras. Cfr.: CRUZ VALENCIA, Katherin. Historia Del Cloud Computing. *Revista de Información, Tecnología y Sociedad. RITS* [online]. 2012, número 7. http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442012000200021&script=sci_abstract. El Cloud Computing posibilita el *outsourcing* de la computación y servicios sin externalizar su control y se basa en utilizar un modelo de pago por uso, con acceso Web a Internet con banda ancha. La industria del Cloud Computing representa un gran ecosistema con muchos modelos, fabricantes y nichos de mercado. Actualmente se percibe como la necesidad más urgente del paradigma en evolución Cloud Computing la protección desde sus dos perspectivas de su seguridad y privacidad. La protección es el tema capital que exige una solución

última generación. Una aplicación fiable y sin interrupciones y un servicio entre nube privada y pública requieren de una arquitectura orientada a servicio. Con sistemas cada vez más heterogéneos, se hace imprescindible un único criterio para organizar y medir tanto los entornos Cloud internos como externos.[23] Con esta visión del futuro, los líderes de TI pasarán a ser agentes y mediadores. El reto será la interacción entre servicios dispares basados en la nube y los sistemas internos, la conexión de peticiones de servicios con el proveedor de servicio más adecuado y la entrega de servicio.

Como ha quedado ya apuntado, el "Cloud Computing" constituye un modelo de consumo y servicio en el que se paga según su uso y que permite la aportación, en tiempo real, de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones o servicios)[24]. Lo habitual es que sean recursos muy "escalables" en el sentido de adaptable, y que a través de Internet pueden adquirir muy diversas compañías, que sólo pagan por aquello que utilizan. Los modelos de trabajo "Cloud Computing" pueden ayudar a las organizaciones a "escalar" sus inversiones a medida que crecen sus negocios. También pueden" abrir la puerta" a nuevos enfoques de negocio a través de aplicaciones, infraestructuras, entornos de pruebas y procesos de negocio estandarizados que ayuden a mejorar la prestación y la eficacia de los servicios.

El término "Cloud Computing" significa y supone un trascendente cambio en la forma con la que se trabaja con el software. Exige un cambio de paradigma, por lo que procede introducir profundas modificaciones en el modelo actual de la computación en la Red. Hoy en día, por computación en nube o "Cloud computing" debemos

---

urgente. AREITIO BERTOLIN, Javier. "Protección del Cloud Computing en seguridad y privacidad". *Revista española de electrónica,* Nº 666, 2010.
http://dialnet.unirioja.es/servlet/articulo?codigo=3217380

[23] Con relación a los usuarios de la red el Cloud Computing tiene muchos puntos de conexión con la Web 2.0 y para las empresas está estrechamente relacionado con los procesos de *outsourcing* de los servicios TIC. MARTIN MIRALLES LOEZ, Ramón. *IDP: revista de Internet, derecho y política = revista d'Internet, dret i política*, Nº. 11, 2010 (Ejemplar dedicado a: Cloud Computing: el derecho y la política suben a la nube). 2010. http://dialnet.unirioja.es/servlet/articulo?codigo=3424002

[24] http://www.satec.es/es-ES/NuestraActividad/Soluciones/Paginas/Soluciones%20Cloud%20Computing.aspx

considerar, fundamentalmente, una modalidad de prestación de servicios de la sociedad de la información, tipo “self-service” y bajo demanda del cliente, a cuya disposición se pone un conjunto de recursos virtuales, y masivamente “escalables”, altamente elásticos en función de sus necesidades y, en su caso de pago por uso[25].

Todo esto, en la práctica, significa que la información que manejamos para trabajar está alojada en el equipo informático y que, sin embargo, ese mismo equipo se configura como una mera ventana de acceso a los datos y programas. La mayoría de las grandes empresas (Microsoft, Google, Amazon, etc.) han incorporado esta filosofía de trabajo a todos sus ámbitos, poniendo a disposición de los usuarios un determinado espacio en sus "nubes particulares” que cualquiera puede usar, a modo de disco duro virtual, con acceso desde Internet y, además, debe tenerse en cuenta que hay cada vez más herramientas a nuestra disposición (Dropbox, Box, Drive, etc.) y todas ellas, cada vez más integradas.

La combinación del trabajo y la nube con las tecnologías de la comunicación establecida ostenta cada vez un papel más importante en nuestra vida, supone una nueva forma de organización que, bien gestionada, multiplica la eficiencia de muchas actividades empresariales[26]. El esquema del *Cloud computing* (donde existe y se hace una analogía de identidad de la nube con Internet) está basado en que con los avances en tecnología, arquitectura, y diseño del software, y de las aplicaciones que actualmente se utilizan en un PC se encuentran, al mismo tiempo, a disposición del usuario en Internet, sin tener que recurrir, por el contrario, al disco duro de un PC o a un servidor de carácter tradicional.

---

[25] Cfr. DE LA TORRE LLORENTE, Carlos. "La nube en la Industria” en P. GARCÍA MEXÍA. Jornada “Internet y los servicios en la nube: retos y oportunidades para la empresa y la Administración”. Santiago de Compostela 14 diciembre, 2.009. http://www.egap.xunta.es/detalleRecurso.php?id=358

[26] Vid.: en http://blog.cinde.es/?p=291. En parecidos términos se pronuncia la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el “Aprovechamiento del potencial de la informática de la nube en Europa”. Septiembre de 2012.

En este sentido, el cómputo en la nube constituye un claro exponente de una tendencia de fondo del sector de las Tecnologías de la Información y la Comunicación, un verdadero desplazamiento de paradigma del objeto al servicio, que está cambiado la forma del desarrollo, del despliegue y de la utilización de los ordenadores. Esta forma de reorganizar las aplicaciones de software en un conjunto de servicios, que interactúan entre sí, es lo que normalmente se conoce como arquitectura orientada al servicio ("SOA"). Consecuentemente con ello los servicios serán lo verdaderamente importante para el usuario, y no el software específico, ni tampoco el utilizado para implementar dichos servicios de hardware[27].

Debe tenerse presente que con el impacto actual del *Cloud computing* en el acceso y almacenamiento de datos, los puestos de trabajo también están experimentando una especie de metamorfosis de las empresas que se mueven hacia la nube[28]. Este cambio no sólo afecta a la transformación de los departamentos TI, sino también al resto de la compañía. Con el *Cloud Computing*, los directores informáticos pueden centrarse en la creación de estrategias de negocio, en lugar de dedicar su tiempo a arreglar los problemas de TI. En la actualidad existe una creciente demanda de *Cloud strategy consultants, Cloud architects*, y *Cloud service planners*. También se necesitarán otros profesionales de la nube como *Cloud product manager, Cloud network engineer, Cloud systems engineer, Cloud consultant, Cloud systems administrator, Cloud developer, Cloud engineer, Cloud sales executive*, y *Cloud software engineer*.

Algunos analistas prefieren dividir la definición sobre el *Cloud computing* en dos partes bien diferenciadas:

---

[27] Vid. COSTILLA, Carmen." Exposición técnica de la Universidad", en Foro sobre Cloud Computing: La nueva ola de computación capaz de transformar una buena parte de las Tecnologías de la Información. Madrid, 15-4-2010.
http://etsit.upm.es/fileadmin/documentos/noticias/noticias2010/150410_c/artelCloud .bmp

[28] Revista *Cloud Computing*. Habilidades necesarias para trabajar en la nube. 19 de febrero de 2013. http://www.revistaCloud Computing.com/2013/02/habilidades-necesarias-para-trabajar-en-la-nube/#sthash.fO2tWoLK.dpuf. http://tratecnosl.wordpress.com/2013/02/21/habilidades-necesarias-para-trabajar-en-la-nube/#more-611.

a) Por un lado, hacen referencia a los servicios en la nube como "*productos, servicios y soluciones de consumo y empresariales que se ofrecen y consumen en tiempo real por Internet*", y;
b) Por otro, definen la informática en la nube como "*un modelo emergente de desarrollo, implementación y prestación de tecnologías de la información que permite la entrega en tiempo real de productos, servicios y soluciones por Internet, (es decir, facilita los servicios de la nube)*".

Al analizar estas definiciones, se hace patente de inmediato que el cómputo en la nube no se refiere a una tecnología específica, sino una manera general de implementar la tecnología para dirigir un negocio[29]. La opción del *Cloud computing* está cobrando mayor peso como una vía para reducir y eliminar los gastos de capital por parte de las empresas. Inmersos en una dura recesión económica en la que la reducción de costes es el principio de gestión imperante, la posibilidad de disponer de recursos informáticos pagando únicamente por lo que se necesita es una proposición de valor bastante atractiva.

Además, supone una alternativa a la compra de licencias de software cada vez más caras y una reducción significativa en los costes de personal. A su vez, dentro del contexto del mundo globalizado, las empresas operan de forma cada vez menos aislada y más integradas con sus clientes y proveedores. Por ello, deben estar más preparadas para responder con rapidez a los cambios que este alto grado de interacción presenta. Las aplicaciones basadas en Internet suponen una alternativa a las aplicaciones internas porque facilitan la colaboración necesaria y son accesibles desde cualquier lugar.

Más aún, el despegue de algunas tendencias económicas y tecnológicas casi siempre guarda estrecha relación con las iniciativas que lleve a cabo el Gobierno de un país. En este caso, se presenta la llamada “g-Cloud” (“Government Cloud”) como prioridad estratégica

[29]Vid. INTECO. Instituto Nacional de Tecnologías de la Comunicación. Observatorio de la Seguridad de la Información. Ministerio de Industria, Turismo y Comercio. Gobierno de España. "Guía para empresas: seguridad y privacidad del ‘Cloud Computing’". Octubre de 2011, obra citada.

para países como Reino Unido o Japón. El papel del sector público no se reduce únicamente a establecer un marco regulatorio para la actividad, sino también a actuar como un consumidor de *Cloud computing* en sí mismo, dada su necesidad de productos y servicios de tecnologías de la información y la comunicación en áreas como educación, sanidad o defensa. Los Gobiernos tendrán así nuevas formas de interactuar con los ciudadanos, ofrecer servicios públicos y compartir información.

La extensión de una tendencia también se suele confirmar cuando empieza a aparecer en los temarios del ámbito académico. En este caso, Facebook anunció la creación de un programa de becas para apoyar a los estudiantes de postgrado en el año escolar 2010-2011 en áreas de estudio como el *Cloud computing*, sistemas escalables y centros de datos eficientes, o recuperación de información[30]. Asimismo, universidades de la talla de Harvard están incluyendo cursos específicos de *Cloud Computing* dentro de su oferta educativa[31], o bien ofrecen un importante contenido de materias relacionadas con el *Cloud computing* en estudios de posgrado, como ocurre con el Master en Protección de Datos, Transparencia y Acceso a la Información de la Universidad CEU-San Pablo de Madrid[32].

También ha de considerarse que, es el momento del "Cloud Computing" desde el punto de vista medioambiental. El cambio climático es una de las cuestiones más candentes y con más presencia en los medios de comunicación, por lo que una reducción en el coste de la energía y en el impacto medioambiental también sería considerada muy positivamente frente a las presiones por implantar políticas «verdes» en las empresas y en la gestión de los Gobiernos. El "Cloud Computing" se establece como modelo de TI sostenible dado que el consumo energético es más eficiente en los centros de procesamiento y almacenamiento compartidos frente al de los individuales de las empresas.

[30]Vid.:http://maestriaicni.blogspot.com/2010/01/facebook-ofrece-becasestudiantes-de.html.
[31]Vid.:http://www.extension.harvard.edu/ courses/csci.jsp#e-175.
[32] http://www.postgrado.uspceu.es/pages/proteccion_datos/presentacion.html?ID_M=84

En definitiva, como si de una tormenta perfecta se tratara, el "Cloud Computing" parece surgir y alimentarse de la convergencia de distintos elementos determinantes del momento que vivimos. Algunas voces apuntan a que esta «tormenta perfecta» no solo provocará un cambio disruptivo en la industria de TI sino que también alterará la manera en que la gente trabaja y las empresas operan[33].

No obstante lo anterior, existe la creencia generalizada de que la prestación de servicios de cómputo en la nube, que supondrá por regle general el tratamiento de un número importante de datos por parte de un proveedor de servicios externo crearía dudas sobre la seguridad. Gartner[34] estima que el mercado de la seguridad en la nube es uno de los que más van a crecer más en los próximos años. Según el informe de Gartner, el mercado de la seguridad basada en la nube llegará a 2,1 mil millones dólares de valor global de este año y se elevará a 3,1 millones en 2015.

Los problemas de privacidad son un factor importante que condiciona la aplicación de todas las formas de servicios basados en la nube. Esto es especialmente cierto en los países y regiones con requisitos regulatorios rígidos. Para el usuario de esta técnica, estos problemas de seguridad se transforman en las limitaciones que esta clase de servicio ofrecerá y los condicionamientos que ello llevará consigo con relación a las garantías de la privacidad de los datos y de la información con la que está trabajando.

Por otro lado, hay que reconocer que en algunos casos estamos tratando con tecnologías incipientes que, muchas veces, fallan en un mal momento, principalmente por su falta de desarrollo. Además, los centros de datos actuales no siempre tienen suficiente capacidad para hacer frente a las inmensas cargas de trabajo que la multiplicación de los datos estructurados y no estructurados provoca en las organizaciones. Y la política de seguir añadiendo servidores y sistemas de almacenamiento a los CPD's no hace más que añadir complejidad a

[33]Vid.:http://www.economist.com/specialreports/displaystory.cfm? story_id=E1_TNQTTRRN.

[34] KAR, Saroj, "Gartner ve la nube mercado de la seguridad es un valor de $ 3,1 mil millones en 2015", en Cloud Times, 8 de noviembre de 2013. http://Cloud times.org/2013/11/08/gartner-sees-Cloud -security-market-is-worth-3-1-billion-by-2015/

un entorno cada vez más difícil de gestionar. La clave está en conseguir un doble objetivo: reducir los costes y, al tiempo que se mantienen los sistemas de negocio funcionando, conseguir liberar recursos para proyectos de innovación. Esto supondrá no sólo mejoras en la velocidad de las transacciones, sino también ahorro de costes energéticos, de instalación, de gestión y de mantenimiento.

3. El artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

A la hora de analizar el Cloud Computing se hace necesario partir del reconocimiento del derecho a la protección de los datos de carácter personal. Este derecho viene reconocido en el artículo 16 Constitucional, que dispone:

> *Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros*[35]*.*

Dicho artículo ha sido desarrollado por la Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPPP) de 2010 y en su Reglamento (RLFPDPPP)[36]. Esta regulación normativa se

[35] Véase el Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación de 1 de Junio de 2009. La normativa sobre protección de datos mexicana puede consultarse en José Luis PIÑAR MAÑAS y Miguel RECIO, *Código de Protección de datos. México*, Tirant Lo Blanch, México, 2013.

[36] Sobre ello vid. José Luis PIÑAR MAÑAS y Lina ORNELAS NUÑEZ (Coordinadores), *La Protección de datos personales en México*, Tirant Lo Blanch, México, 2013.

sitúa entre las más relevantes dentro del Derecho comparado y en particular en la Región Iberoamericana, así como en la Región APEC.

Debemos partir en esta Sección del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que vamos a comentar. En particular es esencial el artículo 52 del Reglamento, cuyo texto es el siguiente:

> ***Artículo 52**. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:*
>
> *I. Cumpla, al menos, con lo siguiente:*
>
> *a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;*
>
> *b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;*
>
> *c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y*
>
> *d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y*
>
> *II. Cuente con mecanismos, al menos, para:*
>
> *a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;*
>
> *b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;*
>
> *c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;*
>
> *d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y*
>
> *e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea*

a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

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

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

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

La prestación de servicios de *cloud* requiere de la celebración de un contrato entre quien presta el servicio (la empresa de *cloud,* que a efectos de la protección de datos tiene la consideración de encargado) y quien lo demanda (el usuario, que a efectos de la protección de datos, tiene la consideración de responsable). En este sentido, el artículo 51 del Reglamento señala que "*La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido".*

Tal contrato puede ser un contrato libremente redactado y pactado entre las partes, de modo que se adapte en particular a las exigencias y necesidades del usuario, o bien puede ser un contrato de adhesión. El artículo 52 se refiere a este segundo supuesto, si bien sus previsiones pueden y deben servir de guía o indicador para cualquier contrato de cómputo en la nube.

Es pues imprescindible, para cualquier empresa que pretenda contratar servicios de cómputo en la nube, tener en cuenta las previsiones del artículo 52, que son las que garantizan el

cumplimiento de las exigencias que en materia de protección de datos contienen tanto la LFPDPPP como su Reglamento.

Centrándonos en particular en el contrato de adhesión, éste es un tipo de contrato cuyas cláusulas son redactadas por una sola de las partes, con lo cual la otra se limita en principio a aceptar o rechazar el contrato en su integridad.

Los contratos de adhesión se basan por regla general en la existencia de formularios contractuales que el usuario o consumidor firma una vez cumplimentado con sus datos identificativos.

Es pues fácil adivinar que el principal problema que plantean los contratos de adhesión y en el ámbito de las cláusulas generales de contratación es el relativo a la validez del consentimiento y la posibilidad de que en ellos se incorporen cláusulas que podrían considerarse abusivas, lo que afectaría a la propia validez del contrato. Para evitar tales situaciones los poderes públicos (el legislador o el legislador secundario) pueden establecer criterios o requisitos que deben respetar los contratos para su validez. Este es el objetivo del artículo 52 del RLFPDPPP, que establece los requisitos que deben cumplir los proveedores de servicios de cómputo en la nube y que deben establecerse en los contratos de adhesión o en las condiciones generales de los contratos que vayan a celebrarse.

El Reglamento en efecto exige que el proveedor del servicio de cómputo en la nube:

I.- Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;

En este sentido deben tenerse en cuenta el Capítulo II de la Ley Federal de Protección de Datos Personales en Posesión de los

Particulares (artículos 6 a 21) y el Capítulo II (artículos 9 a 56) del Reglamento.

El artículo 6 de la Ley dispone que "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley". Por su parte el artículo 9 del Reglamento reitera tales principios y añade que el responsable, asimismo, debe observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley.

En esta primera fase del presente Estudio sobre "Definición y Cuestiones Generales sobre el Cómputo en la Nube" no parece oportuno llevar a cabo un análisis pormenorizado de los principios de la protección de datos que definen la Ley y el Reglamento, pero sí es necesario advertir que el artículo 52 del Reglamento lo que prevé es que el proveedor de servicios de cómputo en la nube debe aplicar "políticas de protección de datos *afines* a los principios y deberes aplicables". Es decir, el Reglamento es consciente de que el proveedor puede estar radicado fuera de México e incluso no estar sujeto a la legislación mexicana de protección de datos (no olvidemos que estamos hablando de contratos de adhesión) por lo que en lugar de exigirle cumplir específicamente con la Ley y el Reglamento, permite, desde un planteamiento más flexible pero no por ello menos garantista para la protección de datos, que tales principios y deberes sean "afines" a los que la normatividad exige[37].

Sí es necesario, sin embargo, hacer una referencia específica al principio de "responsabilidad", al que se refieren los artículos 47 y 48 del Reglamento en los siguientes términos:

[37] Sobre los principios de la LFPDPPP véase José Luis PIÑAR y Lina ORNELAS "Los principios de la protección de datos personales", en José Luis PIÑAR y Lina ORNELAS (Directores), *La protección de datos personales en México*, Tirant Lo Blanch Monografías, México D.F., 2013, págs. 39 a 96.

Principio de responsabilidad. Artículo 47.

En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.
Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

Medidas para el principio de responsabilidad. Artículo 48.

En términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.
Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:
I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;
II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;
III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;
IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad;
V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;
VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;

VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;
VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;
IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o
X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

Hacemos mención especial a dicho principio por cuanto se enumeran una serie de medidas muy significas que deben ser tenidas en cuenta para facilitar el cumplimiento de las previsiones de la normatividad sobre protección de datos por parte de cualquier proveedor de servicios de cómputo en la nube en México.

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

Una de las cuestiones más importantes en materia de contratación de servicios de cómputo en la nube es la de la necesidad de definir con claridad los sujetos participantes en la prestación del servicio. El contrato (sobre todo en casos de contratos de adhesión, como los que preocupan al legislador en el artículo 52 del Reglamento) se presta con una empresa proveedora, pero es muy usual que ésta, a su vez, subcontrate alguno de los servicios prestaos. Esta situación es especialmente relevante en materia de protección de datos pues el subcontratante que en su caso actúe tendrá sin duda acceso a datos personales y deberá hacerlo con todas las garantías y cautelas que la normatividad requiere.

Más adelante en este mismo estudio nos ocupamos con más detalle de las partes del contrato de cómputo en la nube y en particular nos referiremos a los posibles subcontratantes, pero es importante resaltar desde este momento la exigencia del artículo 52 del Reglamento, en el sentido de transparentar las subcontrataciones, lo que redunda en una mayor garantía para el usuario de los servicios de *cloud* y para el adecuado tratamiento de datos que el contrato de cómputo en la nube requiere.

Dicho lo anterior, no queda claro en el Reglamento hasta qué punto es necesario transparentar las subcontrataciones. Entendemos que será necesario al menos:

- Especificar en el contrato los servicios que pueden ser objeto de subcontratación.
- Identificar la empresa con la que se va a subcontratar.
- Garantizar que las empresas subcontratadas cumplen con las previsiones de la normatividad sobre protección de datos.

Asimismo debemos destacar lo que establecen los artículos 53 y 54 del Reglamento:

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

Autorización de la subcontratación. Artículo 55.

Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el artículo anterior se entenderá como otorgada a través de lo estipulado en éstos.

En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos a los que refiere el párrafo anterior, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

En ambos casos, se deberá observar lo previsto en el artículo anterior.

Asimismo debe tenerse en cuenta que el artículo 50.VI del Reglamento establece que el encargado del tratamiento (el proveedor de servicios de *cloud* deberá "*Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente".*

Deberá entenderse que los anteriores artículos, en lo que ahora nos afecta, se cumplen al firmar el contrato de cómputo en la nube siempre que se den las exigencias de transparencia que hemos apuntado.

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.

Se trata de una previsión lógica derivada del hecho de que el titular de los datos es siempre el interesado y nunca el responsable o el encargado de las bases de datos o tratamientos. El proveedor de servicios de *cloud computing* nunca puede pretender ostentar la titularidad de la información personal que someta a tratamiento.

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Es asimismo una consecuencia lógica de la regulación de las obligaciones de los responsables y encargados de bases de datos y tratamientos. El artículo 21 de la LFPDPPP dispone que "El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable". Por su parte, el artículo 50.IV del Reglamento obliga al encargado del tratamiento a "Guardar confidencialidad respecto de los datos personales tratados".

Por otra parte, el artículo 52 del Reglamento obliga al proveedor de servicios de cómputo en la nube a contar con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

Es imprescindible que el proveedor mantenga en todo momento informado al usuario acerca de su política de privacidad. Debe tenerse en cuenta que los proveedores pueden estar radicados fuera del territorio Mexicano y no estar sometidos a la legislación mexicana, lo cual no quita para exigir que se cumplan por el proveedor todas las garantías de la Ley y el Reglamento de Protección de Datos. Se trata, en definitiva, de una previsión que debe incluirse en el contrato que suscriban el Prestador de Servicios de Cloud y el usuario. De inmediato nos referimos a ello.

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

Se trata de una previsión que asimismo debe ser incluida en el contrato de prestación de servicios de cómputo en la nube. Se trata de una previsión no siempre fácil de cumplir en el ámbito de los contratos

de adhesión o en el de las cláusulas generales de contratación, dado su carácter rígido y no fácilmente modificable por el usuario.

Nos remitimos a lo que más adelante diremos sobre los llamados Acuerdos de Nivel de Servicio o, en inglés, "*Service Level Agreement*" (ANS/SLA).

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

Uno de los principios esenciales de la protección de datos es el de seguridad. Los artículos 19 y 20 de la LFPDPPP disponen:

> ***Artículo 19.-*** *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.*
>
> *Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.*
>
> ***Artículo 20.-*** *Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.*

En desarrollo de lo dispuesto en la Ley el Reglamento dedica todo su Capítulo III, artículos 57 a 66, a "las Medidas de Seguridad en el Tratamiento de Datos Personales". Asimismo deben tenerse en cuenta las definiciones de medidas de seguridad administrativas,

físicas y técnicas en las fracciones V, VI y VII del artículo 3 del Reglamento y la fracción III del artículo 50 del Reglamento en cuanto a la obligación del encargado del tratamiento de implementar medidas de seguridad.

El IFAI ha publicado documentos del máximo interés en lo que se refiere a las medidas de seguridad. Es necesario destacar:

- La *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, de Marzo 2014[38],
- Las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales*[39], y
- La *Guía para la elaboración de un Documento de seguridad*[40].
- La *Metodología de análisis de riesgo BAA*, de marzo de 2014[41].
- La *Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de datos personales*[42]

---

[38] http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_implementacion_SGSDP_marzo2014.pdf

[39] http://www.ifai.org.mx/datos_personales/seguridad.

[40] Elaborado por la Dirección General de Clasificación y Datos Personales, Instituto Federal de Acceso a la Información y Protección de Datos, v1.4, 17 de julio de 2009.

[41] http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf. En el Documento se explica el motivo de la expresión BAA (pág. 2 del Documento):

Un acercamiento para evaluar las medidas de seguridad necesarias para proteger los activos de información es a través del análisis de riesgo, de modo que se pueda determinar cuál riesgo es más importante mitigar o cuáles activos se encuentran más expuestos.

La metodología de análisis de riesgos que se presenta en este documento se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

1) Beneficio para el atacante. Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).

2) Accesibilidad para el atacante. Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).

3) Anonimidad del atacante. Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una empresa).

A partir de lo anterior, se ha dado el nombre de "BAA" a esta metodología de análisis de riesgos, lo cual tiene su origen en el Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante.

El objetivo de la metodología es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

[42] http://inicio.ifai.org.mx/DocumentosdeInteres/Tabla_Equivalencia_Funcional_2014.pdf. Se trata de un Documento de gran interés, en el que se analizan desde una metodología comparada los

En particular, la citada *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales* de marzo de 2014[43] recoge una referencia expresa a los contratos de cómputo en la nube, de acuerdo al siguiente tenor:

> *Cuando se establezca un contrato con un prestador de servicios de almacenamiento de información y/o de computo en la nube, además de revisar las clausulas referentes a los requerimientos de seguridad y de tratamiento de datos personales, de manera particular hay que: verificar el nivel de acceso que tiene el prestador y limitar el tratamiento a lo estrictamente necesario*

---

principales estándares internacionales de seguridad, con una referencia expresa a las exigencias de seguridad en el cómputo en la nube. Los estándares analizados son:
ISO/IEC 27001 (2005, 2013), Information Technology - Security techniques – Information security management systems – Requirements.
ISO/IEC 27002 (2005, 2013), Information Technology - Security techniques – Code of practice for security management.
ISO/IEC 27005:2008, Information Technology - Security techniques – Information security risk management.
ISO/IEC 27006:2011, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
ISO/IEC TR 27008:2011, Information technology -- Security techniques -- Guidelines for auditors on information security controls.
ISO/IEC 29100:2011, Information Technology - Security techniques -- Privacy framework.
ISO/IEC 20000-1:2011 Information technology - Service management -Part 1: Service management system requirements.
ISO 22301:2012 Societal security - Business continuity management systems – Requirements.
ISO 31000:2009, Risk management – Principles and guidelines.
ISO GUIDE 72, Guidelines for the justification and development of management systems standards.
ISO GUIDE 73, Risk management – Vocabulary.
ISO 9000:2005, Quality management systems -- Fundamentals and vocabulary.
BS 10012:2009 Data protection – Specification for a personal information management system.
NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems.
OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.
Generally Accepted Privacy Principles (GAPP) from American Institute of CPAs.
Control Objectives for Information and Related Technology (COBIT 4.1).
Control Objectives for Information and Related Technology (COBIT 5).
PCI DSS, Payment Card Industry Data Security Standard.
HIPAA, Health Insurance Portability and Accountability Act.
SOx, Sarbanes-Oxley Act of 2002.
ITIL, Information Technology Infrastructure Library.
The Open Web Application Security Project (OWASP).
Cloud Security Alliance Cloud Controls Matrix (CCM).

[43] Pág. 56.

para el cumplimiento de las condiciones del servicio; verificar el ciclo de vida de la información (por ejemplo, donde se almacena, como se replica, como se elimina en un ambiente distribuido, como se garantiza la eliminación de la información) y la ubicación física de la infraestructura del prestador.

Sin perjuicio de lo anterior, para garantizar la seguridad en la nube, según un reciente estudio llevado a cabo por Dan GRIFFIN y Tom JONES, titulado *Seguridad de nube: uso compartido sin riesgos de soluciones de TI*[44], deben ser dados los siguientes pasos:

a). Establecer una arquitectura orientada a servicios (SOA) para garantizar que puede reubicar cada componente con seguridad.

b). Centralizar la administración de los datos y la implementación y actualizaciones de las aplicaciones.

c). Usar la administración de identidad federada para asegurarse de que se conoce a cada usuario en cualquier punto de la nube.

d). Asignar roles y otros atributos a cada usuario para comprobar las notificaciones de acceso a datos.

e). Asignar reglas para el control de acceso de aplicaciones y datos que puedan moverse también a la nube.

f). Autorizar el acceso a las aplicaciones y datos según las notificaciones de acceso de usuario comprobadas.

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

[44] GRIFFIN, Dan y JONES, Tom**.** *Seguridad de nube: uso compartido sin riesgos de soluciones de TI*. 2010**.** http://technet.microsoft.com/es-es/magazine/gg296364.aspx

Cuando cesa la finalidad o cuando motivada y justificadamente se solicita por el afectado hay que proceder a devolver o cancelar los datos que se hayan transferido al encargado de tratamiento, a los efectos de la prestación objeto del contrato de servicios pactados. A tal efecto, vamos a empezar con el análisis de la obligación contractual de proceder a la devolución de los datos, o de los soportes en los que los mismos se contengan, en el supuesto que ello se hubiera pactado así en el contrato, haciéndose extensiva dicha obligación a los supuestos por defecto, en los casos, en que el contrato hubiera guardado silencio al respecto.

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

En realidad la anterior previsión no es más que una medida de seguridad específica que el Reglamento ha querido resaltar especialmente.

Establecidas todas las anteriores cautelas y exigencias, el artículo 52 del Reglamento advierte que *En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.* Es decir, se prohíbe a los responsables adherirse a servicios que no cumplan con las exigencias de la Ley y el Reglamento (y cualesquiera otras normas aplicables) en materia de protección de datos, lo que, en caso de incumplirse, podría dar lugar a responsabilidad por parte del usuario. Se trata, pues, de una importante y muy tajante previsión que han de tener presente todos cuantos pretendan contratar servicios de cómputo en la nube.

Como antes señalábamos, la mayoría de las previsiones exigidas por el artículo 52 del Reglamento podrían cumplirse mediante los Acuerdos de Nivel de Servicio o "*Service Level Agreement*" (ANS/SLA). Tales acuerdos suelen contemplar contractualmente que la propia empresa prestadora de servicios de Cloud se encargará del mantenimiento y seguridad de los sistemas que alojen la información.

Sin embargo, ese mero compromiso queda lejos de evitar potenciales conflictos respecto de las condiciones en que se llevará a cabo el mantenimiento del servicio y la solución de cuantos problemas de accesibilidad imputables al prestador de servicios de Cloud pudieran surgir o de aquellos relativos a la calidad de la prestación. Por ello, la contratación de servicios de Cloud , el contrato mismo, debería ir acompañado del denominado "Acuerdo de Nivel de Servicio" o "Service Level Agreement" a los efectos tanto de determinar y resolver las condiciones en las que serán prestados y se mantendrán dichos servicios, como en un intento de evitar y resolver los potenciales conflictos imputables al prestador de los mismos, que pudieran surgir en el desenvolvimiento de dicha relación contractual o con ocasión de la misma.

Tales Acuerdos comenzaron a emplearse en la década de 1980 por los operadores de telecomunicaciones, mediante los cuales acordaban con sus clientes empresariales unas condiciones mínimas de prestación del servicio, pues las comunicaciones electrónicas devenían ya en aquellos días fundamentales para el correcto desarrollo de la actividad empresarial. De ahí la necesidad de articular un sistema de responsabilidad para el operador respecto de la calidad del servicio a prestar a las empresas.

De las innumerables definiciones que pueden encontrarse del concepto de Acuerdo de Nivel de Servicio, especialmente significativa resulta la ofrecida por el *Department of Commerce* del Gobierno estadounidense en un documento sobre seguridad y privacidad en el ámbito del "Cloud Computing"[45]:

«Un "ANS" representa el acuerdo entre el beneficiario del Cloud y el prestador de servicios de Cloud respecto del nivel esperado del servicio a prestar y, en el supuesto de que el prestador no ofreciera el servicio a los niveles especificados, la compensación disponible para el beneficiario de los servicios de Cloud. Un "ANS", sin embargo, por lo general constituye solo una parte de los términos de servicio

[45] Vid.: http://www.commerce.gov/

estipulados en el conjunto del contrato o acuerdo de servicios. Los términos de servicio cubren otros detalles de importancia, tales como las licencias de servicios, los criterios de uso aceptable, la suspensión y terminación del servicio, límites a la responsabilidad, política de privacidad y modificaciones de los términos de servicio».

En definitiva, los Acuerdos de Nivel de Servicio, conforman una parte fundamental de la contratación empresarial de servicios de Cloud, encaminada a asegurar la correcta prestación de los servicios en cuestión, de manera que la misma satisfaga las necesidades de la compañía contratante.

Pese a ser esenciales, sin embargo, son precisamente eso: una parte del contrato; y ello, porque el resto del mismo contendrá, entre otros, todos los aspectos analizados con anterioridad, sin los cuales la configuración de los servicios a prestar y del acuerdo mismo carecería de la integridad necesaria.

Generalmente conformados como anexos al contrato, los Acuerdos de Nivel de Servicio (SLA/ANS) establecen una serie de parámetros objetivos acordados entre las partes mediante los que se concretan los grados de cumplimiento del servicio y/o los modos de proceder ante problemas de carácter técnico que pudieran surgir, tiempos de reacción ante tales problemas, tiempos de resolución de los mismos, disponibilidad de agentes encargados del mantenimiento, disponibilidad del servicio en sí mismo, niveles máximos o mínimos de disponibilidad de determinados valores (a modo de ejemplo: de suministro eléctrico, cantidad máxima de paquetes de datos cuya pérdida se entenderá como justificada, niveles de gravedad de incidencias, etcétera).

Es igualmente común que el propio Acuerdo de Nivel de Servicio (SLA/ANS) contemple la posibilidad de revisión (dentro de unos plazos conferidos por las partes al efecto) tanto de los parámetros contenidos en el mismo como de la cuantificación de los mismos. Y ello porque en multitud de ocasiones las partes no alcanzan la precisión deseada respecto de la calidad y grado de mantenimiento de los servicios

mediante una mera teorización a priori de los mismos. No es infrecuente la necesidad de ajustar el contenido de los Acuerdos de Nivel de Servicio (SLA/ANS) una vez puesta en marcha la prestación de los servicios de Cloud y comprobada la eficiencia de las medidas adoptadas para el aseguramiento de la calidad que el cliente necesita para el correcto desarrollo de su actividad empresarial. Por otra parte, no se puede por menos que hacer mención del régimen de responsabilidad asociado a los incumplimientos del Acuerdo de Nivel de Servicio (SLA/ANS). Tal régimen de responsabilidad difiere del configurado para supuestos de incumplimiento contractual de carácter general, en primer lugar, porque al que aquí nos referimos se limita exclusivamente a la inobservancia de lo dispuesto en el Acuerdo de Nivel de Servicio (SLA/ANS) frente al incumplimiento contractual de carácter general al que se vincula el régimen de responsabilidad stricto sensu.

En algunas ocasiones, el propio Acuerdo de Nivel de Servicio (SLA/ANS) contempla las penalizaciones a aplicar al prestador de servicios de Cloud por incumplimiento de lo establecido en el mismo. Sin embargo, no es poco habitual encontrar el desarrollo de las mismas conformando un anexo separado del anterior –si bien, formando aún parte del mismo contrato de prestación de servicios de Cloud -. Los términos que sirven de base para la configuración de las penalizaciones por incumplimiento de las condiciones establecidas en el Acuerdo de Nivel de Servicio (SLA/ANS) pueden adoptar diversas estructuras, siendo en todo caso de carácter económico. Si bien las fórmulas empleadas para la cuantificación de la sanción pecuniaria a abonar en supuesto de incumplimiento pueden alcanzar gran complejidad, por lo general incluyen una serie de parámetros comunes, a saber: la diferencia en la prestación respecto del umbral marcado como objetivo en el Acuerdo de Nivel de Servicio (SLA/ANS) y un importe tomado como referencia (que puede ser la cuantificación del beneficio que se hubiera obtenido si el resultado de la actuación hubiera sido satisfactorio o bien una cantidad a tanto alzado). Es decir, cuanto mayor fuera la desviación respecto de los parámetros acordados como correctos, mayor resultaría el importe a abonar como penalización.

En definitiva, la relevancia que en las últimas décadas han adquirido los Acuerdos de Nivel de Servicio (SLA/ANS) y, consecuentemente, el detalle de las penalizaciones por incumplimiento del mismo, dan una clara idea de la importancia no solo de que el servicio de Cloud sea prestado, sino que el mismo sea llevado a cabo o desarrollado en las condiciones más óptimas posibles.

En fin, el artículo 52 del Reglamento, al que venimos dedicando las anteriores páginas prevé que *Las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube.* En el momento de redactar el presente estudio (junio de 2014) tales criterios no han sido todavía elaborados, si bien más atrás hemos hecho referencia a diversos documentos del máximo interés elaborados por el IFAI en materia de seguridad en el tratamiento de datos que incluyen, como hemos visto, referencias expresas al cómputo en la nube.

Por otra parte, es necesario advertir que en lo que se refiere al cómputo en la nube no sólo debemos tener en cuenta lo que prevé el artículo 52 del Reglamento, sino las exigencias relativas a las transferencias internacionales, por cuanto será relativamente frecuente que el proveedor de servicios de *cloud* esté ubicado fuera del territorio mexicano. A tal fin es imprescindible tener presente lo que dispone el artículo 37 de la LFPDPPP y, en desarrollo del mismo, lo que establecen los artículos 74 a 76 del Reglamento.

Tener en cuenta la regulación de las transferencias internacionales es de suma importancia por cuanto es objetivo del legislador que las garantías sobre protección de datos se respeten también fuera del territorio mexicano cuando afecte a tratamientos que tienen su origen en México. Por eso el artículo 37 de la Ley exige en principio el consentimiento de los afectados para llevar a cabo una transferencia internacional. En caso de no contar con tal consentimiento la transferencia sólo será posible en los siguientes casos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular

Por su parte, el Reglamento establece diversas cautelas para llevar a cabo una transferencia internacional con garantías:

Condiciones específicas para las transferencias internacionales. Artículo 74.

Sin perjuicio de lo dispuesto en el artículo 37 de la Ley, las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

Formalización de las transferencias internacionales. Artículo 75.

A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones

a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.
Opinión del Instituto respecto de las transferencias. Artículo 76.
Los responsables, en caso de considerarlo necesario, podrán solicitar la opinión del Instituto respecto a si las transferencias internacionales que realicen cumplen con lo dispuesto por la Ley y el presente Reglamento.

4. El cómputo en la nube como oportunidad para que México aumente su competitividad internacional

El papel que juega el sector TIC en la economía no ha pasado desapercibido en México. Durante los últimos años, el sector ha crecido en importancia y se ha diversificado. Por ejemplo, de acuerdo con datos del Instituto Nacional de Estadística y Geografía, INEGI[46], el porcentaje del PIB atribuible al sector TIC pasó de 3.2% en el 2000 al 5.6% en el 2010, lo que representa un crecimiento del 75% en 10 años A pesar de estos avances aún quedan áreas de oportunidad para aprovechar plenamente el potencial de las TIC. Un ejemplo es el impulso de las *start-ups* mexicanas. No obstante los esfuerzos del gobierno por promover el nacimiento y consolidación de estas empresas, las cifras siguen siendo bajas. En 2011, se crearon en México .87 empresas por cada mil personas en la fuerza laboral. Mientras tanto en Chile y Brasil se crearon 4.13 y 2.38 empresas por cada mil personas en la fuerza laboral, respectivamente. El sector TIC muestra un crecimiento sostenido y adquiere cada vez una mayor importancia en la economía del país. En 2010, por ejemplo, el sector TIC representaba 5.6% del PIB y su importancia era mayor a la del total de las actividades primarias (3.8%). Además el sector ha mostrado un crecimiento sostenido en los últimos años con tasas de crecimiento anuales de 9.6% entre 2009 y 2012

[46] http://www.inegi.org.mx/

A pesar de sus avances, el sector TIC mexicano se queda corto ante otros competidores. En India, por ejemplo, el sector TIC pasó de representar 1.2% del PIB en 1998 a 7.4% en 2012. Además, en 2012 el sector TIC indio representó ingresos de 100 mil millones de dólares, más del doble que el sector TIC mexicano. Por otro lado, mientras en México la industria de software representa 0.7% del PIB, en Estados Unidos representa el 4% y genera cerca de 2 millones de empleos (*Select USA*, 2012[47]). Además, la importancia del sector TIC para la economía nacional es baja en relación con otros países. En Hong Kong, por ejemplo, el sector representa 8.3% del PIB. En México, la cifra es inferior a naciones como Costa Rica y China, aunque superior a naciones como Chile y Argentina.

En los últimos años, consultores internacionales de empresas especializadas en TI sitúan a México como uno de los jugadores más importantes en el sector. La firma *Gartner* lo colocó en el tercer lugar a nivel mundial en proveeduría de servicios de TI —sólo después de la India y Filipinas—, lo que lo vuelve líder en América Latina. Por otro lado, *ATKearney* ubica al país en el sexto lugar en el *Global Services Location Index*[48].

Una de las ventajas de México es su situación geográfica: su amplia frontera con Estados Unidos y costas en los océanos Pacífico y Atlántico. México tiene también un acceso preferencial a los mercados extranjeros, por los tratados de libre comercio firmados con en torno a 45 países. Además, el país está invirtiendo en formar más talento: se estima que cada año las universidades gradúan a 115,000 nuevos profesionales del ramo[49].

De acuerdo con el Instituto Mexicano para la Competitividad, el cómputo en la nube es el nuevo detonador para la competitividad de

---

[47] http://selectusa.commerce.gov/

[48] http://globaledge.msu.edu/global-resources/resource/293

[49] **"**Los Emprendedores de TIC en México: Recomendaciones de política pública para su nacimiento, crecimiento y consolidación", IMC. Instituto Mexicano para la Competitividad A.C. Abril de 2.014.
http://imco.org.mx/wp-content/uploads/2014/05/20140507_Los_Emprendedores_de_TIC_en_Mexico.pdf

México[50]. Según el IMCO, para el caso de México, los ahorros económicos de adoptar la nube equivalen a 0.31% del PIB nacional, de los cuales 0.23% corresponde al ahorro en el sector privado y 0.08% al ahorro en el sector público. Esta última cifra es similar al ahorro de 0.05% del PIB estadounidense estimado en el *Federal Cloud computing Strategy* para el sector público norteamericano. Asimismo considera que:

- Adoptar la nube podría generar cerca de 63 mil nuevos empleos en México, producto de reducir 1% el costo de entrada para pequeñas medianas empresas y permitiéndoles competir con empresas grandes a través de tecnología de bajo costo.
- El "cómputo en la nube" permite más acceso a la tecnología para la ciudadanía, disminuyendo la brecha digital, promoviendo la colaboración, cultura y la voz de la ciudadanía.
- El "cómputo en la nube" también beneficia al medio ambiente, al disminuir el consumo de electricidad por el mejor uso de la capacidad de cómputo instalado. Para México estimamos que dicho ahorro equivale a retirar 90 mil autos de circulación al año[51].

Se ha determinado que en muchos casos la falta de competitividad aunada a la mínima incorporación de tecnologías son factores que terminan propiciando la desaparición de las empresas, sobre todo de las PYMES, que constituyen el 95% de las compañías establecidas en México, generan más del 75% de la oferta laboral en el país y aportan por encima del 50% del Producto Interno Bruto (PIB). Sin embargo, con la aparición de las nuevas herramientas, como el *Cloud Computing*, los precios han bajado y cualquier compañía puede acceder a lasmnuevas tecnologías. El cómputo en la nube ha ayudado a que las empresas usen tecnología de manera fácil, rápida y a un costo muy razonable. En este sentido, uno de los motores que impulsan la competitividad de las pequeñas y medianas empresas es la adopción de uno o más servicios en la nube como parte integral de su

[50] http://imco.org.mx/wp-content/uploads/2012/6/ppt_computo_en_la_nube_competitividad_final.pdf

[51] Fuente: *Cloud computing End User Analysis Mexico*, FROST y SULLIVAN 2011. http://imco.org.mx/telecom_y_tics/computo_en_la_nube_nuevo_detonador_para_para_la_competitividad_en_mexico_pp/. Vid. también CEBALLOS, Francisco. "Cloud Computing, detonador de competitividad". Forbes México.
http://www.forbes.com.mx/sites/Cloud -computing-detonador-de-competitividad/

infraestructura, de acuerdo con el estudio *Parallels SMB Cloud Insights 2013* para México[52]. El documento detalla que el valor del mercado de PyMES mexicanas que utilizan *Cloud Computing* actualmente es de 5 mil 193 millones de pesos y estima que para el año 2016 el valor se incremente y supere los 15 mil millones de pesos. El incremento en el valor será una respuesta a la adopción de nuevos servicios, pues en 2012 el promedio de aplicaciones y servicios en la nube utilizados por las empresas fue de cuatro, mientras que Parallels prevé que en 2015 esa cifra se incremente a siete.

Respecto de la implementación, en muchos casos es posible acceder de inmediato a la aplicación requerida. Las soluciones en la nube suelen ser lo suficientemente flexibles como para ser configuradas de acuerdo a las necesidades de cada empresa en particular en un período de tiempo más que razonable.

Otra de las características positivas del cómputo en la nube es la relativa a simplificación en la gestión: es el proveedor el que se hace responsable por mantener el software, garantizar que esté funcionando la última versión disponible y ofrecer un centro de datos seguro. Asimismo la nube produce eficiencias en la operación y asignación de recursos, tanto humanos como tecnológicos, con la consolidación de soluciones en un solo recurso digital. Adicionalmente, los servicios de la nube son flexibles y adaptables a las necesidades crecientes de los usuarios, debido a que están basados en internet. En este sentido, las ventajas de la nube pueden ser incorporadas para todo topo de usuario. Además, la facilidad de acceso a los servicios de la nube constituye una gran ventaja para la administración de estos negocios.

En el corto plazo, 30% de las PYMES, que representan aproximadamente 67,400 unidades económicas, pueden ser beneficiadas por estrategias tecnológicas basadas en la nube, con pleno goce de sus efectos multiplicadores. También, pueden verse beneficiadas alrededor de 243,400 micro-empresas, que por su giro de

[52] Cfr.: “Acelera tu competitividad con Cloud Computing”. *Red de Empresarios Visa*. 19 de febrero de 2.013. http://www.redempresariosvisa.com/WorldToday/Article/acelera-tu-competitividad-con-Cloud -computing

negocios (diseñadores de software, consultorías, etc.) son intensivas en el uso de la tecnología y asemejan su consumo de servicios TI a los grandes corporativos.

Por lo tanto la adopción de servicios en la nube, alineada con estrategias empresariales, permite optimizar procesos, reducir costos y aumentar la productividad, lo que finalmente lleva a incrementar los ingresos de las empresas. Para dimensionar los ahorros por empresa, IMCO estimó el gasto de una empresa tipo (de 45 empleados) antes de migrar a la nube y después de hacerlo. Para ello, se comparó el gasto de servicios generales de TI de una empresa 'tipo' que opera con TI *on premise*, contra los costos de estos mismos servicios básicos con el nuevo servicio de Office 365 (en la nube). Los servicios que se consideraron básicos para esta empresa 'tipo' de 45 empleados fueron: correo electrónico, portal de colaboración, servicio de mensajería instantánea empresarial, audio conferencia y videoconferencia, además de paquetería Office.

La empresa tradicional, la que compra el equipo de TI para su operación, gasta 1,248,480 pesos anuales por estas aplicaciones de TI básicas. Dicho gasto no incluye el costo de las computadoras ni el costo de conexión a Internet al ser imprescindibles en ambos casos (con o sin nube). Si bien, es cierto que del total del gasto, 216 mil pesos (17%) son gastos de capital inicial (en servidores) que no se repiten año con año, los gastos de operación y mantenimiento del equipo sí son gastos recurrentes que equivalen a 19% del gasto total.

Según *Kio Networks*[53], la adopción de la tecnología de la nube en las organizaciones empresariales en México creció en los últimos cinco años, al pasar de 3.5 a 46%. Dicho incremento ubica al país en una posición competitiva en cuanto al uso de Cloud, que en el mundo representa 135 mil millones de dólares de inversiones para su implementación. En México la nube es una fuerza económica dentro de las empresas debido a los beneficios que ofrece en materia de

[53]Cfr.: "Aumenta el número de empresas Cloud izadas". EL EMPRESARIO.MX. 2 de septiembre de 2.013. http://elempresario.mx/tecnologia/aumenta-numero-empresas-Cloud izada

tecnología, y se estima que en los próximos cinco años entre 70 y 80% de las organizaciones estará "*Cloud izadas*". El aumento en la adopción de este recurso tecnológico sitúa a México entre los países que recurren más a la nube. En ese sentido, el 51% de las empresas en Inglaterra ya utiliza esa tecnología, en comparación con 46% de las compañías en México que ya cuentan con ésta. En todo caso la penetración de Cloud ha evolucionado de manera acelerada. En 2009 solo 3.5% de las organizaciones utilizaban algunos de los servicios que ofrece la nube. Hubo un punto de inflexión entre 2011 y 2012 en donde ya se conocía qué es el Cloud y sus beneficios y a inicios de 2014 el 46 por ciento de las organizaciones ya tienen alguna iniciativa alrededor de la nube. Hoy en día, se calcula que el uso de la nube como infraestructura de servicio podría llegar a registrar crecimientos de 80% anual, mientras que los incrementos de su uso como plataforma de servicio podrían ser de 36 por ciento.

Por otra parte, el "cómputo en la nube" representa importantes ahorros en energía y por tanto en emisiones de carbono, por lo que es considerada como Green IT. Dichos ahorros derivan principalmente de la optimización de los servidores que existen en el mundo. Si bien, transitar a la nube no necesariamente reduce la necesidad de servidores (aunque esto es debatible) pues se pasa de comprar a rentar servidores, si implica optimizar su uso, lo que reduce el consumo de energía.

El Estudio *Cloud computing and Sustainability: The Environmental Benefits of Moving to the Cloud* realizado en 2010 por Accenture[54] estima que los ahorros de energía por migrar a la nube pueden ser de hasta un 30% para implementaciones grandes (más de 10,000 usuarios) y de hasta un 90% para implementaciones de menor tamaño (100 usuarios).

---

54 http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Sustainability_Cloud_Computing_TheEnvironmentalBenefitsofMovingtotheCloud.pdf

Según el estudio, los factores que contribuyen a este ahorro son:

• Eficiencia: optimizar el uso de servidores existentes a su máxima capacidad (al empatar la capacidad de los servidores con la demanda).

• Tenencia múltiple: distintos usuarios utilizan la misma aplicación simultáneamente, disminuyendo las cargas durante horas pico, al servir a grandes números de usuarios y organizaciones en infraestructura compartida.

• Mayores eficiencias de consumo energético en los centros de datos (lugares donde se hospedan los servidores): utilizando infraestructura avanzada se reduce el consumo energético por el enfriamiento de los sistemas, como se describe más adelante.

Utilizando los supuestos de este estudio, IMCO estimó el ahorro en consumo eléctrico y en emisiones para México, partiendo del consumo base de la empresa 'tipo' de 45 personas y las emisiones de CO2 en el sector de empresas medianas y grandes.

Entonces, si una empresa con 100 empleados reduce sus emisiones de CO2 en 90% por usuario, al cambiar su correo electrónico, calendario, contactos y su portal de colaboración *on premise* a uno en la nube. Y por otro lado una con 1000 trabajadores reduce sus emisiones en 85%, dados los consumos de electricidad de una empresa mediana de 23 Mw/h al año 73 para mantener su infraestructura de TI, las emisiones de CO2 para dichas empresas caerían 13 toneladas al año, mientras que para las empresas grandes en 12 tCO2e al año.

Esto quiere decir que el sector de empresas medianas y grandes en México podría reducir en conjunto hasta 680 mil tCO2e anuales si todas las empresas migraran a la nube, lo que equivale a retirar a 90 mil vehículos de circulación.

Otros estudios son menos optimistas, el estudio *Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport*[55], explica que el consumo de energía del "cómputo en la nube" debe considerarse como una cadena de eventos logísticos que involucra procesos, almacenamiento y transporte de datos.

Por lo que cuando el tráfico de archivos descargados aumenta, incrementa el consumo de energía por el transporte de estos datos. Esto implicaría que por un lado, la nube incrementa el tráfico y consumo de energía, aunque por otro disminuye dicho consumo al optimizar el uso de servidores.

Finalmente, otro estudio que se avoca a entender el impacto ambiental del cómputo en la nube, "Energy-Efficient Cloud Computing" (publicado en *The Computer Journal*[56]) muestra que si bien la nube puede reducir las emisiones de carbono, aún tiene mucho camino que recorrer, principalmente en la optimización del gasto de energía de los sistemas de software y el consumo energético de los centros de datos (a pesar de su avance). Los centros de datos consumen gran cantidad de energía, especialmente por la transmisión y refrigeración de los mismos. Se estima que todos los proveedores de centros de datos consumen entre el uno y dos por ciento de la electricidad mundial. Sin embargo, sólo una mínima parte de dicha energía llega al procesador, el resto se consume en la transmisión y refrigeración.

Finalmente hemos de señalar que la crisis económica ha despertado el interés de las empresas y los Gobiernos (y entre ellos el gobierno Mexicano) por la nube como un medio para reducir costes, pero éste no es su único atractivo, puesto que también ofrece un amplio abanico de posibilidades, algo de lo que los usuarios se están dando cuenta poco a poco, como acabamos de ver. A pesar de esto el margen de crecimiento del Cloud Computing sigue siendo importante. Las principales barreras parecen ser la seguridad y la privacidad,

---

55 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5559320&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5559320

56 Volume 53, tomo 7, 2009, Pp. 1045-1051. Un resumen puede consultarse en http://comjnl.oxfordjournals.org/content/53/7/1045.abstract

aunque la confusión en los términos y la dificultad al gestionar los Acuerdos de Nivel de Servicio (ANS) también son obstáculos importantes. No obstante, las futuras oportunidades de la nube son grandes y una de las más importantes será la explotación de las redes sociales.

En cualquier caso, el *Cloud computing* no está limitado a las empresas. El gran tamaño, la complejidad y la gran expansión de los servicios de tecnología de los gobiernos los hace candidatos en esta carrera por subir a las nubes. En este proceso, la sensibilidad de la información gestionada por las Administraciones será el principal obstáculo. Gobiernos de todo el mundo están lanzando iniciativas a favor de esta tecnología, pero entre ellos destacan los de Gran Bretaña y Japón, que han optado por crear una nube privada «gubernamental».

La Administración tendrá un papel fundamental en la evolución del *Cloud computing* en México, tanto en su función de regulador, fijando las reglas de juego del mercado, como en su papel al adoptar, con las debidas garantías, servicios de *cloud*.

5. Las estrategias y enfoques a nivel internacional sobre el cómputo en la nube

5.1. Estados Unidos

Existen diferencias sobre el desarrollo de la tecnología *cloud* en los Estados Unidos y Europa[57]. Esta tecnología ha parecido siempre universal, acentuando su alcance global como uno de sus beneficios clave[58]. Sin embargo, estadísticas recientes han identificado claras diferencias entre EE.UU. y Europa en el ritmo de adopción de la nube.

[57] Estas cuestiones se comentan y analizan por Robert Assink con profusión en: “Factores que influyen en el éxito de la nube en Estados Unidos y Europa”. Ticbeat 17 de mayo de 2.013.
[58] Cfr.: http://www.revistaCloudComputing.com/2013/05/factores-que-influyen-en-el-exito-del-Cloud -en-estados-unidos-y-europa/

Según los analistas de IDC[59], los servicios de la nube pública alcanzaron 28 mil millones de dólares en 2011. De esta cifra, el 62 por ciento procede de Norteamérica, mientras que Europa no llega al 25 por ciento del total. Aparentemente las condiciones en EE.UU. son bastante diferentes a las de Europa, y existe un número de factores que impactan en el crecimiento, o en la falta del mismo, del modelo *Cloud* en cada mercado. El estímulo para el crecimiento del Cloud computing en EE.UU. El modelo *Cloud* en los EE.UU. ha crecido de forma constante desde sus inicios, debido principalmente a beneficios como la escalabilidad, la flexibilidad y la relación coste-eficacia. Con este crecimiento, los proveedores de servicios americanos han lanzado al mercado una variedad de entornos *Cloud* adaptables, abriendo las posibilidades a empresas de cualquier tamaño, configuración y enfoque para albergar datos o servicios en la nube. Como resultado, en Estados Unidos se está llevando a cabo una importante migración de datos a entornos *Cloud*, lo que ha llevado a una tasa de crecimiento promedio del 24 por ciento en las ventas de *Cloud* desde el año 2010, y a ratios de adopción del modelo que están creciendo a un ritmo 4 veces más rápido que el gasto en tecnología en general.

En febrero de 2012, la firma de inversiones *Kleiner Perkins Caulfield & Byers*[60] había invertido ya 120 millones de dólares durante el año anterior en 11 empresas de nueva creación dedicadas al *Cloud*, y anunciaba que pretendía invertir otros 100 millones de dólares durante 2012.

El Gobierno de los EE.UU. gastó 724 millones de dólares en el modelo *Cloud* sólo en 2012. Esta cifra ha crecido tras el lanzamiento por parte de la Casa Blanca de una iniciativa para transformar su habilidad en el uso de Big Data para descubrimientos científicos, investigación biomédica y de medio ambiente, educación y seguridad nacional. Similar a inversiones federales anteriores en tecnologías tales como internet, esta iniciativa apunta a expandir el número de tecnologías a través del patrocinio federal, incluyendo infraestructura

[59] Puede verse recientemente http://www.idc.com/research/viewtoc.jsp?containerId=247846
[60] Cfr.: https://www.kpcb.com/news

Cloud pública[61]. Como parte de este emprendimiento, los Institutos Nacionales de la Salud (NIH) migrarán a la *Cloud* pública el mayor conjunto mundial de datos sobre variación genética humana. Estos datos equivalen a 200 terabytes (aproximadamente 16 millones de archivadores llenos de textos o más de 30.000 DVD estándar).

Según Daniel CASTRO, analista de la Fundación para Información Tecnológica e Innovación[62] la cuantificación de los ingresos que las empresas de Cloud americanas podrían perder si la Casa Blanca o el Congreso no toman medidas drásticas para frenar las operaciones de inteligencia de la NSA ascenderían a entre 22.000 millones de dólares y 35.000 durante los próximos tres años.

Según el informe *CIO Agenda* para 2011 elaborado por la empresa de investigación de mercados *Gartner Executive Programs*[63], los sistemas de información en las compañías estadounidenses miran hacia el *Cloud computing*, como el siguiente gran paso a dar en la industria, vigilando igualmente los costos y la eficiencia.

Un estudio de la firma de IT *Neovise*[64] de 2013 revela que un 54% de las compañías de Estados Unidos está usando algún servicio de nube. De 161 organizaciones entrevistadas que utilizan la nube como servicio de plataforma IaaS, un 74% usa más de un sólo tipo, los cuales pueden ser públicos, privados o incluso una mezcla de ambas.

Otro estudio publicado por la compañía *Redwood Software*[65] indica que un 58% de las empresas en Estados Unidos usan servicios

---

[61] Cfr.: "El Estímulo para el crecimiento del Cloud computing en EE.UU, en "Factores que influyen en el éxito de la nube en estados Unidos y Europa". Catedra de Seguridad de la Universidad de Salamanca.
http://catedraseguridad.usal.es/blog/2013/05/factores-que-influyen-en-el-exito-de-la-nube-en-estados-unidos-y-europa/

[62] Cfr.: AP/IML. "Tecnológicas reclaman privacidad en internet". El Impulso.com. 10 de diciembre de 2.013. http://elimpulso.com/articulo/tecnologicas-reclaman-privacidad-en-internet, y GUILARTE, María. "Los proveedores de cloud se defienden de la NSA". Obra citada.

[63] Cfr.: MCDONALD, MARK P. "Teimagine IT: the 2011 CIO Agenda".21 de enero de 2.011 http://blogs.gartner.com/mark_mcdonald/2011/01/21/reimagine-it-the-2011-cio-agenda/

[64] NEOVISE. "Podcast Series: Neovise Cloud Perspectives". 2013. http://www.neovise.com/neovise-podcasts

[65] REDWOOD. Software Blog. http://www.redwood.com/blog/category/cloud-automation-2

de la nube como almacenamiento privado, mientras que en el Reino Unido ese número sólo llega a un 35%. El informe también demostró que las organizaciones en USA tienen una actitud más positiva hacia el *Cloud computing* que aquellas en el Reino Unido.

No obstante lo anterior, las empresas de *Cloud computing* estadounidenses experimentan también no pocos problemas. Una de las razones es la privacidad de los datos que se almacenan en sus servidores o que pasan por sus redes y que se ha visto comprometida tras conocerse el caso del espionaje masivo llevado a cabo por la NSA (Agencia de Seguridad Nacional) de Estados Unidos[66]. *Network World*, ha señalado que en los mercados de Europa Occidental, los proveedores de Cloud (tan grandes como Google o Microsoft) han tratado de suavizar las preocupaciones de sus clientes de la zona, que se encontraban alarmados debido a leyes como la *Patriot Act*[67] que permiten al gobierno de Estados Unidos acceder a los datos almacenados en empresas estadounidenses[68].

En cuanto a las repercusiones del espionaje masivo de Estados Unidos en los servicios de computación en la nube, cabe indicar que los documentos publicados por Edward Snowden**[69]** revelaron que uno

---

[66] Cfr.: GUILARTE, María." Los proveedores de cloud se defienden de la NSA". My Cloud. 27 de febrero, 2014 y CORBIN, Kenneth, en "Cloud Service Providers Fight Back, Challenge NSA" , en Network World, 26 de febrero de 2.014.

[67] Promulgada el 26 de octubre de 2001 y modificada por ley promulgada el 9 marzo de 2006.

[68] Hay numerosos estudios sobre la Patriot Act, sobre todo en relación con su incidencia en los derechos fundamentales y en la relación entre seguridad y rpivacidad. Vid entre otros los interesantes trabajos incluidos en *The Patriot Act and Related Provisions: The Heritage Foundation's Research, por* The Heritage Foundation, disponible en http://www.heritage.org/research/reports/2004/11/the-patriot-act-and-related-provisions-the-heritage-foundations-research . Una muy breve pero útil explicación de la Patriot Act puede consultarse en The USA PATRIOT Act: Preserving Life and Liberty, del Departamento de Justicia de Estados Unidas, disponible en http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf. Asimismo, Amitzai Etzioni, *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism*, Roudletdge, Londres, Nueva York, 2004; Cary Stacy, Ph.D. Smith, Li-Ching and Ph.D. Hung *The Patriot Act: Issues and Controversies*, Charles C. Thomas, Publisher, Sprinfield, 2010.

[69] Cfr.: LEYDEN, John. "Security guru: You can't blame EDWARD SNOWDEN for making US clouds look leaky And anyway, people aren't switching away". *The Register* 30 de abril de 2.014. http://www.theregister.co.uk/2014/04/30/mikko_hypponen_infosec_keynote_speech/ Cfr.: "Survey reveals impact of Snowden leaks on business attitudes to cloud computing". Out-law.com , 31 de marzo de 2.014. http://www.out-law.com/en/articles/2014/march/survey-reveals-impact-of-snowden-leaks-on-business-attitudes-to-cloud-computing/ Cfr.: NAUGTHON, John. "After Edward Snowden's

de los principales objetivos del espionaje masivo de la NSA de Estados Unidos, no ha sido el terrorismo sino el industrial y económico[70]. Una consecuencia directa ha sido la concienciación tanto de ciudadanos y empresas en establecer mayores mecanismos de protección de su privacidad y de su información más sensible, exigiendo que sus datos se almacenen en servidores ubicados en países con legislación más restrictiva.

Las repercusiones económicas han sido casi inmediatas. Según un estudio de la Fundación de Tecnología de la Información e Innovación[71], en 2016 las principales compañías tecnológicas norteamericanas soportarán una caída de ingresos de 35.000 millones de dólares (unos 25.800 millones de euros).

En la MEMO de la ***Comisión Europea***, **What does the Commission mean by secure Cloud computing services in Europe?**[72] se menciona cómo el programa PRISM de espionaje de la ***NSA*** ha afectado al desarrollo del *Cloud computing* en la institución:

- La Comisión estableció un *European Cloud Partnership Steering Board* ante las revelaciones del año 2013 y la reunión de julio discutieron sus posibles consecuencias.
- Los miembros del *Steering Board* expresaron una seria preocupación sobre el efecto de ***PRISM*** en relación a la adopción del *Cloud computing* en Europa y pidieron medidas urgentes para solucionarla.
- Después de ***PRISM*** se presentaron dos asuntos:

---

revelations, why trust US cloud providers? The NSA's activities are a massive blow for US computer businesses". *The Guardian Observer*. 15 de septiembre de 2.013. http://www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing

[70] Cfr. PALMA VILLALÓN, María del Valle, *La computación en la nube en Europa y en España: una oportunidad de negocio*. http://www.revistagestiondocumental.com/2014/03/18/httpwww-revistagestiondocumental-com20140317la-computacion-en-la-nube-en-europa-y-en-espana-una-oportunidad-de-negocio/#28B. Utilizamos este interesante trabajo para analizar las principales iniciativas de cómputo en la nube en Europa. Como podrá apreciarse, no pocas de las reflexiones siguientes se basan en dicho trabajo.

[71] http://www.itif.org/

[72] Cfr.: What does the Commission mean by secure Cloud computing services in Europe?. European Commission - MEMO/13/898. Bruselas 15 de octubre de 2013. http://europa.eu/rapid/press-release_MEMO-13-898_en.htm

- En primer lugar, una reticencia de los ciudadanos europeos, empresas y administraciones públicas a usar la computación en nube, considerando que los usuarios anteriormente ya tenían algunas reservas sobre la seguridad y confidencialidad de la información en la nube, el conocimiento de ***PRISM*** agravó esta situación.
- En segundo lugar, las revelaciones sobre ***PRISM*** han contribuido a incrementar las iniciativas de computación en la nube nacionales o regionales, lo que supone una oportunidad para las empresas que operan en Europa ya que ofrecen una nube con servicios confiables que cada vez más los usuarios exigen a nivel mundial. Aunque advierten que esta fragmentación o segmentación del mercado de la computación en la nube podría desgraciadamente detener el desarrollo del *Cloud computing* en Europa. Las administraciones públicas nacionales impiden que algunos tipos específicos de datos se transfieran fuera de sus fronteras, incluso dentro de la UE. Un mercado mayor aumentaría la competencia y la reducción de costes y también abriría nuevas oportunidades para los proveedores de la nube europeos, que en este momento están lejos de ser líderes en el mercado.

Los países latinoamericanos están también reaccionando, dado que la NSA ha controlado también sus comunicaciones. Entre ellos el más vigilado ha sido Brasil[73], seguido de Colombia[74] y México[75]. Entre los principales objetivos de la vigilancia cabe destacar la interceptación de secretos comerciales en el sector del petróleo y adquisiciones militares en Venezuela o el sector energético en México.

---

[73] Cfr.: http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0

[74] Cfr.: “Protegiendo la nube después de las filtraciones de la NSA”. Tienda Cloud. http://www.tiendacloud.co/noticias/protegiendo-la-nube-despues-de-las-filtraciones-de-la-nsa#sthash.7sgtiluW.dpuf. Fuente: http://www.cioal.com/

[75] Cfr.: MLOT, Sthephanie. “U.K., Canadian Firms Wary of U.S. Cloud After NSA Leaks”. PC NEWS. 10 de enero de 2.014. http://www.pcmag.com/article2/0,2817,2429392,00.asp. Cfr: NICCOLLS, Chris. “The NSA's New Target: Everyone!”. About.com Outsourcing. http://outsourcing.about.com/od/disruptive/a/The-Nsa-New-Target-Everyone.htm

Por otra parte, la implantación o el uso de servicios de *cloud computing* en Estados Unidos debe tener en cuenta el marco regulatorio existente.

Como es sabido, Estados Unidos carece de una Ley general de protección de datos, aunque sí deben ser tenidas en cuenta las leyes sectoriales aplicables[76]. En particular es imprescindible tener en cuenta no sólo la *Patriot Act* que ya hemos citado, sino también, entre otras, la *Health Insurance Portability and Accessibility Act* (HIPPA), de 21 de agosto de 1996; *Health Information Technology for Economic and Clinical Health Act* (HITECH), de 17 de febrero de 2009; *Children's Online Privacy Protection Act* (COPPA), de 21 de octubre de 1998; *Children's Internet Protection Act* (CIPA), de 21 de diciembre de 2000[77]; *CAN-SPAM Act (Federal law regarding unsolicited electronic mail)*, de 16 de diciembre de 2003; *Sarbanes–Oxley Act* (*Act To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes)*, de 30 de julio de 2002; o la Gramm–Leach–Bliley Act (Financial Services Modernization Act) de 12 de noviembre de 1999[78]. Todas ellas, como decimos, leyes sectoriales que entre otras cosas regulan las exigencias de privacidad en los ámbitos a que se refieren, previendo en algunos casos cuantiosas mutas para los infractores. Esto implica que quienes presten o requieran servicios de *cloud compunting* en alguno de dichos sectores (por ejemplo en el ámbito de la sanidad o en el sector financiero, o implique el tratamiento de datos de menores), deben tener muy presentes las exigencias impuestas por tales marcos regulatorios[79].

---

[76] Una relación, aunque no completa, de las leyes federales que afectan a la privacidad, puede consultarse en http://www.informationshield.com/usprivacylaws.html

[77] Fue declarada constitucional por Sentencia de la *United States Supreme Court* de 23 de Junio de 2003.

[78] Sobre las implicaciones de algunas de las anteriores leyes en el *colud computing*, vid. Thoran RODRIGUES, "What US businesses should know about compliance and regulatory issues before adopting a cloud strategy", en *Between the Lines* 4 de marzo de 2013. Disponible en http://www.zdnet.com/what-us-businesses-should-know-about-compliance-and-regulatory-issues-before-adopting-a-cloud-strategy-7000012085/

[79] Aunque no se refiere a todas las leyes que hemos citado en el texto, es útil el breve comentario *Cloud computing: Legal and Regulatory Issues*, de Vic (J.R.) WINKLER, TechNet Magazine, Mayo, 2012, disponible en http://technet.microsoft.com/en-us/magazine/hh994647.aspx

A lo anterior hay que añadir, en fin, la posible aplicación de los principios de Puerto Seguro. En efecto, la Unión Europea y Estados Unidos han llegado a un acuerdo por el que las empresas que se adhieran al sistema de Puerto Seguro o *Safe Harbour*, podrán ser consideradas por la Unión Europea como adecuadas en cuanto al tratamiento de datos personales, lo que facilita enormemente la transferencia internacional de datos desde la Unión Europea a tales empresas[80]. Esto implica que en principio las empresa estadounidenses adheridas al Puerto Seguro[81] deberán aplicar garantías en materia de protección de datos (incluidos los tratamientos en la nube) semejantes a las requeridas por la Unión uropea.

5.2. Unión Europea

Pese a que la penetración de la nube en Europa no ha sido igual de rápida y decisiva como en USA hay un interés considerable en todo lo relacionado con la nube.

La consultora IDC[82] ha previsto para Europa una tasa anual de crecimiento de la nube del 30% entre 2011 y 2016, frente a una tasa anual del 18,5% en USA, por lo que en unos años el nivel de adopción podría equipararse. Como antes hemos señalado, uno de los temas de discusión sobre la nube europea es que las leyes de protección de datos están dificultando la adopción del *Cloud computing*. Debe señalarse en cualquier caso que el interés en nube privada es cada vez mayor. Según IDC, los europeos están cada vez más interesados en la nube privada. Un 73% de las empresas encuestadas en el año 2012 aseguraron que están pasándose a la nube de algún modo, por encima del 67% del año anterior. Y el 55% dijo que se están pasando a la nube privada, frente al 36% de 2011.

---

[80] Vid las páginas Web http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm, y http://www.export.gov/safeharbor/ , que son sumamente útiles para una mejor comprensión del sistema de Puerto Seguro.

[81] La lista puede consultarse en https://safeharbor.export.gov/list.aspx

[82] CATTANEO, Gabriella. “The demand of Cloud computing in Europe: drivers, barriers, market estimates”. Associate VP IDC European Government Consulting. IDC. Bruselas. 2 de mayo de 2.012.
http://cordis.europa.eu/fp7/ict/ssai/docs/future-cc-2may-gcattaneo-presentation.pdf

GigaOM[83] ha resumido en un artículo algunas claves del despliegue de la nube en Europa, resaltando en particular tres aspectos: 1. Diferencias entre los mercados de Europa y Estados Unidos. 2. La adopción de la nube no está siguiendo los patrones de adopción de tecnologías anteriores. 3. La normativa sobre protección de datos.

Resalta en dicho artículo que al contrario que Europa, donde el mercado está muy fragmentado (diferentes idiomas, gobiernos, legislaciones, sistemas impositivos, etc.), USA tiene la ventaja de ser un mercado más grande y a la vez más homogéneo, donde proveedores como Amazon lo tienen mucho más fácil para despegar. De este modo, la adopción del *Cloud* en Europa varía mucho por países, y también por "especialidades", ya que mientras la adopción de SaaS está bastante extendida, la de IaaS es mucho más reducida.

Asimismo advierte que hasta ahora los primeros países europeos en adoptar una tecnología solían ser Reino Unido o países escandinavos como Finlandia, pionero en adoptar los teléfonos móviles; y posteriormente, las tendencias se expandían hacia el sur y los países mediterráneos. En cambio, en la adopción del *Cloud computing* podría darse al contrario, ya que los países del sur de Europa, que tanto están luchando actualmente por superar la crisis económica, podrían ver la nube como una manera de superarla.

Por otra parte, es de destacar que en septiembre de 2012, la Comisión Europea[84] adoptó la *Estrategia Europea de Cloud*

[83] Cfr.: "5 motivos por los que el Cloud computing no ha penetrado tanto en Europa como en Usa". Revista Cloud computing. 19 de septiembre de 2.012. http://www.revistacloudcomputing.com/2012/09/5-motivos-por-los-que-el-cloud-computing-no-ha-penetrado-tanto-en-europa-como-en-usa/

[84] «Liberar el potencial de la computación en nube en Europa». Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Comisión Europea. 27 de septiembre de 2.012, COM(2012) 529 final. Cfr.: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF. Asimismo, http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_lineas_ccoperacion/pae_Cooperacion_Internacional/pae_Estrategia_Europea_de_Cloud _Computing.html#.U23mvNhZrcc

computing[85]. Con ello busca habilitar y facilitar la adopción de las tecnologías *Cloud computing* en todos los sectores de la economía como palanca de productividad, crecimiento y empleo[86].

La *Estrategia Europea de Cloud computing* de la Comisión Europea está recogida en la comunicación «Liberar el potencial de la computación en nube en Europa»[87]. En la misma se proponen medidas para obtener 2,5 millones de nuevos puestos de trabajo en Europa, así como un incremento anual del PIB en la Unión igual a 160 000 millones de euros (en torno a un 1 %) de aquí a 2020.

Las tres acciones claves de la estrategia son:

a). Clarificación de normas y estándares

b). Contribuir a la clarificación de las normas técnicas para que los usuarios de los servicios *Cloud computing* dispongan de interoperabilidad, portabilidad de datos y la reversibilidad. La Comisión trabajará con el apoyo de ENISA y otros órganos pertinentes para ayudar al desarrollo en toda la UE de esquemas voluntarios de certificación así como una lista de dichos programas en 2014.

c). Creación de términos justos de contratación

El objetivo de la estrategia de *Cloud computing* es el desarrollo de términos de contratación de servicios en modelo *Cloud* para cubrir cuestiones no cubiertas por la normativa común de compraventa europea, tales como:

- preservación de datos después de la terminación del contrato

[85] Cfr. PALMA VILLALÓN, María del Valle, *La computación en la nube en Europa y en España: una oportunidad de negocio*., ya citado.

[86] Sobre la Estrategia, vid. Ramón Miralles, *Datos personales y contratación de servicios 'cloud': riesgos y oportunidades*, localizable en http://www.abogacia.es/2012/10/03/datos-personales-y-contratacion-de-servicios-cloud-riesgos-y-oportunidades/

[87] Cfr.: «Liberar el potencial de la computación en nube en Europa». Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Comisión Europea. 27 de septiembre de 2.012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF

- divulgación de datos e integridad
- localización y transferencia de datos
- la propiedad de los datos

Como ha señalado Ramón Miralles[88] el documento pone un especial énfasis en los beneficios de carácter económico derivados del *cloud compunting*, pero "también alerta sobre aspectos que deben ser mejorados para garantizar un desarrollo rápido, y sin obstáculos, de este tipo de servicios, y sobre todo destaca la necesidad de generar confianza en su empleo".

En este sentido, la Estrategia "identifica a las condiciones y términos que figuran en los contratos de servicios de *cloud*, como una de las cuestiones que deben ser solucionadas de manera inmediata". Resalta la importancia de llevar a cabo un mínimo análisis de riesgos y advierte que los servicios de *cloud* pueden producir la pérdida de control de la información, que como riesgo debe minimizarse todo lo posible.

"Una pérdida de control –destaca Miralles- amplificada por la general falta de transparencia en las condiciones de los servicios *cloud*, lo que dificultará llevar a cabo un análisis de riesgos apropiado, y que a su vez complicará el cumplimiento de determinadas obligaciones, en especial las relacionadas con el tratamiento de datos de carácter personal.

Esa pérdida de control se materializa en 3 dimensiones:

a) Perdemos el control directo de los datos: cuestión de especial relevancia en el caso de los datos de carácter personal

b) Perdemos el control directo de los procesos de tecnologías de la información: el rendimiento y disponibilidad de las tecnologías de la información, y su seguridad técnica pasa a

[88] Op. ult, cit.

depender de terceros, y todo ello con dependencia casi absoluta de las telecomunicaciones

c) Perdemos el control en relación a la capacidad contractual: salvo contadas excepciones no podremos negociar los términos y condiciones contractuales".

En cualquier caso, en la Estrategia la Comisión Europea deja claro que los servicios de *cloud* son una realidad y lo serán más en el futuro. Y en este escenario es imprescindible respetar el derecho a la protección de datos, lo que aconseja que la propuesta de nuevo Reglamento europeo de Protección de Datos sea aprobada a la brevedad.

Por otra parte, debe destacarse el establecimiento de un Partenariado Europeo de *Cloud computing*. El *European Cloud Partnership* (ECP)[89] reúne a expertos de la industria y de los usuarios del sector público para trabajar en los requisitos de contratación comunes para la computación en nube en forma abierta y completamente transparente. El sector público tiene un papel clave que desempeñar en la configuración del mercado de la computación en nube. Pero con el mercado del sector público fragmentado, sus requisitos tienen poco impacto, la integración de servicios es baja y los ciudadanos no tienen la mejor relación calidad-precio. La asociación de los actores públicos de la Unión Europea en un mismo foro se hace consecuentemente necesario para romper con el actual escenario que se constituye como una barrera para la adopción del *Cloud computing*.

La ECP funciona a dos niveles: un Consejo Directivo y un nivel de implementación. El Consejo de Dirección asesora a la Comisión sobre las opciones estratégicas para transformar la computación en nube en un motor para el crecimiento económico sostenible, la innovación y el coste-eficacia de los servicios públicos. El Consejo Directivo cuenta

[89] The European Cloud Partnership (ECP) brings together industry and the public sector to establish a Digital Single Market for cloud computing in Europe. Digital Agenda For Europe. A Europe 2020 Iniciative. European Cloud Partnership.Comisión Europea.
http://ec.europa.eu/digital-agenda/en/european-cloud-partnership

con un Presidente y está compuesto por representantes de alto nivel de la industria de TI y telecomunicaciones y los responsables de la toma gubernamental de política de TI. El nivel de implementación se articulará mediante una serie de proyectos cofinanciados por la Comisión Europea.

No obstante lo anterior, en el ámbito europeo todavía existe un gran desconocimiento en el mercado de lo que es y las ventajas que ofrece la tecnología *Cloud computing*, dato que ha quedado corroborado en el análisis cuantitativo de este informe. Concretamente, el 20,5% de las microempresas pymes españolas reconoce tener un sólido conocimiento de la tecnología Cloud Computing mientras un 54,9% señala no conocerla en absoluto[90].

En la antes citada MEMO de la Comisión Europea, *What does the Commission mean by secure Cloud computing services in Europe?*[91] se resalta:

- Lo que podría ganar Europa por ser un región de confianza en la nube líder en el mundo:
- La computación en la nube supone una ventaja competitiva para los proveedores europeos porque ofrecen estándares altos de protección de datos, seguridad, interoperabilidad y transparencia en los niveles de servicio y en el gobierno del acceso a la información. La propuesta para la regulación de protección de datos proporcionará un fundamento jurídico uniforme para la protección de datos personales en Europa. En particular, la nube pone las mejores soluciones al alcance de las pequeñas empresas que son la piedra angular de la economía europea, y la nube permitirá un salto particularmente grande de productividad en Europa si se convence a estas empresas para que la usen.
- Las posibles economías de escala de un mercado único de toda la UE realmente funcionarían para el *Cloud computing*, donde las barreras al libre flujo de datos en la UE se

[90] http://www.ontsi.red.es/ontsi/sites/default/files/2-_resumen_ejecutivo_Cloud _computing_vf.pdf
[91] *What does the Commission mean by secure Cloud computing services in Europe?.* European Commission - MEMO/13/898. Bruselas 15 de octubre de 2013, citada.

reducen sustancialmente, lo cual supondría un enorme impulso a la competitividad. Es la razón por la que Europa debe establecer un mercado interior completamente funcional para Cloud Computing.

- Una amplia adopción de *Cloud computing* por el sector público conduciría a fijar el marco adecuado para que el negocio de la nube en Europa pueda salir adelante, el sector público en Europa se debe posicionar como un *early adopter* de la computación en la nube.
- La restauración de la confianza y construcción de una nube más segura y confiable en Europa:
- La confianza de los clientes puede restaurarse con una mayor transparencia y el uso de altos estándares. La estrategia europea de *Cloud computing*, incluye medidas para mejorar la transparencia del mercado. Para ello son esenciales: una descripción mejor de los estándares, una certificación del uso de dichas normas y unas condiciones del contrato seguro y justo para el *Cloud computing*. Los niveles de servicio deben ser transparentes, como el tiempo en que se desarrolla el servicio y lo que ocurre cuando no funciona. Los informes y auditorías sobre el acceso a los datos deben estar accesibles a los clientes para poder controlar qué usuarios consultaron sus datos y los porqués. Asimismo se deben contemplar aspectos tan importantes como la interoperabilidad o la comunicación a los usuarios de situaciones potenciales de bloqueo en posibles infracciones de seguridad. Además, para restaurar la confianza y la transparencia se debe establecer un marco de gobernabilidad para el acceso, informando de aquellos casos en que los gobiernos y los servicios de inteligencia, en cumplimiento de las leyes y de la seguridad nacional, solicitan consultar los datos de los clientes.
- Los servicios transfronterizos en la nube son necesarios: Los servicios en la nube transfronteriza deben ser la norma, no la excepción. Se debe evitar la fragmentación del mercado y evitar la necesidad de una reforma en la reglamentación de la industria de nube.

- Necesidad de colaboración entre los Estados miembros y el sector privado para la adopción de servicios en una nube segura: Tiene que ser un esfuerzo combinado ya que la adopción de servicios en una nube segura en Europa no va a ocurrir a través de acciones independientes realizadas por actores individuales. La estrategia europea para *Cloud computing* ayudará pero también necesitará que los Estados Miembros trabajen juntos para compartir sus propias soluciones de mejoras. En este sentido, la Comisión está apoyando la iniciativa en la nube para Europa, preparando al sector público para la contratación de servicios en la nube, maximizando los beneficios y competencia, y minimizando riesgos. Aunque la industria de la nube también deberá participar invirtiendo en soluciones de seguridad innovadoras.
- Las soluciones en la nube pueden ser más seguras que las locales: Muchas empresas prefieren procesar y almacenar sus datos localmente porque les parece que están más seguros. Indiscutiblemente se pueden crear nubes locales en dichos centros pero puede que no sean seguras ya que no cumplirían los niveles más altos de seguridad. Por otra parte, actualmente los sistemas no están tan herméticamente cerrados como en el pasado debido al uso de los servicios móviles, la tendencia hacia el uso de dispositivos propios y el intercambio de plataformas con clientes, ciudadanos, socios de negocios, etc. Por esta razón, la computación en nube, con las debidas especificaciones, se presenta como una alternativa más segura.
- Se recomienda la encriptación en el tránsito y almacenamiento para proteger información sensible: el cifrado puede y se debe usar para proteger la información sensible cuando está transitando y cuando se almacena. Aunque se puede romper el cifrado, es necesario desarrollar soluciones para hacerlo muy seguro. La autenticación de la seguridad podría permanecer sólo en manos del titular de los datos, de esta manera se eliminaría el riesgo de que alguien más pueda descifrarlo.

En este contexto por parte de la Comisión Europea, se asignó como tarea al *European Telecommunications Standards Institute* (ETSI) realizar un mapa de los estándares *Cloud Computing* en colaboración con todas las partes interesadas pertinentes.

En noviembre de 2013 ETSI[92] publicó un mapa de estándares necesarios para el *Cloud Computing* en el que se presenta una definición de los roles, una colección y clasificación de más de 100 casos de uso; una lista de 20 organizaciones normalizadoras relevantes; una selección de alrededor de 150 documentos asociados, normas y especificaciones; informes y *white papers* producidos por dichas organizaciones; una clasificación de actividades que necesitan llevarse a cabo por los clientes o los proveedores de los servicios de Cloud durante todo el ciclo de vida del servicio; y un mapeo de los documentos de *Cloud Computing* (en particular de estándares y las especificaciones) en estas actividades.

El documento de ETSI parte de la existencia de tres fases en la provisión de servicios de *cloud*[93]:

- Phase 1: Acquisition of Cloud Service
- Phase 2: Operation of Cloud Service
- Phase 3: Termination of Cloud Service

En el análisis de dichas fases se adoptan las siguientes perspectivas[94]:

- The Service Level Agreement (SLA) Perspective
- The Interoperability Perspective
- The Security Perspective

La Comisión Europea se comprometió a trabajar con el apoyo de ENISA[95] (*European Network and Information Security Agency*) y otros

[92] Cfr.: ETSI. "ETSI delivers report on Cloud computing Standards", 16 de diciembre de 2.013. http://www.etsi.org/

[93] Pág. 6 y págs.. 14 y ss.; y 19 a 26, del Documento.

[94] Págs. 6 a 13.

órganos pertinentes para ayudar al desarrollo de sistemas de certificación voluntaria de toda la UE en el área de computación en nube y establecer una lista de dichos planes para el año 2014. También se estableció el grupo de trabajo *Industry Group* (SIG)[96] en la certificación para apoyar el trabajo de certificación. La certificación de servicios de *Cloud computing* puede ayudar a proporcionar mayor transparencia en el mercado, permite a los proveedores demostrar a sus clientes que están cumpliendo con ciertos estándares, por ejemplo, en red y en seguridad informática. Esto ya ha generado resultados intermedios: una lista de sistemas de certificación existentes y un conjunto de principios y recomendaciones que el grupo SIG-certificación considera importante cuando se trata de certificación de computación en la nube.

Como también destaca PALMA VILLALON[97], ENISA[98] ya publicó en el 2009, un informe sobre la gestión de riesgos en la nube, *Cloud Computing Security Risk Assessment* apoyada por un grupo de expertos integrado por representantes de la industria, instituciones académicas y organizaciones gubernamentales. Se llevó a cabo una evaluación de riesgos en el modelo de negocio y tecnologías de computación en nube en el contexto del proyecto *Emerging and Future Risk Framework*. El resultado es un análisis en profundidad e independiente que describe algunos de los beneficios de seguridad de información y los riesgos de seguridad clave de *Cloud computing*. El informe también proporciona un conjunto de recomendaciones prácticas. Este es un análisis en profundidad e independiente que describe algunos de los beneficios de seguridad de información y los riesgos de seguridad clave de la computación en la nube. El informe también proporciona un conjunto de recomendaciones prácticas.

---

[95] Cfr.: ENISA. “Cloud computing”. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

[96] Cfr.: “Cloud Select Industry Group on Certification Schemes”. Digital Agenda For Europe. A Europe 2020 Initiative. Comision Europea. https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-certification-schemes

[97] “La computación en la nubeen Europa y en España….”, cit.

[98] Cfr.: ENISA. “Cloud computing”, cit.

En la misma dirección, en enero de 2011, ENISA publicó en colaboración con INTECO[99] una guía para las administraciones públicas en materia de *Cloud computing*, *Security and Resilience in Governmental Cloud's* que muestra los pasos a seguir para implementar una arquitectura de estas características e identifica un modelo de toma de decisiones con respecto a los requisitos operativos, jurídicos y de seguridad de la información a la identificación de la solución de arquitectura de computación que mejor se adapte a las necesidades de su organización. INTECO también publicó un documento en el 2011, *Riesgos y amenazas en Cloud Computing*, que analiza la problemática de estos entornos, proporcionando una visión global, desde los puntos de vista de NIST, Gartner y CSA. Actualmente ENISA está desarrollando una visión sobre la importancia de los servicios en la nube, el ahorro en los costes de los servicios de centros de datos y del impacto de un fallo de estos servicios.

Muchos de estos pasos necesarios ya se han identificado como acciones en el *Single Market Pillar* de la *Digital Agenda for Europe*[100].

En Europa, las empresas europeas que ofrecen servicios de cómputo en la nube se han constituido en asociaciones nacionales y han formado una federación, EuroCloud. Los países que la integran son: Portugal, España, Francia, Reino Unido, Bélgica, Luxemburgo, Alemania, Suiza, Suecia, Austria, Eslovenia, Italia, Irlanda, Bulgaria, Eslovaquia, Polonia, Rumanía, Serbia y Hungría.

Por otro lado, 9 organizaciones de toda Europa ((Inria (Francia), CNR (Italia), Genias (Holanda), HP (Italia), Linagora GSO (Francia), STFC (Reino Unido), Tiscali (Italia), VU – University, Amsterdam (Holanda), Tiscali (Italia), Zlab (Slovenia), ZIB zuse Institute Berlin (Alemania)) han colaborado en Contrail la European Cloud Federation

---

[99] Cfr.: http://www.inteco.es/viewCloud/inteco_cloud_en/

[100] Las acciones clave de la Agenda Digital, como recuerda PALMA VILLALÓN, son:
Acción clave 1: Promover un uso mayor de los estándares del Cloud y de la certificación de servicios en la nube.
Acción clave 2 – Términos y condiciones de contratos seguros y justos
Acción clave 3 – Promover un liderazgo común del Sector público a través de una asociación Europea de Cloud

Framework, que es el primer nivel de la Federación Open Computing Infrastructure for Elastic Services[101].

En un informe de Verizon y Emc[102] se incluyen las principales barreras en Europa para la adopción del *Cloud computing*: seguridad y protección de datos (30%), confiabilidad (25%), localización de los datos (24%), soporte local (23%), control del cambio (22%), propiedad de la personalización (21%), evaluación de su utilidad (18%), conexión lenta a internet (18%), lenguaje local (18%) e incentivos fiscales en gastos de capital (17%). En cuanto a la las principales preocupaciones de los clientes destacan: quién es el responsable de los datos y de su integridad; qué ocurre si se produce una brecha de seguridad; facilidad para cambiar los datos a otro proveedor en la nube, o conectar con otra aplicación de otro proveedor.

Dicho lo anterior, es imprescindible advertir que el desarrollo del *Cloud computing* en Europa está muy condicionado por la normativa de protección de datos. En este sentido, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[103] es el marco normativo de referencia, que ha inspirado todas las leyes que sobre protección de datos existe en los Estados miembros de la Unión Europea. Así lo ha resaltado el llamado Grupo del Articulo 29, o Grupo Europeo de Autoridades de Protección de Datos, en su importante Opinión 5/2012, sobre *Cloud computing*, de 1 de julio de 2012, Documento WP 196. En dicho Documento se llama la atención acerca de la necesidad de que el desarrollo del *Cloud computing* en Europa respete en su integridad el derecho a la protección de datos de carácter personal.

---

[101] PALMA VILLALON, María del Valle. “La computación en la nube en Europa y España: una oportunidad de negocio”. Revista de Gestión Documental. 18 de marzo de 2.014 http://www.revistagestiondocumental.com/2014/03/18/httpwww-revistagestiondocumental-com20140317la-computacion-en-la-nube-en-europa-y-en-espana-una-oportunidad-de-negocio/

[102] Cit. por PALMA VILLALON, “La computación en la nube…”, cit. Cfr.: KAR, Saroj. “ EMC Partners with Verizon to Offer Cloud Services”. 18 de junio de 2.012. http://cloudtimes.org/2012/06/18/emc-verizon-services-terremark/

[103] Diario Oficial nº L 281, de 23 de Noviembre de 1995

La Directiva, en efecto, es sin duda el instrumento normativo más importante en materia de protección de datos en Europa. Todas las leyes sobre protección de datos aprobadas en los 28 Estados Miembros de la Unión Europea son transposición de dicha Directiva. Es decir, son un fiel reflejo de su texto.

Además constituye punto de referencia a nivel mundial, pues no sólo ha sido y es utilizada como modelo por las regulaciones sobre protección de datos que se han aprobado en numerosos países no europeos (por ejemplo en la mayoría, por no decir todos, de los países de América Latina que cuentan con normatividad sobre protección de datos, a los que luego nos referiremos) sino que numerosos países están adaptándose a la Directiva y numerosas empresas multinacionales (algunas de ellas importantes proveedoras de servicios de *cloud*) se someten a sus previsiones, por ejemplo al adherirse al sistema de Puerto Seguro. En este sentido es importante resaltar la reciente Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, asunto C-131/12, *Google vs. Agencia Española de Protección de Datos y Mario Costeja*. El Tribunal de Justicia se ocupa fundamentalmente del llamado derecho al olvido, pero también analiza la aplicación extraterritorial de la Directiva 95/46. Para ello, como ha estudiado PIÑAR MAÑAS[104], parte de la base de que Google Inc. (con sede en Estados Unidos) gestiona el motor de búsqueda, que indexa páginas web de todo el mundo, y de que el Grupo Google utiliza una filial en España, Google Spain, como agente promotor de venta de los espacios publicitarios que se generan en "www.google.com". En este marco interpreta el art. 4.1.a) de la Directiva, según el cual los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para su trasposición a "todo tratamiento de datos personales cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro". En su análisis el Tribunal parte de la base de que el precepto no exige que el tratamiento de datos sea efectuado "por" el

[104] "Aplicación extraterritorial de la Directiva 95/46/CE sobre protección de datos y derecho al olvido frente a los motores de búsqueda. Comentario rápido a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2013, caso Google", en *Revista IURIS* (LA LEY - Wolters Kluwer), núm. 215, 1.ª quincena de junio de 2014, págs. 20 y ss. y en la *Revista Latinoamericana de Protección de Datos Personales*, Julio, 2014.

propio establecimiento sino “en el marco” de sus actividades; resalta que la Directiva debe garantizar una protección eficaz y completa de los derechos y en particular del derecho a la intimidad en lo que respecta al tratamiento de datos, así como su “efecto útil”; y recuerda que las actividades del gestor del motor de búsqueda y las de su establecimiento en España están indisociablemente ligadas. Y en base a todo ello concluye que la Directiva y la legislación nacional de trasposición son aplicables a Google Inc. De este modo se aclara, en este caso, el espinoso problema de la aplicación de la Directiva en relación con tratamientos de datos llevados a cabo fuera de su territorio, lo que asimismo refuerza la opción de la propuesta de nuevo Reglamento Europeo de Protección de datos, cuyo artículo 3.1 recoge el principio de aplicación extraterritorial de la Directiva en ciertos casos.

La Directiva 95/46/CE es, pues, de una gran importancia en el marco del desarrollo del *cloud computing* en Europa y más allá de sus fronteras.

La Directiva, como es sabido, recoge los principios de protección de datos (información, finalidad, habilitación del tratamiento, sobre todo en base al consentimiento, calidad del dato, seguridad y principio de control independiente), regula las relaciones entre responsable y encargado, las transferencias internacionales de datos, la autorregulación en materia de protección de datos y prevé la existencia necesaria de autoridades independientes de protección de datos que tutelen y garanticen de forma efectiva el derecho a la privacidad.

Tras la Directiva, que está todavía en vigor, fue aprobada la Carta Europea de Derechos Fundamentales, cuyo artículo 8 ha reconocido expresamente el derecho fundamental a la protección de datos en los siguientes términos:

Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de

otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente

Es decir, se ha elevado a rango "constitucional" el reconocimiento de la protección de datos como derecho fundamental, lo que debe ser tenido en cuenta por todos cuantos operan como clientes o prestadores de servicios de *cloud computing*.

Precisamente la importancia de la perspectiva de la protección de datos en el ámbito del cómputo en la nube ha sido puesta de manifiesto por el llamado Grupo del Artículo 29, así denominado por haber sido creado en virtud de lo dispuesto por el artículo 29 de la Directiva 95/46/CE e integrado por las Autoridades Europeas de Protección de Datos, además del Supervisor Europeo de Protección de Datos y la Comisión Europea. Se trata de un grupo de enorme prestigio y reconocimiento que, como antes adelantábamos, ha elaborado la Opinión 5/2012, sobre *Cloud computing*, de 1 de julio de 2012.

Según indica el Documento[105], "Una de las principales conclusiones del presente dictamen es que las empresas y las administraciones que deseen utilizar la computación en nube deben efectuar, como un primer paso, un análisis de riesgos completo y riguroso. Los proveedores en el EEE [Espacio Económico Europeo] deben proporcionar al cliente toda la información necesaria para evaluar adecuadamente los pros y los contras de la adopción de tal servicio. La seguridad, transparencia y seguridad jurídica para los clientes deberán ser los principales impulsores de la oferta de servicios de computación en nube". El Documento subraya, "las responsabilidades de un cliente de servicios de computación en nube (como responsable del tratamiento) y … recomienda, por tanto, que el cliente seleccione un proveedor de servicios de computación en nube que garantice el cumplimiento de la legislación de la UE sobre

[105] Pág. 2

protección de datos. El dictamen aborda las salvaguardias contractuales apropiadas estableciendo la condición de que todo contrato entre el cliente y el proveedor deberá ofrecer garantías suficientes en términos de medidas técnicas y de organización. También es importante la recomendación de que el cliente de servicios de computación en nube deberá verificar si el proveedor de tales servicios puede garantizar la legalidad de las transferencias internacionales de datos"[106].

Del Dictamen merece la pena asimismo transcribir los siguient4es párrafos: "El dictamen especifica los principios aplicables a los responsables y los encargados del tratamiento derivados de la Directiva europea sobre protección de datos (95/46/CE), como la especificación de la finalidad y la limitación, la supresión de datos y las medidas técnicas y de organización. El dictamen establece directrices sobre los requisitos de seguridad, como salvaguardia estructural y de procedimiento. Se hace especial hincapié en las disposiciones contractuales que deben regular la relación entre los responsables y los encargados del tratamiento en este sentido. Los objetivos clásicos de seguridad de los datos son la disponibilidad, la integridad y la confidencialidad. Sin embargo, la protección de los datos no se limita a la seguridad y, por tanto, estos objetivos se complementan con los objetivos específicos de transparencia, aislamiento, posibilidad de intervención y portabilidad para justificar el derecho del individuo a la protección de datos, con arreglo a lo previsto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE.

Por lo que se refiere a las transferencias de datos personales fuera del EEE, se analizan instrumentos tales como las cláusulas contractuales estándar adoptadas por la Comisión Europea, la comprobación del nivel adecuado de protección de los datos y posibles futuras normas corporativas vinculantes (NCV) relativas al encargado del tratamiento, así como los riesgos para la protección de los datos derivados de las solicitudes internacionales de intervención legal"[107].

[106] Pág. 2
[107] Págs. 5-6.

Por otra parte debemos hacer mención a la propuesta de nuevo Reglamento Europeo de Protección de Datos de carácter personal que, presentada en diciembre de 2012 parece que será aprobado en los primeros meses del próximo año 2015[108]. Dicha reforma, en cuyo detalle ahora no es preciso entrar dado que todavía se trata de una propuesta, ha sido objeto de debate en el Parlamento Europeo, que ha aprobado una posición común el pasado día 12 de marzo de 2014[109], lo que permite aventurar que puede ser finalmente aprobado. En cualquier caso, no contiene una regulación específica del cómputo en la nube, si bien contiene alguna novedad, en lo que ahora interesa, digna de mención. Así, se recogen expresamente los principios de privacidad desde el diseño y por defecto (*privacy by design* y *privacy by default*), así como el principio de responsabilidad (*accountability*) y el de portabilidad. Se resalta la importancia del análisis y prevención de riesgos, y el papel de la autorregulación. Regula con mayor detalle las relaciones entre el responsable del tratamiento y el encargado (así como con los posibles subencargados), lo que es especialmente relevante en materia de *cloud computing*. Contiene un régimen sancionador más riguroso y prevé la existencia del llamado *Data Privacy Officer*, en algunos casos con carácter voluntario y en otros obligatorio. En fin, refuerza el principio de aplicación extraterritorial de la normatividad europea.

Resulta pues evidente que el desarrollo del *cloud computing* en Europa es muy notable. Y merece la pena destacar que tal desarrollo se produce conviviendo con un marco regulatorio sobre protección de datos muy restrictivo y garantista de los derechos de los titulares de los datos.

---

[108] Vid. http://ec.europa.eu/justice/data-protection/review/index_en.htm

[109] *(A7-0402/2013 - Ponente: Jan Philipp Albrecht)* Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

5.3. Asia

En relación con Asia es muy destacable el incremento que está experimentando el uso del *Cloud computing*. Así lo resalta la *Asia Cloud computing Association*[110].

Según el Estudio elaborado en 2013 por CISCO junto con INTEL *The Impact of Cloud on IT Consumption Models Insights from Cisco/Intel Study of 4,226 IT Leaders Across 18 Industries and Nine Key Economies*[111] en Asia[112], el 96% de los encuestados dice que el Cloud computing es “algo” o "muy positivo" para las organizaciones TI, pero un 46% señaló que la seguridad que plantea el Cloud computing es un gran inhibidor para su adopción. En cuanto al presupuesto gastado en Cloud computing por organizaciones TI se estima en un 24% en el año 2013, presupuesto que podría alcanzar un 30% en 2016.

El 92% de los encuestados piensa que el impacto del Cloud computing va a actuar más como una “agente de servicios” para la empresa. El impacto que se generará en organizaciones descentralizadas será de un 21%, mientras que en organizaciones más centralizadas de un 79%. El 80% de las organizaciones esperan aumentar sus plantillas y el 20% cree que tendrá menos plantilla o no realizará ningún cambio.

Nos referiremos a continuación a los casos de China, India y Japón. También debe destacarse que en Corea del Sur el uso de servicios de Cloud está experimentando un crecimiento realmente notable como se pone de manifiesto en el Documento *Cloud computing Market in Korea 2014-2018*[113] en el que se pone de manifiesto que el

---

[110] http://www.asiacloud.org/index.php

[111]http://www.cisco.com/web/about/ac79/docs/re/Impact-of-Cloud-IT_Consumption-Models_Study-Report.pdf

[112] Cfr. : La adopción e impacto del Cloud computing en el mundo ». Comunidad Baratz. 17 de septiembre de 2.013. http://www.comunidadbaratz.com/blog/la-adopcion-e-impacto-del-cloud-computing-en-el-mundo

[113] http://www.researchandmarkets.com/research/q3gd5q/cloud_computing

Gobierno pretende llegar a una aportación en el mercado del Cloud que suponga el 10% del mercado global del cómputo en la nube en ese país[114].

5.3.1. China

El auge del *Cloud computing* en China comenzó a finales de 2010[115], cuando el gobierno anunció los planes de desarrollo económico hasta 2015 en los que las tecnologías de la información y comunicación entraron a formar parte esencial del plan de ruta diseñado por el PCC (Partido Comunista de China) como uno de los 7 pilares esenciales que deben posicionar al país como líder no solo en materia económica, sino también tecnológica. En la actualidad los centros de proceso de datos europeos y americanos se encuentran situados mayoritariamente en Japón, Singapur Hong Kong e India.

Un Informe del Centro de Investigación, Inteligencia y Análisis (CRIA) destaca como la rápida expansión del sector de la computación en la nube en China, podría contener "minas terrestres". La computación en la nube está creciendo rápidamente en China gracias al fuerte apoyo del gobierno. Según la Asociación de la Industria de Software del país Asiático, en la cadena de valor del *Cloud computing* se espera un incremento de al menos 122 mil millones de dólares en 2015. Los mismos beneficios que inducen la adopción del Cloud Computing en los EE.UU. y en otros lugares, como el fácil almacenamiento de datos y el mantenimiento a bajos costos, han sido los puntos por los cuales China ha optado por su adopción gradual, especialmente en agencias del gobierno, las finanzas, la petroquímica, y los sectores de la salud. Aunque hay muchos otros sectores en los que puede expandirse, teniendo en cuenta que China tiene la mayor población mundial de usuarios de Internet.

---

[114]http://www.businesswire.com/news/home/20140124005545/en/Research-Markets-Cloud-Computing-Market-Korea-2014-2018#.U6cPLPl_uSo

[115] Cfr.: XATAKA MOVIL. "China apuesta fuerte por el Cloud computing". 25 de marzo de 2.012. http://www.xatakamovil.com/servicios/china-apuesta-fuerte-por-el-cloud-computing

La expansión del cómputo en la nube en China fue declarada una prioridad en el 12º Plan Quinquenal del gobierno lanzado en 2011, junto a otros esfuerzos para estimular las industrias "de nueva generación".

Mientras que la necesidad de las empresas extranjeras por ofrecer servicios y tecnología es clara, los autores del informe CRIA, "Red Cloud"[116] aconsejan proceder con cautela. Preparado a petición del Consejo Económico EEUU-China y la Comisión de Revisión de Seguridad, el informe pone en relieve algunos problemas potencialmente espinosos que acompañan la incursión de compañías extranjeras en el mercado de *Cloud computing* en China.

Muchas empresas extranjeras localizadas en China desconfían de la situación. Mientras que el 38% de los encuestados de la AmCham[117] con la *China Business Survey Report* manifestaron que sus compañías estaban trasladando los recursos a la nube, sólo el 10 % dijo que consideraba el uso de los servicios de cómputo en la nube con sede en China, y la razón que se dio fue abrumadora: "preocupaciones sobre la seguridad de los datos". Mientras tanto, el 42% de los encuestados dijeron a AmCham que "ellos creen que el riesgo de una fuga de datos de [sus] operaciones en China" está aumentando.

Dicho lo anterior, debe destacarse que la República Popular China cuenta con un marco regulatorio sobre protección de datos relativamente reciente. El 28 de diciembre de 2012 fue adoptada la "*Decision of the Standing Committee of the National People's Congress to Strengthen the Protection of Internet Data"* (*"Decision"*)[118]. Tal Decisión tiene el valor de una ley y regula la protección de datos en

---

[116] Cfr.: ¿Será el Cloud computing en China una bendición o peligro para las empresas?. Tienda Cloud. 2013.http://www.tiendacloud.co/noticias/sera-el-cloud-computing-en-china-una-bendicion-o-peligro-para-las-empresas#sthash.Zr0EPKXJ.dpuf

[117] AmCham China. 2013 China Business Climate Survey Report http://web.resource.amchamchina.org/cmsfile/2013/03/29/0640e5a7e0c8f86ff4a380150357bbef.pdf

[118] Vid. Tina U. AMIN, China adopts privacy legislation strengthening online personal data protection, Baker & Hostetler LLP, Enero 2013. Disponible en http://www.lexology.com/library/detail.aspx?g=3dcc0bf1-73f1-4efd-9b8f-90dcf5300cb1

China. En principio cabe afirmar que la Ley responde a los estándares de las leyes de protección de datos que hemos ido analizando si bien se aplica fundamentalmente en el ámbito de Internet (dispone, entre otras cosas que no es posible utilizar identidades falsas en internet) y no hacer referencia expresa al cómputo en la nube. Regula el tratamiento de determinados datos sensibles (datos de salud, datos financieros o crediticios), establece principios de finalidad, consentimiento o calidad del dato. Se reconoce el derecho de acceso y rectificación, pero no en todos los casos el de cancelación. Impone la implantación de medidas de seguridad en el tratamiento de datos y regula las transferencias internacionales de datos. Pero la Ley no contiene una previsión en relación con la autoridad independiente que debe tutelar la protección de datos. Hay previsto un régimen sancionador que es aplicado por diversas autoridades gubernamentales no independientes[119].

5.3.2. India[120]

La percepción de la importancia de la privacidad en India no es todavía muy importante, pero poco a poco va en aumento[121]. La importancia que a la protección de datos se concede queda patente por el hecho de que pese a que la India no cuenta con una específica Ley de Protección de datos, en 2011 se ha dado un paso importante en orden a su regulación.

En efecto[122], no existe una legislación específica sobre la privacidad y protección de datos en la India. Sin embargo, la Ley de

---

[119] Vid. *Data protection in China: overview*, Q&A guide to data protection in China, Junio 2014. Disponible en http://uk.practicallaw.com/4-519-9017

[120] La información sobre la situación en India la tomamos de "La nube del Gobierno en India". Serie global de blogs CISCO. "El papel de la nube en los gobiernos locales". 14 de junio de 2.013. http://www.blogciscolatam.com/2013/06/la-nube-del-gobierno-en-india-2/

[121] Vid el muy interesante Documento *Privacy in India: Attitudes and Awareness V 2.0*, Ponnurangam Kumaraguru (\PK"), Niharika Sachdeva, Indraprastha Institute of Information Technology, Delhi, 2012.

[122] Vid. el capítulo sobre India en *DATA PROTECTION LAWS OF THE WORLD*, elaborado por DLAPiper, disponible en http://www.dlapiperdataprotection.com/#handbook/world-map-section . Asimismo en http://www.mondaq.com/india/x/231376/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+India.

Tecnología de la Información, de 2000 (la "Ley") contiene disposiciones específicas destinadas a proteger los datos electrónicos (incluyendo los registros no electrónicos o información que han sido, son en la actualidad o que están destinados a ser procesados electrónicamente).

El Ministerio de TI de la India adoptó las Information Technology Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) ("Privacy Rules"). Las Privacy Rules, que entraron en vigor en 2011, exigen que las entidades corporativas que recolecten, procesen y almacenen datos personales, incluyendo información personal, cumplan con ciertos procedimientos. Distingue entre 'información personal' e 'información personal sensible'.

En agosto de 2011, el Ministerio de Comunicaciones e Información de la India emitió una *"Press Note" Technology (Clarification on the Privacy Rules*)[123]. En cualquier caso, debe advertirse que no existe una autoridad de control independiente que garantice la tutela del derecho a la protección de datos.

En India el gobierno ha implementado la nube GI, que es una iniciativa nacional que permitirá al gobierno, en distintos niveles, hacer uso del cómputo en la nube para una entrega más eficiente de servicios de gobierno electrónico.

El objetivo de esta iniciativa es respaldar finalmente la implementación del Plan Nacional de Gobierno Electrónico de India (NeGP) mediante la creación de un ambiente de nube privada, que será utilizado por las agencias o departamentos a nivel nacional, estatal y local para acelerar la distribución de servicios electrónicos a los ciudadanos. Esto también aumentará la agilidad y la eficacia operacional mientras ayuda a compartir recursos para inversión en otras áreas clave.

La iniciativa completa se llevará a cabo en dos partes. En primer lugar, se intentará replicar en todos los estados las iniciativas que ya

[123] Vid. Ruth BOARDMAN, Divya SHARMA, Gabriel VOISIN, *India's new data protection regime*. Disponible en http://www.twobirds.com/en/news/articles/2013/indias-newdp-regime

fueron implementadas con éxito en pocos estados. La segunda parte llevará a cabo la creación de un repositorio común de recursos basados en la nube y aplicaciones disponibles de manera compartida.

Junto con esto, el Departamento de Electrónica y TI (DeiT) también ha implementado un borrador de hoja de ruta para la nube GI. Esta hoja de ruta evalúa esencialmente la infraestructura de Tecnologías de la Información y la Comunicación (TIC) existente y las iniciativas de TIC, así como los posibles obstáculos. Luego, define un plan para la implementación efectiva de la nube GI que incluye el uso de centros de datos nuevos y existentes. La evaluación ayudó a definir la arquitectura esta nube.

La nube nacional que se utilizará para proporcionar varios servicios -desde el almacenamiento hasta el desarrollo de aplicaciones-, recibirá soporte de las nubes estatales y se creará un directorio de servicios para ayudar a las organizaciones del sector público a buscar y suscribirse a varios servicios.

El directorio de servicios proporcionará visibilidad y control integrados para ayudar a los departamentos a eliminar la responsabilidad de adquisiciones y mantenimiento prolongado de una infraestructura de TIC, un ejercicio que muchos, especialmente a niveles estatales y locales, consideran difícil de realizar. Esto proporcionará la oportunidad para las agencias que atraviesan su primera automatización, de avanzar de un salto pues podrán comprar los servicios directamente sin tener que atravesar el ciclo completo de evolución de TIC.

El modelo de pago por uso de asignación de precios en la nube, garantiza que los recursos y aplicaciones de TIC estén disponibles sin una inversión significativa en compras de infraestructura. La nube también facilitará la movilidad del usuario, por que le permitirá el acceso en cualquier momento, en cualquier lugar.

La nube GI también reducirá el esfuerzo del gobierno por administrar la tecnología, pues las ofertas de la nube se basan en un

fundamento de tecnología prefabricado y estandarizado que permite un mejor soporte.

La nube GI establecerá las normas en cuanto a interoperabilidad, integración, seguridad, y portabilidad de datos eliminando de esta manera los escenarios bloqueados por el proveedor.

Finalmente, también dividirá los silos entre las agencias y los departamentos aumentando la agilidad y eficacia operacional, lo que permitirá a las agencias ofrecer mejores servicios, más rápido y en tiempo real. Y con las crecientes presiones que enfrentan los gobiernos en la actualidad, esto sigue siendo más importante que nunca.

Con todo esto, la nube GI proporciona una solución cooperativa para agencias nacionales, estatales y gubernamentales, pero finalmente, lo que una solución de la nube para el gobierno hace en realidad en términos sencillos es crear nuevas posibilidades para los ciudadanos y empleados.

Con relación a la India, debe indicarse que el escenario exige claramente una imagen clara de las oportunidades del mercado y el futuro esperado de la nube en el país. Para entender esto, es conveniente tomar en consideración un resumen de algunos informes de firmas de analistas de investigación publicados recientemente[124], la mayoría publicados en el último trimestre de 2013: Gartner[125]; Servicios de Consultoría de Cisco (CCS)[126]; VMware, Inc. índice Cloud: estudio realizado por Forrester Research[127] en 12 países de Asia Pacífico; CII [128]; Estudio de Microsoft IDC[129]; EMC y Zinnov Management

[124] http://www.forbes.com
[125] Cfr.: Gartner. “Says Indian Public Cloud Services Market on Pace To Total $550 Million In 2014”. Gartner Newsroom. 21 de febrero de 2.014. http://www.gartner.com/newsroom/id/2669116
[126] Cfr.: Bradley, Joseph, MACAULAY, James, NORONHA, Andy, y SETHI, Hiten. CISCO SYSTEM. “Influencia de la nube en los modelos de consumo de la TI 10 conclusiones principales”. http://www.cisco.com/web/about/ac79/docs/re/Impact-of-9-Cloud_IT-Consumption-Models_Top-10_es-eu.pdf
[127] Cfr.: ANDERSON, Dane. “India Datacenter Study: Cloud computing”. 1 de agosto de 2.010. http://www.forrester.com/India+Datacenter+Study+Cloud+Computing/fulltext/-/E-RES59575
[128] Cfr.: “The Indian Cloud Revolution”. Confederation of Indian Industry. http://www.cii.in/cloudreport

Consulting[130]. En todos ellos se resalta el notable incremento que va a experimentar el Cloud computing en India, y la importancia que tiene en su desarrollo económico y tecnológico.

5.3.3. Japón[131]

La Ley de Protección de Datos Personales de Japón (Ley N ° 57 de 2003), promulgada el 23 de mayo de 2003, entró en vigor el 30 de mayo de ese año para el sector público y el 1 de abril de 2005 para el sector privado. La Ley tiene como objetivo "proteger los derechos e intereses de las personas, teniendo en cuenta la utilidad de los datos personales, habida cuenta del notable incremento en el uso de la información personal debido al desarrollo de la sociedad de la información y la comunicación" (artículo 1).

Es muy importante señalar que la Ley constituye sólo una parte de la totalidad del marco regulatorio de Japón. La Ley esboza requisitos y obligaciones generales, dejando los detalles de su regulación e interpretación a los diferentes Ministerios del Gobierno, que emiten directrices administrativas para los sectores empresariales de los que son responsables[132].

Según el *Global Cloud computing Scorecard* de 2012 realizado por Business Software Alliance (BSA), ya citado en este Estudio, Japón es el país que brinda un ambiente más amigable para los proveedores

---

[129] Cfr.: MICROSOFT “Cloud computing to Create 14 Million New Jobs by 2015”. Microsoft News. 5 de marzo de 2.012. http://www.microsoft.com/en-us/news/features/2012/mar12/03-05cloudcomputingjobs.aspx

[130] ET BUREAU Cfr.: “Cloud computing landscape to deliver up to 50% saving to India Inc, create 1 lakh additional jobs by 2015”. THE ECONOMIC TIMES. 19 de julio de 2.011 http://articles.economictimes.indiatimes.com/2011-07-19/news/29790777_1_cloud-adoption-cloud-market-zinnov-management-consulting

[131] Cfr.: CRUZ, Xath. “The State of Cloud computing Around the World: Japan”. *Cloud Times*. 4 de diciembre de 2.012. http://cloudtimes.org/2012/12/04/state-cloud-computing-around-world-japan/

[132] Vid. Michiru TAKAHASHI, *Personal Information Protection Law in Japan*, noviembre 2005. Disponible en http://www.jonesday.com/personal-information-protection-law-in-japan-11-09-2005/. Asimismo, Lawrence G. CARTER y Ryo TAKIZAWA, capítulo sobre Japón, en *DATA PROTECTION LAWS OF THE WORLD*, DLAPiper, Disponible en http://www.dlapiperdataprotection.com/#handbook/about-section

de servicios en la nube, gracias a su alta tasa de adopción de banda ancha, las fuertes leyes contra los delitos cibernéticos y su marco sólido para promover la seguridad y proteger la privacidad de los usuarios[133].

Como se ha resaltado en el Estudio elaborado por INTECO sobre "El cloud computing en el sector público en España"[134] en Japón merece destacar como caso de éxito en el sector público el Proyecto - Red cloud Kasumigaseki (Plan TIC Hatoyama). Impulsado por el Ministerio de Asuntos Internos y Comunicaciones de Japón, el Plan Hatoyama tiene como objetivo desarrollar la industria y empleo de las TIC y optimizar la gestión tecnológica en los organismos públicos. Una de las iniciativas que contempla este Plan es la implantación de la red cloud Kasumigaseki que integrará servicios, plataformas e infraestructuras para la mayoría de ministerios en un entorno de procesamiento de datos centralizado, servicios compartidos y aplicaciones en línea. Se prevé que esté disponible en el 2015. La red estará orientada a la integración de los servicios tecnológicos e infraestructuras de los Ministerios del Gobierno de Japón. Gracias a esta integración se mejorará en la estandarización tecnológica, la compartición de servicios y la interoperabilidad de los organismos públicos, que redundará en la calidad y accesibilidad de los trámites electrónicos que se prestan a los ciudadanos y empresas.

Entre los servicios más destacados de la futura "nube" japonesa está el sistema de Archivo Nacional Digital, futuro repositorio de documentos, expedientes, datos y otros activos documentales electrónicos oficiales del Gobierno nipón que serán publicados a los ciudadanos en formatos accesibles para cumplir con los principios de transparencia y open data.

En cuanto a las empresas, cada vez es mayor el número de datos e información que almacenan, por lo que se presenta cada vez más

---

133 http://empresas.it/2013/03/estos-son-los-mejores-y-los-peores-paises-para-el-computo-en-la-nube/#sthash.rjIo6VCg.dpuf

134 http://www.cfnavarra.es/observatoriosi/pdf/estudio_inteco_cloud_computing_en_sector_publico/estudio_inteco_cloud_computing_en_sector_publico.pdf

necesario optar por servicios en la nube, en cuanto tecnología capaz de proporcionar un almacenamiento ilimitado.

Las empresas de telecomunicaciones locales (tales como NTT, Fujitsu y NEC) están construyendo infraestructuras de Cloud computing con el fin de atender a las crecientes demandas de rapidez en el mercado. Fujitsu ha optado claramente por el *Cloud* como lo demuestra la colaboración en el interesante documento *The Impact of Cloud*, elaborado por The Economist[135]

Debe tenerse en cuenta la celebración de la "Cloud computing Expo de Japón"[136] en la primavera de 2015, que reunirá a los diversos tipos de productos y servicios de Cloud computing.

5.4. Latinoamérica

Según el ya citado Estudio elaborado en 2013 por CISCO junto con INTEL *The Impact of Cloud on IT Consumption Models Insights from Cisco/Intel Study of 4,226 IT Leaders Across 18 Industries and Nine Key Economies[137],* en Latinoamérica[138] el 95% de los encuestados afirmó que el *Cloud computing* es "algo" o "muy positivo" para las organizaciones TI, pero un 32% señaló que la seguridad que plantea el *Cloud computing* es un gran inhibidor para su adopción. En cuanto al presupuesto gastado en *Cloud computing* por organizaciones TI se estima en un 30% en el año 2013, presupuesto que podría alcanzar un 32% en 2016.

---

[135] http://www.fujitsu.com/es/Images/wp-eiu-impact-of-cloud.pdf

[136] Cfr.: " Cloud computing Expo Japan Spring". http://www.japan-it.jp/en/Concurrent-Shows_Spring/CLOUD/About/

[137] http://www.cisco.com/web/about/ac79/docs/re/Impact-of-Cloud-IT_Consumption-Models_Study-Report.pdf

[138] Cfr : La adopción e impacto del Cloud computing en el mundo ». Comunidad Baratz. 17 de septiembre de 2.013. Obra citada.

El 72% de los encuestados piensa que el impacto del *Cloud computing* va a actuar más como una "agente de servicios" para la empresa. El impacto que se generará en organizaciones descentralizadas será de un 54%, mientras que en organizaciones más centralizadas de un 46%. El 69% de las organizaciones esperan aumentar sus plantillas y el 31% cree que tendrá menos plantilla o no realizará ningún cambio.

Según la consultora internacional IDC, el mercado del *Cloud computing* en Latinoamérica se puede valorizar en 280 millones de dólares y tendrá una tasa de crecimiento anual de un 70% entre el 2012 y 2016.

La variedad de proveedores presentes en la región, los beneficios de conectividad y seguridad, y la reducción de costos para las empresas, serían algunas de las razones que convertirían a "la nube" en un espacio deseado por las compañías de América Latina.

Según una encuesta realizada en 2010 por la *Information System and Audit Control Association* (ISACA)[139] a 433 de sus socios, profesionales del área de negocios y tecnología de América Latina, cerca de un tercio de las organizaciones optaría por servicios de Cloud Computing durante ese año.

El 41% de los entrevistados en la encuesta "*IT Risk/Reward Barometer*" de ISACA[140], opina que los beneficios asociados a la implementación de *Cloud computing* son mucho mayores que los riesgos.

Asimismo, un estudio sobre adopción de servicios Cloud Computing, realizado por *SpiceWorks*[141] indica que el 43% de la

139 Cfr. : « América Latina en la Nube: Cloud computing como una solución tecnológica". AETECNO. 16 de enero de 2.011. http://tecno.americaeconomia.com/noticias/america-latina-en-la-nube-cloud-computing-como-una-solucion-tecnologica Cfr.: http://www.isaca.org/. Cfr: "La nube y las empresas en América Latina". Caracas Digital. http://www.caracasdigital.com/pasado/noticias-masdetalle_imprimir.php?detalle=2505

140 *ISACA's 2012 IT Risk/Reward Barometer*. http://www.isaca.org/Pages/2012-Risk-Reward-Barometer.aspx

141 Cfr.: AeTecno. "America Latina en la Nube: Cloud computing como una solución tecnológica". 16 de enero de 2.011. Cfr.: **"**La opción tecnológica de las empresas hoy es el Cloud computing".

pequeña y mediana empresa en América Latina ha elegido poner su información en la nube, durante el primer semestre de 2010. Este sector concentra a los negocios emergentes, que son más arriesgados en la búsqueda de soluciones tecnológicas que los países del Norte y Europa.

En la actualidad, varias empresas en América Latina[142] proveen esta plataforma para que otras compañías y organizaciones puedan almacenar su información como respaldo.

En cuanto a los sectores que más optan por los servicios de *cloud*, destacan la industria farmacéutica, financiera, de retail, agroindustrial, de la salud, manufacturera, de energía, de telecomunicaciones, servicios, la Banca, el Gobierno y la educación, principalmente universidades, con precios, espacio y funcionalidades de acuerdo a las necesidades del consumidor.

Respecto a la implementación del almacenamiento en la nube las empresas que quieran recibir servicios de *cloud* deben tener acceso a una buena red pública de datos. Adicionalmente el cliente debe contar con la organización interna y los recursos humanos necesarios para poder explotarlos. Por otro lado, la preferencia de los consumidores va por el lado de los centros de datos, soluciones de almacenamiento y seguridad.

El desarrollo de esta tecnología está ligada a las ventajas que ofrece el servicio. Así empieza a existir la creencia común de que estar conectados es una necesidad imperiosa tanto para las personas como para las empresas. Con la nube, es posible acceder desde cualquier computador con conexión a internet, a cualquier hora y en cualquier lugar a los datos almacenados por el usuario, sin necesidad de llevar

---

Ediciones Especiales On Line. 28 de abril de 2.011. http://www.edicionesespeciales.elmercurio.com/hoy/detalle/index.asp?idnoticia=20110428703417&idcuerpo=612

[142] Cfr. : «Informe plantea los retos del Cloud computing en América Latina". Tienda Cloud. http://www.tiendacloud.co/noticias/informe-plantea-los-retos-del-cloud-computing-en-america-latina#sthash.tdDoPU2f.dpuf

dispositivos externos ni trasladar la información físicamente, con riesgo de perderla.

La reducción de costos es también un elemento importante, sobre todo, mirando hacia la pequeña y mediana empresa. Se destaca el hecho de que no haya que pagar por servidores, licencias de software ni mantención de infraestructura, sólo se paga por un servicio. El costo total de una plataforma segura de mensajería, colaboración y comunicación en la nube puede costar un 60 a 80% menos que en una arquitectura interna. Al parecer, el tema de los ataques informáticos o la pérdida de datos está resuelto por los proveedores. El uso de data centers en alianza con empresas especializadas, con la encriptación y monitoreo de la información correspondiente, son algunas de las maniobras utilizadas para que el almacenamiento en la nube se convierta en una de las soluciones IT preferidas en la región.

Las preocupaciones más frecuentes entre los usuarios giran en torno a la pérdida de control que se deriva de transferir datos y procesos a la nube.

Pero desafíos tales como la pérdida de datos y el robo de propiedad intelectual se encuentran clasificados por debajo de otros temas como los retos de integración y costos de implementación.

Los encuestados clasificaron los desafíos relacionados con la seguridad como algunos de los más difíciles de superar, lo que indica que los proveedores todavía tienen el reto de cambiar esta percepción.

De ahí que no sorprenda que en esta primera encuesta las mayores preocupaciones estén en torno de fallas en seguridad por parte del proveedor. En segundo lugar está el miedo a la fuga de información de los clientes, seguida de la continuidad del negocio en caso de eventualidades.

Los países están mejorando el ambiente legal para “La Puntuación Global de la nube”[143], pero el ritmo es irregular, a punto de

[143] Cfr. : «La BSA presenta el estudio "La Puntuación Global de la Nube". 14 de marzo de 2012.

representar obstáculos para concretizar el potencial pleno de las tecnologías de computación en nube, según lo indica el ya citado informe de la BSA[144].

Como sabemos, se considera que México es el país de América Latina con una mejor predisposición para implantar servicios de *Cloud*. Países latinoamericanos como Argentina y Brasil continúan progresando. Ya lo hicieron en el 2013 y se espera que este crecimiento sea mayor en el 2014, pues han subido posiciones en la clasificación global de políticas, debido al gran compromiso con el desarrollo del sector informático y telecomunicación, así como la actualización y aprobación de leyes beneficiosas para el cómputo en la nube lo que reflejó significativamente y de forma positiva su puntuación en el informe del 2013.

Dicho lo anterior, cabe señalar que ya son numerosos los países de América Latina que cuentan con normatividad sobre protección de datos. Las normas generales (no se recogen las normatividades sectoriales) hasta ahora aprobadas son:

Argentina

— Ley 25.326, de 2 de noviembre de 2000, de Protección de Datos Personales (Boletín Oficial de 2 de noviembre de 2000)

— Decreto 1558/2001, de 29 de noviembre, reglamentación de la Ley 25.326 (Boletín Oficial de 3 de diciembre de 2011)

Brasil

— Ley 12.965, de 23 de abril de 2014, por la que se aprueba el Marco Civil de Internet (Diario Oficial de 24 de abril de 2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Chile

---

http://cioperu.pe/articulo/9514/la-bsa-presenta-el-estudio-la-puntuacion-global-de-la-nube/

[144] Cfr. : http://empresas.it/2012/03/white-paper-la-puntuacion-global-de-la-nube/

— Ley 19628 sobre protección de la vida privada (Publicada el 28 de agosto de 1999)

— Decreto 779 por el que se aprueba el Reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos (Publicado el 11 de noviembre de 2000)

Colombia

— Ley Estatutaria 1581 de 2012, por la que se dictan disposiciones generales para la protección de datos personales

— Decreto 1377 de 2013, de 27 de junio, por el cual se reglamenta parcialmente la Ley 1581 de 2012

— Decreto 886 de 13 de mayo de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos

— Ley Estatutaria 1266 de 2008, de 31 de diciembre por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Costa Rica

— Ley nº 8968, de 7 de julio de 2011, de Protección de la Persona frente al tratamiento de sus datos personales (Publicada en la Gaceta nº 170 de 5 de septiembre de 2011)

— Decreto Ejecutivo nº 37554-JP, de 30 de octubre de 2012, por el que se aprueba el Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Publicado en El Alcance N° 42 a La Gaceta N° 45 de 5 de marzo de 2013).

México

— Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicada en el Diario Oficial de la Federación de 5 de julio de 2010)

— Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicado en el Diario Oficial de la Federación de 21 de Diciembre de 2011)

— Ley de Transparencia y Acceso a la Información Pública Gubernamental (Publicada en el Diario Oficial de la Federación de 11 de Junio de 2002)

Nicaragua

— Ley Nº. 787, de 21 de marzo de 2012, de Protección de Datos Personales (Publicada en La Gaceta Nº. 61 de 29 de marzo)

Paraguay

— Ley Nº 1682, de 16 de enero de 2001, que Reglamenta la Información de Carácter Privado

Perú

— Ley Nº 29733 de Protección de Datos Personales (Publicada en el Diario Oficial El Peruano Nº 445745, de 3 de julio de 2011)

República Dominicana

— Ley Orgánica 172-13, sobre Protección de Datos de Carácter Personal (Promulgada por el Poder Ejecutivo el 13 de diciembre de 2013

Uruguay

— Ley Nº 18.331 de Protección de Datos Personales y Acción de "Habeas Data" (Publicada en el Diario Oficial Nº 27549, de 28 de agosto de 2008).

Cabe destacar que la mayoría de las leyes generales de protección de datos responden a un esquema muy semejante: se regulan los conceptos de protección de datos (dato personal, tratamiento, base de datos…), los principios de protección de datos (información o transparencia, calidad del dato, finalidad, seguridad, consentimiento…), los llamados derechos ARCO (acceso, rectificación, cancelación y oposición) las relaciones entre responsable y encargado, las transferencias internacionales de datos, los esquemas de autorregulación, la autoridad de protección de datos, los procedimientos y el régimen sancionador. Evidentemente cada ley tiene peculiaridades propias, pero, como decimos, responden a esquemas semejantes. Sin embargo, por ahora sólo Argentina y Uruguay han obtenido lo que se conoce como Decisión de Adecuación en materia de protección de datos, aprobada por la Unión Europea. En efecto, respecto a Argentina debe tenerse en cuenta Decisión de la Comisión de las Comunidades Europeas C(2003) 1731 de 30/06/2003 sobre la adecuación de la protección de los datos personales en Argentina, mientras que en relación con Uruguay debe tenerse en cuenta la Decisión de Ejecución de la Comisión 2012/484/UE, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales.

No obstante, no nos referiremos a todos los países de América Latina en lo que se refiere al desarrollo del *cloud computing*, sino sólo a los que consideramos más representativos.

5.4.1. Colombia

Colombia cuenta con un marco sólido en materia de protección de datos[145]. Como acabamos de señalar, destaca la Ley Estatutaria 1581 de 2012, por la que se dictan disposiciones generales para la protección de datos personales[146]. Pese a que no se regula específicamente el tratamiento de datos en la nube, los principios que la ley recoge son perfectamente aplicables al *cloud computing*. Tales principios son: legalidad, información (transparencia), libertad (autorización, consentimiento), finalidad, veracidad o calidad, acceso y circulación restringida, seguridad, confidencialidad y vigilancia o control independiente. La autoridad de protección de datos es la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio[147].

Asimismo, Colombia está fomentando el desarrollo del *Cloud Computing*[148]. El Plan Nacional de Tecnologías de la Información y las Comunicaciones[149] es la estrategia nacional para la utilización de TIC cuyo objetivo está orientado a contribuir en el fortalecimiento de las políticas de inclusión y aumentar la competitividad del país. El plan propone una serie de políticas, acciones y proyectos de investigación, desarrollo, innovación, competitividad empresarial entre otros.

El *Cloud Computing* genera oportunidades para el mercado colombiano en el proceso de adopción de la nube para grandes organizaciones: mayor agilidad para responder a las condiciones del mercado, permite a las organizaciones centrarse en su negocio

---

[145] Vid. Piñar Mañas, *Protección de datos y transparencia en un mundo global*, Presentación Power Point, Universidad de Los Andes, Bogotá, Julio de 2014.

[146] Como hemos visto, desarrollada por el Decreto 1377 de 2013, de 27 de junio, por el cual se reglamenta parcialmente la Ley 1581 de 2012 y Decreto 886 de 13 de mayo de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

[147] http://www.sic.gov.co/drupal/delegatura-para-la-proteccion-de-datos-personales

[148] Cfr. : Ministerio de Comunicaciones de Colombia : « Plan Nacional de Tecnologías de la Información y Telecomunicaciones », en http://www.slideshare.net/ikandlar/plan-nacional-de-tecnologias-de-la-informacin-y-telecomunicaciones

[149] Cfr. : http://www.colciencias.gov.co/programas_estrategias. Cfr. : « Plan Nacional de Ciencia, Tecnologia e Innovacion para el desarrollo de los sectores ELECTRÓNICA, TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (ETIC)
http://www.fiti.gov.co/Images/Recursos/5_Plan_Nacional_de_CTI.pdf

principal además de brindar la posibilidad de adoptar nuevas tecnologías.

Las oportunidades de mercados para las PYMES colombianas son múltiples, generan un mayor acceso a las últimas tecnologías, costos más bajos de inversión inicial en TI y reducción de costos operativos. El *Cloud computing* presenta desafíos regulatorios que nos obligan a repensar conceptos de privacidad, por ello es necesario establecer estrategias de mercadeo que incluyan campañas de sensibilización acerca de las oportunidades y beneficios del *Cloud Computing* como una solución para mejorar la competitividad de las empresas, educar a los usuarios y fomentar el interés, la participación y el uso del *Cloud computing* en Colombia.

5.4.2. Argentina

Argentina se ubica en el puesto 16° de los analizados en el estudio de BSA[150] elevando su posición en el ranking debido a su compromiso con el desarrollo del sector informático, telecomunicación y con la actualización de leyes que benefician la computación en nube[151]. Algunas de las principales conclusiones del estudio indican que, si bien no ha habido grandes cambios entre los resultados de Argentina y los informes del 2012 y 2013, el ranking ubica al país un puesto por debajo del año anterior. Las políticas de todas las naciones afectan el mercado global en nube. Es imprescindible que Argentina se empeñe en concretar mejorías con el fin de perfeccionar mucho más su posición y estimular el crecimiento de nube global. A pesar de su descenso en el ranking, Argentina registró desarrollos en el sector de informática y telecomunicación y actualizó normativas que son beneficiosas para la computación en nube. Por ejemplo, leyes efectivas contra delito digital, firmas digitales y protección de datos ya están en aplicación, aunque la implementación y la fiscalización de normas de protección de datos sean limitadas. En particular, cabe reseñar que

[150] http://cloudscorecard.bsa.org/2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf, cit.

[151] Cfr.: DERGARABEDIAN, Cesar. "Argentina, con malas notas en el ranking de la "cloud computing" 25 de marzo de 2.013. http://www.iprofesional.com/notas/157190-Argentina-con-malas-notas-en-el-ranking-de-la-cloud-computing

Argentina cuenta con la primera Ley general de protección de datos aprobada en América Latina: se trata de la Ley 25.326, sancionada el 4 de octubre de 2000.

La Ley cuenta con unas Disposiciones Generales y a continuación regula los principios generales relativos a la protección de datos, los derechos de los titulares de datos, el régimen de los usuarios y responsables de archivos, registros y bancos de datos, el régimen del control el derecho sancionador y la acción de protección de los datos personales. La autoridad encargada de tutelar el derecho a la protección de datos es la Dirección Nacional de Protección de Datos Personales[152]

Asimismo es de destacar que, como ya hemos señalado más atrás, Argentina ha obtenido por parte de la Unión Europea el reconocimiento de país adecuado en materia de protección de datos[153], lo que sin duda facilita de forma muy considerable el desarrollo del cómputo en la nube. En efecto, al obtener tal reconocimiento (que también se ha otorgado a Uruguay, como asimismo ha quedado apuntado más atrás), resulta mucho más sencillo para las empresas argentinas ofrecer servicios de *cloud computing* a clientes europeos y al mismo tiempo las empresas europeas que ofrezcan servicios de *cloud* pueden ubicar sus servidores en Argentina sin que para ello sea necesaria la previa autorización de las autoridades europeas de protección de datos en cuanto a la transferencia internacional de datos que tales servicios puedan suponer. Por ello, se recomienda vivamente que México alcance el reconocimiento europeo de país adecuado a efectos de protección de datos, pues ello incrementaría sin duda las posibilidades de negocio al reducir los riesgos derivados del posible incumplimiento de la normatividad europea sobre protección de datos.

En lo que refiere a propiedad intelectual, la reglamentación no ha acompañado a la tecnología moderna, según la BSA. No existe

[152] http://www.jus.gob.ar/datos-personales.aspx

[153] Comisión de las Comunidades Europeas. Decisión C(2003) 1731 de 30/06/2003 sobre la adecuación de la protección de los datos personales en Argentina.

cobertura directa para asuntos tales como la "disponibilidad" on-line no autorizada de material protegido por derecho de autor.

5.4.3. Chile[154]

Chile carece de una Ley de protección de datos que responda a los estándares de las actuales leyes latinoamericanas sobre la materia. Destaca en cualquier caso la Ley 19.628 , del 28 de agosto de 1999 sobre Protección a la Vida Privada, modificada en 2002[155], 2010[156], 2011[157] y 2012[158], y que ha sido desarrollada por el Decreto 779/2000, por el que se regula el Registro de Bancos de Datos Personales a Cargo de los Organismos Públicos.

Asimismo puede hacerse referencia a la Ley 19946, de 7 de febrero de 1997, que Establece Normas sobre Protección de los Derechos de los Consumidores.

No existe, por tanto, una normatividad específica sobre *cloud computing* si bien son de aplicación principios de protección de datos y de protección de los consumidores semejantes a los de otros países.

No obstante, el Gobierno de Chile acaba de hacer público un "Ante proyecto de Ley Protección de las Personas del Tratamiento de Datos Personales"[159] que ha sometido a consulta pública[160], y que se

---

[154] Cfr. : « Generalidades de los servicios de Cloud computing en Chile ». http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CDIQFjAC&url=http%3A%2F%2Fwww.accenture.com%2Fcl-es%2FPages%2Fservice-technology-cloud-computing-overview.aspx&ei=TsSlU-vMC8a60QW3iIHgDw&usg=AFQjCNHrQPm791ryilkwbkoM2uGkzBH_aQ&bvm=bv.69411363,d.bGQ

[155] Ley 19.812, de 13 de junio, de 2002.

[156] Ley 20.463, de 25 de octubre de 2010

[157] Ley 20.521, de 23 de julio de 2011

[158] Ley 20.575, de 17 de febrero de 2012

[159] http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de. Según se afirma en dicha dirección Web:

"El Proyecto de Ley da forma a un Sistema de Protección de Datos sustentado en el derecho de las personas de controlar y proteger su información, de manera de evitar que sus derechos sean afectados por el tratamiento de datos.

El Ante Proyecto recoge la experiencia y la discusión nacional que se ha dado en el Congreso Nacional y en los Tribunales de Justicia, de manera de dar un salto en el estándar de protección de

adapta a los estándares internacionales sobre protección de datos, si bien no hay una regulación específica del cómputo en la nube.

Cabe destacar que en Chile se estima que los servicios de *outsourcing* basados en Cloud por proveedores con data center local, continuarán creciendo y aumentando en variedad, de acuerdo al informe "Predicciones IDC 2013 Oportunidad para Innovar". La capacidad de los sistemas de almacenamiento creció sobre el 60% en 2012, superando los 18 Petabytes. En este último punto es en el que precisamente el *Cloud computing* ofrece mayores ventajas para quienes lo utilizan, gracias a la flexibilidad y rapidez con que escala, así como también los ahorros que generan este tipo de arquitecturas[161].

Por todo lo anterior, se puede afirmar que el *Cloud computing* se está convirtiendo en Chile en el aliado estratégico de numerosas medianas y grandes empresas de todos los sectores de la economía.

5.4.4. Brasil

El gobierno brasileño ha lanzado su propia plataforma en la nube, que incluirá software como servicio, para las diferentes municipalidades del país, como parte de una renovación de los servicios públicos. La medida también ha sido vista por algunos como una forma de evitar el

---

los derechos de las personas, adaptando a Chile a las exigencias que el concierto internacional nos exige para mantenernos integrados, pero sin dejar de considerar la tradición jurídica de Chile.
Para la elaboración del Proyecto de Ley se tuvo en consideración el estándar que internacionalmente se ha ido configurando y que se encuentra reflejado en la "Resolución de Madrid", la Directiva 45/96 de la Unión Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, las Directrices de la OCDE relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, la Ley Orgánica 15/1999 de España de Protección de Datos Personales, la Ley Estatutaria de Colombia Nº 1581 por el cual se dictan disposiciones generales para la protección de datos personales, la Ley Nº 8968 de Costa Rica de Protección de la persona frente al tratamiento de sus datos personales y la Ley 18.331 de Uruguay sobre protección de datos personales. Adicionalmente, se consideró el texto del Reglamento de la Unión Europea que está en revisión".

[160] Fecha de Inicio:25 de Julio 2014 Fecha de Término: 15 de Agosto 2014

[161] Cfr.: AETECNO. «Chile continua siendo lider en Cloud computing ». 29 de agosto de 2012. http://tecno.americaeconomia.com/noticias/chile-continua-siendo-lider-en-cloud-computing

espionaje de Estados Unidos al país, alojando la información en servidores locales y dejando de depender de servicios externos.[162]

Del mismo modo las ventas de servicios de Cloud computing en Brasil seguirá siendo fuerte, creciendo a una tasa compuesta anual del 74,3% en los próximos tres años según pronostica la consultora IDC hasta llegar a unas ventas anuales de 798 millones de dólares en el año 2015[163].

En 2012, las ventas de soluciones en la nube crecieron un 68,4%, mientas que en 2011 lo habían hecho en un 57%. No obstante, debido a las particularidades y el nivel de madurez del mercado local, con respecto a la tecnología, algunos de los servicios basados en la nube se prevé que crezcan más que otros.

Tal es el caso de la infraestructura-como-un-servicio (IaaS). De los 257 millones de dólares invertidos en la nube en 2013, las estimaciones son que la mayoría (123 millones de dolares) se han destinado a soluciones de IaaS.

IaaS es la parte más visible de la nube para empresas de Brasil, y también en la Región, debido a los crecientes procesos de virtualización y el aumento de los servicios de centro de datos. Debe tenerse en cuenta también las exenciones fiscales para la infraestructura de telecomunicaciones, que incluye los centros de datos, lo que debe proporcionar otro impulso al mercado.

En cualquier caso, es muy importante destacar la reciente aprobación en Brasil del llamado “Marco Civil de Internet”, por el que se regulan los derechos de los usuarios de Internet.

---

[162] Cfr.: « El Gobierno Brasileño crea su propia plataforma en la nube para evitar el espionaje de Estados Unidos ». *Revista Cloud computing*. 23 de septiembre de 2.013. http://www.revistacloudcomputing.com/2013/09/el-gobierno-brasileno-crea-su-propia-plataforma-en-la-nube-para-evitar-el-espionaje-de-estados-unidos/#sthash.Ue2xahxZ.dpuf

[163] Cfr.: OZORES, Pedro. « Brazil cloud computing sales to grow 74.3% over next three years – IDC”. 13 de marzo de 2013. http://www.bnamericas.com/news/technology/brazil-cloud-computing-sales-to-grow-743-over-next-three-years-idc

El nuevo Marco Civil de Internet, aprobado el 23 de abril de 2014, constituye una especie de "Constitución" para los usuarios de Internet y se ha aprobado con la idea, incluso, de inspirar la adopción de normas similares a nivel mundial[164].

Entre otras cosas, la norma obliga a las empresas extranjeras de Internet a aplicar la normatividad brasileña, incluso en los casos en los que no estén instaladas en el país.

También obliga a los proveedores de Internet a respetar la inviolabilidad de las comunicaciones de los usuarios y les prohíbe suministrar a terceras personas o empresas informaciones sobre sus clientes.

También establece el principio de "neutralidad de la red", una medida que implica que los prestadores de conexión deben garantizar a sus clientes la velocidad contratada, independientemente del contenido al que estos accedan. En particular, el artículo 9 del Marco Civil dispone en su párrafo primero que *"O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".* Asimismo señala en su último párrafo que "*Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo*".

[164] En este sentido, el pasado día 16 de junio de 2014 tuvo lugar en la *Camera dei Diputati* de Roma un Congreso Internacional sobre *Towards an Internet Bill of Rights?* en el que se analizó el Marco Civil como referente a nivel mundial en la regulación de Internet y la privacidad. En dico Congreso participó como ponente uno de los autores de este estudio, el Prof. Dr. José Luis Piñar.

6. Las partes interesadas en las relaciones jurídicas de la computación en la nube. Especial referencia al prestador y al usuario de los servicios

En el marco de los servicios de cómputo en la nube debemos tener en cuenta como partes interesadas el usuario y el prestador del servicio. Asimismo es muy usual que el prestador subcontrate con un subcontratista la prestación de algunas partes del servicio.

Desde la perspectiva de la protección de datos de carácter personal las partes interesadas en las relaciones de cómputo en la nube tienen la siguiente naturaleza:

- El usuario tiene la consideración de responsable del tratamiento.
- El prestador del servicio tiene la consideración de encargado del tratamiento.
- El subcontratista tiene la consideración de subencargado del tratamiento.

6.1. Prestador de servicios de cómputo en la nube

El art. 3 IX de la Ley define Encargado como “La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable”.

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

El artículo 50 fija las obligaciones del encargado:

“El encargado tendrá las siguientes obligaciones respecto del

tratamiento que realice por cuenta del responsable:

I. Tratar únicamente los datos personales conforme a las instrucciones del responsable;

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables[165]*;*

IV. Guardar confidencialidad respecto de los datos personales tratados[166]*;*

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

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

Asimismo el artículo añade que "*los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente*".

La relación entre el usuario y el prestador del servicio de *cloud* requiere, obviamente, la remisión de datos personales desde el primero al segundo. Pues bien, según el artículo 53 del Reglamento
"Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento".

[165] Como sabemos, deben tenerse en cuenta el artículo 19 de la LFPDPPP y el Capítulo III del Reglamento.
[166] Véase, como sabemos, el artículo 21 de la Ley.

En cuanto a la formalización de la relación entre el responsable y el encargado (así como entre el encargado y el subencargado), ya sabemos que el artículo 51 del Reglamento dispone que "La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido". Ya hemos analizado más atrás el alcance de esa relación contractual, sobre todo a partir del contenido del artículo 52 y a lo que ya hemos dicho nos remitimos. Lo que si es necesario destacar es que la relación entre responsable y encargado, es decir entre el usuario de *cloud* y el prestador de servicios de cómputo en la nube, es necesario que se formalice un instrumento jurídico (por regla general un contrato) de modo que sea posible "acreditar su existencia, alcance y contenido". No son admisible, por tanto, ni contrataciones no formalizadas (por ejemplo verbalmente) ni otro tipo de relación que no permita dejar constancia de los extremos que exige el artículo 51.

En caso de que falte esa constancia documental, las consecuencias pueden ser graves. Por ejemplo, podrá considerarse que no existe una relación entre un responsable y un encargado, sino entre dos responsables (el usuario y el prestador del servicio) lo que requerirá todas las exigencias que establece la Ley y el Reglamento para legitimar la transferencia de datos entre dos responsables. En este sentido, el artículo 68 del Reglamento dispone que "Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 37 de la Ley[167]; deberá ser informada a este

[167] El citado artículo 37 dispone:

Artículo 37.- Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

último mediante el aviso de privacidad y limitarse a la finalidad que la justifique". Por su parte, el artículo 69 del Reglamento dispone que "Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realizó conforme a lo que establece la Ley y el presente Reglamento la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales".

Del mismo modo, según el artículo 53 del Reglamento:

> "*El encargado, será considerado responsable con las obligaciones propias de éste, cuando:*
> *I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o*
> *II. Efectúe una transferencia, incumpliendo las instrucciones del responsable.*

El mismo precepto añade que el encargado, es decir, en nuestro caso el prestador de servicios de cloud, "*no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable conforme a lo previsto en el presente Reglamento".*

Hemos señalado en reiteradas ocasiones que en la prestación de servicios de *Cloud computing* es usual que el prestador subcontrate algunas partes del servicio. Lo que da lugar a la figura de la subcontratación. Dicha posibilidad se prevé expresamente, y con carácter general, en el Reglamento, en los términos que recogen los artículos 54 y 55:

VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Véanse asimismo el artículo 44 de la Ley y los artículos 17, 78 a 74, 79 a 86 y transitorio quinto del Reglamento.

Subcontratación de servicios. Artículo 54.

Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último.

Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.

La persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado en la Ley, el presente Reglamento y demás disposiciones aplicables[168]*.*

La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.

Autorización de la subcontratación. Artículo 55.

Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el artículo anterior se entenderá como otorgada a través de lo estipulado en éstos.

En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos a los que refiere el párrafo anterior, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

En ambos casos, se deberá observar lo previsto en el artículo anterior.

[168] Véase el artículo 50 del Reglamento.

6.2. Usuario: sector privado y público

Según el artículo 3 XIV de la LFPDPPP, Responsable es la "Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales". Pues bien, como ya hemos reiterado a lo largo de este documento, los usuarios de servicios de *cloud* tienen la consideración, a efectos de la legislación de protección de datos, de responsables de la base de datos o del tratamiento.

También hemos reiterado que el usuario puede ser tanto una persona (física o moral) privada como pública. En efecto, son cada vez más los sujetos públicos que optan por el *Cloud computing* por múltiples motivos, algunos de los cuales han sido también puestos de manifiesto en este documento.

En lo que se refiere al sujeto privado, es de aplicación lo establecido tanto en la LFPDPPP como en su Reglamento. A los sujetos públicos, sin embargo, les será de aplicación lo establecido por la Ley de Ley de Transparencia y Acceso a la Información Pública Gubernamental de 2002[169] y las normas estatales de transparencia y acceso a la información pública, en lo que, tanto en una como en otras, regulen los aspectos de la protección de datos de carácter personal. Asimismo deberán tenerse en cuenta los Lineamientos de Protección de Datos Personales aprobados por el IFAI[170].

En lo que a la Ley Federal de Protección de Datos, ha de partirse de la exigencia contenida en su artículo 6: "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley". Tales principios son regulados en los artículos 7 a 21 de la Ley y en los artículos 9 a 56 del Reglamento. Por supuesto, deberá respetar e implementar las medidas de seguridad que sean exigibles, en los términos que ya conocemos.

---

[169] Diario Oficial de la Federación de 11 de Junio de 2002.
[170] Publicados en el Diario Oficial de la Federación de 30 de Septiembre de 2005.

Por otra parte, el usuario (y el prestador del servicio de cómputo en la nube), deberán respetar, en su caso, la legislación sectorial que sea de aplicación. Por ejemplo, en el caso de tratamiento de datos de salud, deberá tenerse en cuenta Ley General de Salud[171] y la Norma Oficial Mexicana NOM-024-SSA3-2010, Que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud[172], así como la Norma Oficial Mexicana NOM-168-SSA1-1998, del Expediente Clínico[173].

Por su parte, la Ley de Transparencia y Acceso a la Información Pública recoge en sus artículos 20 a 26 el régimen de la protección de datos a que están sometidos los sujetos obligados.

En particular, el artículo 20 dispone que Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los

[171] Publicada en el Diario Oficial de la Federación de 7 de Febrero de 1984; última reforma publicada en el Diario Oficial de la Federación de 30 de Enero de 2012.
[172] Diario Oficial de la Federación de 8 de Septiembre de 2010
[173] Diario Oficial de la Federación de 30 de Septiembre de 1999.

lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado[174].

El artículo 21 establece que "Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información". No obstante, el artículo 22 dispone que no se requerirá el consentimiento de los individuos para proporcionar los datos personales, entre otros casos, "V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido"[175]. Este es precisamente el caso del cómputo en la nube, en el que, como sabemos, se contrata la prestación de un servicio (precisamente el de *cloud computing*) que implica el tratamiento de datos personales.

---

[174] Véase el Capítulo V, De la Seguridad de los Sistemas de Datos Personales, apartados vigésimo séptimo a trigésimo octavo, de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación de 30 de Septiembre de 2005

[175] Los demás casos son:

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

y

VI. En los demás casos que establezcan las leyes.

Distinto es el tema de la contratación del servicio. Pues dadas las características de la contratación de los sujetos obligados (sujetos públicos) deberán observarse las exigencias materiales y procedimentales de las licitaciones públicas y en este sentido parece lógico que no será posible acudir a fórmulas de contratos de adhesión o de cláusulas generales de la contratación. Sin embargo, entendemos que por analogía deben tenerse en cuenta todas las cautelas y exigencias que recoge el artículo 52 del RLFPDPPP.

7. La generación de confianza mediante el cómputo en la nube en todos los sectores

A la vista de las cuestiones expuestas hasta este momento, debemos hacer una referencia concreta a la generación de la debida confianza que se deriva de la computación en la nube, mediante el análisis de los beneficios directos que proporciona el *Cloud Computing*.

Una adecuada gestión de las tecnologías de la información y de la comunicación implica facilitar los flujos de información a los efectos de apoyar los procesos de negocio, brindar nuevas oportunidades o aumentar la eficiencia de los actualmente en curso.

Para prestar estos servicios con los niveles de calidad adecuados se necesitan habilidades, métodos y herramientas que faciliten precisamente el gobierno y la gestión de dicha tecnología. Sólo de esta manera es posible mejorar los resultados, la productividad, y la eficiencia. Es necesario, en este orden de cosas racionalizar y optimizar los recursos y costes. Esta adecuada gestión permite a las empresas acceder a nuevos mercados, les facilita nuevas oportunidades y formas de estar en contacto con sus clientes reales o potenciales, y, desde luego, les permite conseguir ahorros y eficiencias en sus procesos actuales, lo que les hace ser mucho más competitivas.

Las empresas[176] (y los sujetos públicos, sin perjuicio de sus especialidades) que apuestan por la implementación de modelos tecnológicos basados en *Cloud Computing* adquieren un conjunto de ventajas operacionales inmediatas en el despliegue y consumo de los servicios tecnológicos necesarios para su negocio:

a) La eficiencia en costes (se puede llegar a lograr un ahorro del 50% de costes tecnológicos respecto del modelo tradicional).
b) El ajuste de la inversión.
c) La agilidad en el despliegue de nuevos procesos, productos y servicios, y;
d) La focalización de los recursos en los procesos de valor de la compañía.

Aunque con carácter general la integración de servicios de *Cloud computing*, implica el desarrollo de todas estas ventajas y oportunidades para la competitividad de las empresas, son las áreas de tecnología las que asumen el mayor impacto, beneficios y riesgos con la adopción de este modelo. Una organización de servicios TIC, centrada en sus clientes, se tiene que caracterizar por una estrecha colaboración, al menos durante todas las fases del ciclo de vida del servicio, que debe hacerse en colaboración muy próxima con el cliente, teniendo en cuenta las necesidades del negocio. Cuanto más estrecha sea esa colaboración, cuanto más centrado esté el proveedor en el hecho de satisfacer las demandas del negocio del cliente, más posibilidades de éxito habrá para el cliente y también, lógicamente, para el propio proveedor de tales servicios[177] en la nube.

La informática en la nube constituye un nuevo enfoque de las tecnologías de la información porque las empresas pueden disponer de la tecnología de forma escalable y como servicio, cuando realmente lo necesitan. Esto acelera el "*time-to-market*", o paralización de procesos. Si un proceso requiere un uso computacional alto, con intensos trabajos de manejo de datos que toman mucho tiempo, es posible vivir

[176]Según el studio realizado por Deloitte en el año 2010 "*What Cloud Computing means for business, and how to capitalize on it".*
[177] Vid. "Servicios TIC centrados en los clientes ". En A+ número 23. Junio 2008.

en varios procesos y ejecutarlos paralelamente con muchas unidades de procesamiento, a los efectos de ponderar reducir el tiempo total de procesamiento a sólo una fracción del tiempo original.

Con la elasticidad[178] del sistema es posible pagar por esta gran cantidad del cómputo sólo en el momento en que la misma se requiere, reduciendo los tiempos de desarrollo de los productos, por ejemplo, dando la ventaja competitiva al negocio. Este nuevo enfoque de las tecnologías de la información puede implicar también el hecho de eliminar los obstáculos de acceso tradicionales, y permite a las empresas aprovechar nuevas oportunidades de mercado. Y todo ello tendrá un profundo impacto sobre la propia estructura del mercado de muchos sectores a medida que la competencia aumente y, en consecuencia, sobre el rendimiento macroeconómico global. Además de aprovechar las oportunidades de creación de negocio, las organizaciones también pueden reducir sus costos de forma drástica mediante esta tecnología.

En este mismo sentido, cabe afirmar que las organizaciones, incluidas los sujetos públicos, pueden utilizar los servicios en la nube para reemplazar sucesivamente los centros de datos de los departamentos de tecnologías de información y comunicación (TIC) gestionados de forma interna. Las empresas pueden utilizar los servicios en la nube para hacer pruebas y expandir rápidamente lo que ofrecen a sus clientes, porque pueden hacerlo sin tener que crear infraestructuras físicas, ni tampoco invertir en ellas.

Gracias a la homogeneización de las interfaces (el equivalente a las tomas eléctricas) los usuarios pueden dejar que se ocupen de los detalles (cómo crear, hacer funcionar y proteger un centro de datos) expertos que al dar servicios a muchos usuarios consiguen economías

[178] La elasticidad de la computación en nube se refiere a la capacidad de un proveedor o una aplicación para crecer y reducir la cantidad de la infraestructura de TI, según sea necesario para satisfacer la demanda. La elasticidad se considera una característica clave nube, ya que reduce la necesidad de una organización para llevar la capacidad de sobrecarga o de repuesto.http://searchdatacenter.techtarget.com/es/cronica/Computacion-de-almacenamiento-en-las-nubes-desde-A-hasta-Z

de escala mucho mejores que las que conseguirían los usuarios individuales. Además, los servicios en la nube ofrecen economías de escala de gran tamaño, lo que significa que es improbable que hacer esfuerzos en solitario a nivel nacional pueda ofrecer la eficiencia óptima en función de los costes.

Además, el aumento sin precedentes del flujo de datos y del procesamiento de la información a través de Internet tiene un impacto medio ambiental importante en cuanto a consumo de agua y de energía, así como en lo que se refiere a las emisiones de gases de efecto invernadero. El cómputo en la nube puede contribuir a mitigar estos problemas gracias al uso más eficiente del hardware y, más específicamente, mediante la construcción de centros de datos que utilizan servidores de bajo consumo energético y energía no contaminante.

Por consiguiente, cabe esperar mejoras de eficiencia sustanciales en todos los sectores económicos si las empresas y otras organizaciones, en especial las PYMES, adoptan el cómputo en la nube. Esta tecnología también podría ser especialmente importante para las pequeñas empresas con dificultadas económicas o ubicadas en regiones rurales y remotas, pues podrían entrar en mercados de otras regiones más desarrolladas. Asimismo, la nube puede dar empleo a trabajadores con conocimientos de TIC en vez de desarraigarlos en busca de un puesto de trabajo y, por consiguiente, puede llevar trabajo y dinero a regiones menos favorecidas.

Es importante señalar que actualmente existen distintas nubes creadas por empresas pero que carecen de interoperabilidad entre ellas. En otras palabras, no hay estándares que permitan la comunicación entre las distintas nubes. Bajo esta premisa, el *"*Cloud Computing*"* se convierte en fungible, es decir, que una nube puede ser fácilmente sustituida por otra y la información trasladada de un lugar a otro. Para ello se propone lograr la portabilidad de datos y aplicaciones, establecer un servicio de seguridad federado y promover unos modelos comunes deinterfaces, semántica y programación. Si esto no se logra es posible que los gobiernos intervengan a la fuerza para regular la

nube. Dado el breve recorrido del "Cloud Computing" hasta ahora, se corre el riesgo de que unos estándares más restrictivos puedan perjudicar la innovación.

A los efectos de ordenar adecuadamente el régimen jurídico del "Cloud Computing", la Comisión Europea propone una serie de áreas clave en las que es preciso tomar decisiones a los efectos de garantizar la seguridad jurídica en su funcionamiento. A su vez, el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos ha publicado una serie de documentos entre los que se incluye un conjunto de definiciones ampliamente aceptado. También el Instituto Europeo de Normas de Telecomunicaciones (ETSI) ha establecido un grupo cuya misión es considerar la necesidad de estandarización de la nube y el cumplimiento de las normas de interoperabilidad.

Está claro que serán necesarias iniciativas adicionales para el establecimiento de normas. Sin embargo, ahora la prioridad es utilizar las normas existentes para desarrollar la confianza en la informática en la nube a través de una serie de servicios comparables, así como hacer ofertas diversas con capacidad de interoperabilidad. Además de identificar el cumplimiento de las normas pertinentes es necesaria la certificación. Muchas organizaciones, y sin duda todas las de mayor tamaño, requieren la certificación del cumplimiento de sus sistemas informáticos con los requisitos legales y de auditoría, y requieren además que esas aplicaciones y sistemas sean interoperables.

La generación de confianza en el cómputo en la nube será más notable si va acompañado de un marco regulatorio adecuado, sobre todo en el ámbito de la protección de datos de carácter personal. En este sentido es importante resaltar que el desarrollo de los servicios de *cloud computing* no resulta obstaculizado por la normatividad en materia de protección de datos. Hemos visto cómo México es considerado como un país propicio para el desarrollo del cómputo en la nube, pese a que cuenta con una regulación ya consolidada en materia de protección de datos de carácter personal. También hemos podido apreciar que en los países de la Unión Europea, donde aplica la Directiva 95/46/CE sobre protección de datos y las normas nacionales

de trasposición de la misma, el desarrollo del cómputo en la nube es notable.

En este sentido, parece muy aconsejable que las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitan cuanto antes los criterios para el debido tratamiento de datos personales en el cómputo en la nube tal como está previsto en el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. En cualquier caso, resulta imprescindible que, aún a falta de esos criterios (y sin olvidar los documentos que ya ha aprobado el IFAI en materia de protección de datos, sobre todo en materia de seguridad), la puesta en marcha de servicios de *cloud* tenga en cuenta desde el principio los requerimientos de la protección de datos, con aplicación de los principios de *pricvacy by design* (o privacidad desde el diseño) y *privacy by default* (privacidad por defecto).

Por otra parte, las principales barreras percibidas por las empresas para la adopción de los servicios en la nube son la falta de confianza y la falta de seguridad. Hay que señalar que el rol de las Instituciones Públicas y la generación de confianza resultarán claves para superar esa percepción y conseguir un desarrollo creciente del cómputo en la nube con pleno respeto a la protección de datos de carácter personal.

III. EL CÓMPUTO EN LA NUBE EN MÉXICO

1. Introducción a la Regulación de *cloud computing* en México

En el marco de la Constitución Política de los Estados Unidos Mexicanos, el uso del cómputo en la nube (*cloud computing*) cobra importancia en la redacción del artículo 6 a partir de la reforma constitucional en materia de telecomunicaciones. En relación con este precepto, cabe destacar dos puntos[179]:

1. **Reforma constitucional en materia de telecomunicaciones[180]:**
   Artículo 6, tercer párrafo: *"El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios."*
   Artículo 6, inciso B, fracción I: *"El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales*".
   * La reforma fomenta el uso del cómputo en la nube porque:
   - Se incrementa el acceso a la banda ancha a través de dos redes mayoristas: una red troncal que utilizará la fibra óptica obscura (propiedad de la Comisión Federal de Electricidad) y una red abierta que proporcionará banda ancha móvil empleando el espectro del dividendo digital[181].

---

[179] Casasola Robles, Mario, Maqueo Ramírez, María Solange, Molina Rodríguez, Marlon, Moreno González, Jimena, Recio Gayo, Miguel (2014), *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo*, CIDE, México.

[180] Véase el Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones. Publicado en el Diario Oficial de la Federación el 11 de junio de 2013 y disponible en la dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_208_11jun13.pdf

[181] Al respecto, tómese en consideración el proyecto México Conectado, del Gobierno de la República, que tiene por objeto contribuir a garantizar el derecho de acceso a Internet de banda ancha en sitios y espacios públicos. Véase más información sobre dicho proyecto en la dirección de Internet http://www.mexicoconectado.gob.mx/

- Se crea un nuevo ente regulador con autonomía constitucional que fortalecerá la capacidad reguladora del sector. Se trata del nuevo Instituto Federal de Telecomunicaciones (IFT)[182].

2. Reforma constitucional en materia de transparencia[183]:

Artículo 6: Otorga autonomía constitucional a los órganos garantes del derecho a la protección de datos personales en posesión de los particulares, tanto a nivel federal como estatal.

A su vez, da nuevas facultades al órgano garante federal con el objeto generar criterios homogéneos en la protección de dicho derecho. Las más importantes son: la posibilidad de atraer recursos de revisión que por su interés y trascendencia nacional así lo ameriten, así como la facultad para revisar las resoluciones de los organismos especializados de los Estados.

Artículo 73, fracción XXIX-S: Otorga al Congreso de la Unión la facultad de emitir una Ley General reglamentaria en materia de protección de datos personales en posesión de los sujetos obligados del sector público para fijar los principios, bases y procedimientos respecto de este derecho.

No obstante lo anterior, para analizar la regulación del cómputo en la nube en México es necesario hacer referencia a los documentos y programas elaborados en el marco de las políticas públicas relacionadas con las Tecnologías de la Información y la Comunicación (TIC) y a los esfuerzos de entes particulares en esta materia[184].

El artículo 26, apartado A, de la Constitución Política de los Estados Unidos Mexicanos faculta al Poder Ejecutivo para organizar un sistema de planeación democrática del desarrollo nacional a través de

[182] Sobre el IFT, puede verse más información en http://www.ift.org.mx/iftweb/

[183] Véase el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. Publicado en el Diario Oficial de la Federación el 7 de febrero de 2014 y disponible en la siguiente dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

[184] En relación con los programas y documentos citados: Téllez Valdés, Julio (2013), *Lex Cloud Computing. Estudio Jurídico del Cómputo en la nube en México*, Universidad Nacional Autónoma de México, México.

un **Plan Nacional de Desarrollo** (en adelante PND), al que deberán sujetarse los programas de la Administración Pública Federal[185].

Conforme con esta regulación y con el objetivo de llevar a México a su máximo potencial, el gobierno actual elaboró el PND 2013-2018, cuyas metas nacionales son: un México en paz, un México incluyente, un México con educación de calidad, un México próspero y un México con responsabilidad global. A su vez, en este documento se presentan estrategias transversales aplicables a todas las políticas públicas que tienen como cometido democratizar la productividad, consolidar un gobierno cercano y moderno, e incorporar la perspectiva de género[186].

Uno de los objetivos de la estrategia que busca alcanzar un gobierno cercano y moderno es establecer un **Programa Digital Nacional** para fomentar la adopción y el desarrollo de las TIC, así como para impulsar un gobierno eficaz que permita insertar al país en la sociedad de la información y del conocimiento[187]. Dicho programa se encuentra a cargo de la Oficina de la Presidencia de la República[188].
Para ello se propone, entre otras cosas:

a) Incrementar el nivel de inversión pública y privada en ciencia y tecnología;
b) Transparentar y hacer eficiente la relación entre la ciudadanía y el gobierno;
c) Eliminar fallas del mercado que pidan a sectores o regiones alcanzar su máximo potencial;

---

[185] El Estado organizará un sistema de planeación democrática del desarrollo nacional que imprima solidez, dinamismo, competitividad, permanencia y equidad al crecimiento de la economía para la independencia y la democratización política, social y cultural de la nación.
[186] El PND 2013-2018 se puede consultar en http://pnd.gob.mx/.
[187] VI.A. Estrategias y líneas de acción transversales: …Gobierno Cercano y Moderno:
• Garantizar el acceso a la información y a la protección de los datos personales, fomentando la rendición de cuentas.
• Establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las tecnologías de la información y la comunicación, e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento.
• Consolidar un gobierno que sea productivo y eficaz en el logro de sus objetivos, mediante una adecuada racionalización de recursos, el reconocimiento del mérito, la reproducción de mejores prácticas y la implementación de sistemas de administración automatizados.
[188] Ver el Reglamento de la Oficina de la Presidencia de la República en http://dof.gob.mx/nota_detalle.php?codigo=5294161&fecha=02/04/2013

d) Identificar y adoptar infraestructura y Tecnologías de la Información para impulsar la productividad y el crecimiento;
e) Impulsar la utilización de las TI para fines educativos y para ampliar el acceso a la cultura;
f) Utilizar la ciencia y la tecnología para el desarrollo del capital humano nacional y para generar productos y servicios con un alto valor agregado;
g) Utilizar las nuevas tecnologías para el acceso al financiamiento de micro, pequeñas y medianas empresas;
h) Impulsar la economía digital y fomentar el desarrollo de habilidades en el uso de las TIC[189].

1.1. Mecanismos del Gobierno para impulsar el desarrollo de TIC

1.1.1. Secretaría de la Función Pública y la Agenda de Gobierno Digital

La Secretaría de la Función Pública (SFP) es una dependencia del Poder Ejecutivo Federal que vigila que los servidores públicos federales se apeguen a la legalidad durante el ejercicio de sus funciones, sanciona a los que no lo hacen, promueve el cumplimiento de los procesos de control y fiscalización del gobierno federal y de disposiciones legales en diversas materias, dirige y determina la política de compras públicas de la Federación, coordina y realiza auditorías sobre el gasto de recursos federales, coordina procesos de desarrollo administrativo, gobierno digital, opera y encabeza el Servicio Profesional de Carrera, coordina la labor de los órganos internos de control en cada dependencia del gobierno federal y evalúa la gestión de las entidades, también a nivel federal[190].

[189] En este contexto, existe un proyecto de Ley para el Desarrollo de la Sociedad de la Información que ya ha sido aprobado por la Cámara de Diputados y que está pendiente de ser discutido en el Senado[189]. Esta norma propone formalizar una Agenda Digital Nacional y crear un sistema nacional para el desarrollo de la sociedad de la información, dirigido por el Presidente de la República y administrado por un secretario ejecutivo.

[190] Página de la Secretaría de la Función Pública
http://www.funcionpublica.gob.mx/index.php/conoce-la-sfp.html

La Secretaría de la Función Pública tiene a su cargo la **Agenda de Gobierno Digital**[191], que tiene por objeto mejorar la eficiencia, la productividad y la transparencia del gobierno mediante el uso de las TIC. A pesar de que no se trata específicamente el tema de *cloud computing* en este documento, se establecen temas relevantes que inciden directamente en su uso. Se propone la utilización de las TIC para facilitar el acceso a la información y a los servicios gubernamentales y el impulso de las buenas prácticas en el uso de dichas tecnologías. Entre estas prácticas se encuentran la homologación de procesos y trámites, tales como firmas y certificados digitales, así como la interoperabilidad entre sistemas de los gobiernos federal, estatales y municipales.

1.1.2. Esquema de Interoperabilidad de Datos Abiertos de la Administración Pública Federal

El **Esquema de Interoperabilidad de Datos Abiertos de la Administración Pública Federal** está dirigido por la Secretaría de la Función Pública[192]. En este documento se señalan las bases, los principios y las políticas que deben seguir las dependencias y entidades de la administración pública federal y la Procuraduría General de la República, para la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar las plataformas y los sistemas de información, con el objeto de incrementar la eficiencia operativa de la administración pública federal y su relación con la sociedad. Cabe señalar que este documento tiene gran importancia para el cómputo en la nube porque trata sobre interoperabilidad, datos abiertos y transparencia de las gestiones gubernamentales.

El artículo segundo, fracción V, define al cómputo en la nube como un *"modelo de prestación de servicios digitales que permite a las instituciones públicas acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como*

[191] http://dof.gob.mx/nota_detalle_popup.php?codigo=5077667
[192] http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011

servicios, de plataforma como servicios y de software como servicios". También, en este precepto, en su fracción XVIII, se define la Interoperabilidad como *"la capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las dependencias y entidades compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicaciones".* Y el mismo precepto, en su fracción XXIV, denomina Portabilidad *"al conjunto de características que permiten la transferencia de la información de un sistema o aplicación a otro. Tratándose de servicios de cómputo en la nube, a la capacidad para trasladar un servicio de un proveedor a otro"*. Por último, otra definición importante a tomar en consideración, es la de neutralidad tecnológica, que, conforme a la fracción XXII, del precepto ya citada, se entiende como *"la opción de elegir la alternativa tecnológica más adecuada a las necesidades de las dependencias y entidades, con el propósito de no excluir, restringir, condicionar o favorecer alguna tecnología o modelo de negocio informático en particular."*

A su vez, en el artículo octavo se establecen obligaciones para las dependencias y entidades tendentes a lograr la Interoperabilidad Técnica[193]. Entre dichos deberes se encuentra *"establecer los términos y condiciones de contratación que garanticen la portabilidad de las soluciones a través del tiempo, especialmente cuando se trate de contrataciones vinculadas a servicios digitales basados en soluciones de cómputo en la nube, en las modalidades de: infraestructura como servicio, plataformas como servicio y software como servicio".*

[193] Definida en la fracción XXI, del artículo segundo, como *"las especificaciones técnicas que garantizan que los componentes tecnológicos de los sistemas de información están preparados para interactuar de manera conjunta".*

1.1.3. Secretaría de Comunicaciones y Transportes y la Agenda Digital del Sistema Nacional e-México 2010-2015

La Secretaría de Comunicaciones y Transportes (SCT) tiene como misión promover sistemas de transporte y comunicaciones seguros, eficientes y competitivos, mediante el fortalecimiento del marco jurídico, la definición de políticas públicas y el diseño de estrategias que contribuyan al crecimiento sostenido de la economía y el desarrollo social equilibrado del país, ampliando la accesibilidad de los servicios, logrando la integración de los mexicanos y respetando el medio ambiente[194].

La **Agenda Digital del Sistema Nacional e-México 2010-2015** está a cargo de esta entidad y busca impulsar un proceso de adopción tecnológica en el país que impacte en la competitividad, en el desarrollo social y humano y en el empoderamiento de los ciudadanos, con el objeto de que el país evolucione hacia la sociedad de la información y el conocimiento[195].

Los objetivos estratégicos son tres: a) eliminar la brecha que separa a los ciudadanos con acceso y sin acceso a las TIC; b) universalizar la conectividad institucional y comunitaria de banda ancha para alcanzar una cobertura integral, principalmente en zonas marginadas; y c) aumentar la disponibilidad y la relevancia de contenidos, aplicaciones y servicios en línea de alto impacto social y gubernamental. Para alcanzar estas metas se han diseñado tres programas:

1. Plataforma Tecnológica del Sistema Nacional e-México, la cual busca implantar un modelo de e-infraestructura.

---

[194] Misión de la Secretaría de Comunicaciones y Transporte, portal http://www.sct.gob.mx/

[195]http://www3.diputados.gob.mx/camara/content/download/242550/688896/file/Agenda%20Digital%20eMexico%20Camara%20de%20Diputados%20V5.6.pptx

Los objetivos de este documento corresponden a compromisos internacionales adquiridos en el marco de los Objetivos del Milenio de la ONU (2000), así como en la Cumbre Mundial de la Sociedad de la Información (2003 y 2005).

2. Focos de producción e-México, que tienen por objeto generar un sistema nacional de producción y entrega de servicios, contenidos y aplicaciones digitales.
3. Campaña Nacional de Inclusión Digital Vasconcelos 2.0, para erradicar la brecha que existe entre todos los ciudadanos para la apropiación tecnológica.

1.1.4. Estrategia Digital Nacional

La Estrategia Digital Nacional[196] (EDN) es el plan de acción que el Gobierno de la República implementará durante los próximos 5 años para fomentar la adopción y el desarrollo de las Tecnologías de la Información y la Comunicación. El propósito fundamental es lograr un "México Digital" en el que la adopción y uso de las tecnologías maximicen su impacto económico y social en beneficio de la calidad de vida de todos. Tiene principalmente 5 objetivos:

a) Transformación gubernamental. Además de otras metas, se pretende generar y coordinar acciones orientadas hacia el logro de un gobierno abierto, instrumentar la ventanilla única nacional para trámites y servicios; instrumentar una política digital de gestión del territorio nacional; crear una política de TIC sustentable para la APF; usar datos para el desarrollo y el mejoramiento de políticas públicas; adoptar una comunicación digital centrada en el ciudadano.
b) Economía Digital. Entre otras cosas, se pretende desarrollar el mercado de bienes y servicios digitales; potenciar el desarrollo del comercio electrónico; estimular la innovación de servicios digitales a través de la democratización del gasto público y asegurar la inclusión financiera mediante esquemas de banca móvil.
c) Educación de Calidad. Se pretende desarrollar una política nacional de adopción y uso de las TIC en el proceso de enseñanza-aprendizaje del Sistema Educativo Nacional; ampliar

[196] La página principal de la Estrategia se encuentra dentro de la página de la presidencia de la República: http://www.presidencia.gob.mx/edn/

la oferta educativa a través de medios digitales; mejorar la gestión educativa mediante el uso de las TIC; y desarrollar una agenda digital de cultura.

d) Salud Universal y Efectiva. Se va a incorporar el uso de las TIC para facilitar la convergencia de los sistemas de salud y aumentar la cobertura de los servicios de salud; establecer la personalidad única en salud a través del padrón general de salud; implementar el Expediente clínico electrónico, el certificado electrónico de nacimiento, la cartilla de vacunación; implementar sistemas de información del Registro electrónico para la salud; instrumentar mecanismos de Telesalud y Telemedicina[197].
e) Seguridad Ciudadana. Para generar herramientas y aplicaciones de denuncia ciudadana en múltiples plataformas; desarrollar instrumentos digitales para la prevención social de la violencia; impulsar la innovación cívica por medio de las TIC; prevenir y mitigar los daños causados por desastres naturales mediante el uso de las TIC.

Para cumplir sus objetivos cuenta con ciertos habilitadores:

a) **Conectividad**. El plan implica construir el terreno para las políticas públicas a desarrollar en materia digital, por ejemplo ampliar kilómetros a la red troncal de fibra óptica; el número de operadores móviles virtuales[198] ; se pretende ampliar el número de sitios públicos conectados a internet de banda ancha[199].

   Para las metas planteadas, aún se encuentran en proceso la publicación de los siguientes documentos:

   1) Documento con las Reglas de Operación de la Red Compartida. Se busca fomentar el uso óptimo de bandas de 700MHz y 2.5 GHz, de acceso universal, no discriminatorio, compartido y continuo.

[197] Con esto se refieren a mejorar la calidad de los servicios de salud y facilitar la atención médica a través del desarrollo de técnicas de telesalud y telemedicina

[198] En el momento sólo hay un operador en México, por lo que se pretende fomentar inversiones que amplíen la infraestructura de banda ancha, especialmente en zonas rurales y marginadas, y se promoverán las asociaciones público-privadas para el despliegue, desarrollo y uso eficiente de la infraestructura de conectividad.

[199] Se garantizará el acceso a internet de banda ancha en sitios públicos y se considerará el número potencial de usuarios en cada sitio para satisfacer la demanda, con el objetivo es alcanzar cobertura universal para 2018 en estos sitios.

2) Documento con el Programa Nacional de espectro a corto, mediano y largo plazo, armonizando atribuciones internacionales de espectro.
3) Documento con los lineamientos de la política satelital de largo plazo
4) Documento con la política de IXP. Se busca facilitar la instalación y operación de IXP en México, instalando puntos de intercambio, con el objeto de optimizar el uso de redes troncales y permitir que el transporte del tráfico nacional no utilice cruces transfronterizos.
5) Documento con la Política de transición a IPv6.

b) **Inclusión y habilidades digitales**. Que se cuente con una política que tenga como objetivo cerrar la brecha digital y que los beneficios de la digitalización alcancen a todos los sectores de la población.
c) **Interoperabilidad**. Se quiere lograr que los sistemas que utiliza el Gobierno tengan la capacidad de hablarse entre sí y generar información que pueda ser consultada por el ciudadano en formatos neutrales e interoperables. Para esto se encuentran en proceso los siguientes documentos:
1) Lineamientos y políticas de interoperabilidad, intercambio y validación de la información en poder del Estado.
2) Impulsar la interoperabilidad de los documentos de identificación.
3) Mejorar la experiencia del ciudadano simplificando la relación entre ciudadano y gobierno mediante la interoperabilidad.
d) **Marco jurídico.** Con el objeto de realizar cambios en las leyes que vayan conforme a las políticas públicas a desarrollar en materia digital. En éste ámbito se espera lo siguiente:
1) Publicación de la Política TIC
2) Publicación del Decreto de la Política de Datos Abiertos
3) Publicación del Decreto de Creación de Ventanilla Única
4) Contratos Marco para compra de Tecnología
e) **Datos abiertos.** Para el gobierno de la República los datos abiertos son activos prioritarios para detonar un ecosistema de innovación en colaboración con la ciudadanía para crear valor económico, social y político, a la vez que promueve la

transparencia y rendición de cuentas. Se encuentra en proceso la elaboración del diagnóstico, y una encuesta ciudadana para medir la demanda de la información pública en formatos abiertos. Después de ello se elaborará e implementará la Política de Datos Abiertos, desarrollo de la plataforma única (datos.gob.mx)[200] y establecer acuerdo de colaboración para la publicación de datos abiertos con estados, municipios y órganos autónomos.

En relación con el cómputo en la nube, la EDN hace referencia específicamente a *"privilegiar el cómputo en la nube"*, si bien hace también referencia a continuación a *"Generar acciones para garantizar la Soberanía de datos, como país, y hacia adentro de las organizaciones"* [201] Esta soberanía de datos, en la práctica, puede implicar limitaciones al uso de la tecnología, lo cual podría resultar en perjuicio de las Administraciones Públicas[202].

Existe un Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de Aplicación General en dichas materias. Este Acuerdo, en su artículo 5,

---

[200] Al momento de redactar este documento, esta plataforma se encontraba disponible en versión beta.

[201] Véase esta Línea de Acción en el marco del objetivo secundario relativo a crear una política de TIC sustentable para la Administración Pública Federal. Pág. 19 de la EDN, ya citada, que puede verse en http://cdn.mexicodigital.gob.mx/EstrategiaDigital.pdf

[202] Sobre esta cuestión, puede verse, VV.AA., *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo*, ya citado. En dicho estudio se indica que *"el cómputo en la nube debe ser considerado en un contexto global, por lo que otra de las líneas de acción, la relativa a la soberanía de datos38, debería ser reconsiderada. La soberanía de datos es un concepto que entra claramente en conflicto con otros principios ya que puede ser utilizada para negar la posibilidad de despliegue de tecnologías de la información o servicios proporcionados por prestadores de servicios extranjeros e incluso es una postura que ha sido rechazada a nivel internacional"*. Pág. 24. Y también, como se cita en el documento anterior, el Dr. Julio Téllez, en *Lex Cloud Computing: Estudio Jurídico del Cómputo en la Nube en México,* indica que *"nuestro marco jurídico debe atender, entre otras cosas" "1. Romper con la idea tradicional de soberanía por cuanto hace a la economía digital y el uso de medios electrónicos y de comunicación, como es Internet y el procesamiento de datos, pues los retos implican una nueva comprensión del fenómeno social y la economía, cosa que el derecho no debe limitar, sino armonizar, para su óptimo desarrollo; la protección de los datos o la información de los usuarios no depende del territorio donde estos residan o estén alojados, son del estándar de privacidad y seguridad bajo el cual están protegidos."* Pág. 99.

fracción I, que se refiere al Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETIC) que elaboren las entidades y dependencias de la Administración Pública Federal y demás sujetos obligados, señala que dicho Plan debe *"favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, teniendo en consideración la seguridad de la información"*[203].

Dicho Acuerdo, en su artículo 13 señala que en el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente: […]

II. 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;…

…..

IV. Analizar el alojamiento de su infraestructura de operación 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;

V. Almacenar y administrar en los Centros de Datos que se encuentren en las instalaciones de las Instituciones, los datos considerados de seguridad nacional, seguridad pública e información reservada y confidencial, conforme a la normatividad aplicable;[…]

Además de los servicios de centro de datos, que permiten almacenar y administrar información en los mismos, el Acuerdo también se refiere a la contratación de otros servicios, tales como los de correo electrónico (SaaS) o servicios de plataformas de procesamiento de datos.

Es recomendable que se consulten los "Avances" de ésta Estrategia Nacional, ya que se actualizan regularmente. Éstos se

[203] Ver http://www.normateca.gob.mx/Archivos/66_D_3755_12-05-2014.pdf

pueden encontrar en la página: http://www.presidencia.gob.mx/edn/indicadores/

1.1.5. Secretaría de Economía y PROSOFT 3.0

A grosso modo, la Secretaría de Economía (SE) es la Institución que promueve e instrumenta políticas públicas y programas orientados a crear más y mejores empleos, más y mejores empresas, y más y mejores emprendedores[204].

Como parte de sus funciones han implementado **el Programa para el Desarrollo de la Industria de Software** (PROSOFT). Éste programa apoya la capacitación y certificación, habilitación y equipamiento tecnológico, normas y modelos, adopción y producción de TI, Innovación, comercialización, estudios para desarrollar capacidades de negocio, servicios profesionales diversos, eventos, creación y fortalecimiento de fondos y aceleración de la política pública[205].

El 24 de julio del 2014 se lanzó una nueva convocatoria para **apoyar a empresas mexicanas del sector de tecnologías de información,** está dirigida a empresas o agrupamientos que realizan actividades vinculadas al sector TI: desarrollo de software, servicios de TI, tercerización de proceso de negocio (*Business Process Outsourcing*) y medios creativos digitales. Asimismo, pretende apoyar a empresas para adoptar TI cuando el proveedor sea una de las más de 525 empresas de TI basadas en México que cuentan con una certificación de calidad. Por regla general, un proyecto puede recibir un 25% de apoyo del PROSOFT sobre el valor total del proyecto y ser beneficiario de otro 25% por parte de las entidades federativas que participan en el programa[206].

---

[204] Misión de la Secretaría de Economía: http://www.economia.gob.mx/conoce-la-se/mision-y-vision-se

[205] Lo que apoya el programa PROSOFT, preguntas frecuentes en: http://www.prosoft.economia.gob.mx/preguntas/

[206] Ésta última convocatoria expira el 22 de agosto del 2014, y las bases se encuentran publicadas en la página: www.prosoft.economia.gob.mx.

Actualmente, el PROSOFT está experimentando su tercera evolución (3.0) que busca posicionar a México como un jugador global de servicios de TI con iniciativas y acciones que son prioritarias en la agenda nacional. Los problemas que se enfrentan actualmente son:

a) Más del 50% de las empresas de TI tiene dificultades al contratar personal calificado.
b) Sólo el 25% de las empresas de TI innovan. En general, en el país sólo el 12% de las empresas innova.
c) El gasto en servicios de TI y software en México es 41% menor al de economías desarrolladas. Y Sólo el 1% de los servicios de TI del gobierno se hace con proveedores locales.
d) Sólo el 25% de las empresas del sector de TI exporta y las que lo hacen, el valor de sus exportaciones está entre el 7% y el 27% de sus ventas.
e) De las empresas de Ti que se acercaron a intermediarios financieros, sólo el 23% consiguieron el crédito.
f) La heterogeneidad de los marcos jurídicos locales no favorecen el desarrollo de la innovación de las TI y la reducción de la brecha digital.
g) Se carece de estrategias claras que fomenten la especialización inteligente que diferencia la oferta local no solo a nivel país sino global[207].

[207] PROSOFT 3.0 en la página http://www.prosoft.economia.gob.mx/doc/Agenda%20sectorial%20PROSOFT%203.0.pdf

El programa correrá del 2014 al 2024. La visión y metas[208] son:

VISIÓN 2024	**METAS 2024**
Ser jugador global en exportación	2º país exportador (hoy 3º)
Ser destino outsourcing	3º destino de TI (hoy 6º)
Tener mayor escala de empresas y ventas	Multiplicar por 4 el valor de mercado de TI (hoy 14.4 BUSD)
Ampliar la densidad de uso de TI	3º en LATAM en uso de TI empresarial (hoy 5º)
Contar con centros de desarrollo certificados con calidad suprema	1,000 centros de calidad (hoy 527)
Facilitar el encadenamiento cercano con otros sectores	Acercamiento a 15 sectores
Contar con talento de excelencia de fácil acceso	90% de demanda de talento cubierta (hoy 50%)
Facilitar innovación con TI y en TI	50% de empresas de TI innovan (hoy 25%)
Mayor valor agregado en el sector	25% de valor agregado de servicios (hoy 9.4%)
Mantener una intensa vinculación con la academia	30% con proyectos vinculados (hoy 5%)
Tener acceso a capital emprendedor y fondeo	50% de empresas obtienen créditos (hoy 23%)
Contar con especialización diferenciada país	5 polos globales de TI en el país (hoy 0)
Mantener estrecha colaboración del ecosistema	Planeaciones estratégicas anuales
Contar con marco normativo de vanguardia	Líder LATAM en leyes relaciones con TI (hoy 5º)

[208] Visión y Metas en Agenda PROSOFT 3.0 1,000 centros de calidad (hoy 527)

1.1.6. MEXICOIT

MexicoIT[209] es un programa de promoción de la industria local de TI para mostrar, representar y promover la oferta del conjunto de tecnologías, talento y capacidades actuales del país, en los mercados globales de TI. Representa un esfuerzo por posicionar a la industria mexicana de TI, llevado a cabo por la iniciativa privada mediante la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI)[210], y el Gobierno Federal a través de la Secretaría de Economía. Pretende principalmente:

a) Presentar a México con otras compañías globales como de calidad mundial y de como una alternativa para soluciones TI.
b) Probar los beneficios de invertir en México en la industria de TI
c) Administrar consultas de la industria global de TI.

1.1.7. MexicoFIRST

Es una iniciativa respaldada por Secretaría de Economía y el Banco Mundial, cuyo objetivo principal es la generación de capital humano con el fin de fortalecer la oferta laboral tanto en cantidad como en calidad, todo para facilitar el desarrollo y competitividad de las empresas mexicanas, así como la atracción de inversiones extranjeras que busquen en México un jugador de clase mundial.

Se realizan convocatorias anuales para *profesionales, empresas, estudiantes y académicos* del sector de Tecnologías de la Información, establecidos en la República Mexicana, que deseen capacitarse en tecnologías avanzadas de información y obtener diversas certificaciones, participando a través del programa MexicoFIRST que ofrece apoyos económicos substanciales[211].

[209] Más información en su página: http://www.mexico-it.net/
[210] En referencia al CANIETI ver página 46 de éste documento
[211] Más información en su página: http://www.mexico-first.org/

1.2. Organizaciones no gubernamentales

1.2.1. CANIETI

La Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías[212] de la Información (con más de 70 años de vida en México) es una institución de interés público, autónomo, con personalidad jurídica y patrimonio propio, diferente al de cada uno de sus afiliados, constituida conforme a lo dispuesto en Ley de Cámaras Empresariales y sus Confederaciones[213].

En la CANIETI se afilian las personas físicas o morales establecidas legalmente tanto en la República Mexicana como en el extranjero, que se dedican habitualmente a actividades relacionadas con el sector electrónico, de telecomunicaciones o de Tecnologías de la Información.

La Cámara se integra por más de 1000 empresas afiliadas en todo México, agrupadas para defender y vigilar sus derechos e intereses comunes.

1.2.2. AMITI

La Asociación Mexicana de la Industria de Tecnologías de la Información[214] (fundada en 1985) está constituida como una Asociación Civil. Tiene como objetivos, entre otros: promover el desarrollo sostenido de la industria de tecnologías de la información, ser foro de participación en el que se involucran micro, pequeñas y medianas empresas de la industria de TI; involucrar a los sectores público, privado, académico y social en proyectos que usando TI resuelvan problemas particulares y de prioridad nacional[215].

---

[212] Página de la CANIETI: http://www.canieti.org/

[213] Ésta ley tiene como objeto normar la constitución y funcionamiento de las Cámaras de Comercio, de la Industria, y confederaciones que las agrupan. Se encuentra publicada en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LCEC.pdf

[214] Página del AMITI: www.amiti.org.mx

[215] Ver más objetivos en los Estatutos Constitutivos de AMITI A.C., publicados en: http://amiti.org.mx/wp-content/uploads/2011/10/estatutos_amiti.pdf

La AMITI ofrece a sus socios un foro en donde puedan llevar a cabo sus actividades, crear sinergias, y elaborar propuestas y proyectos en beneficio de la industria y del país.

Cuenta con convenios de Colaboración y Relaciones con Universidades, Embajadas, Dependencias de Gobierno, Asociaciones y Cámaras, así como otras instituciones y organismos, para promover el desarrollo de la industria de Tecnologías de Información. Actualmente cuenta con 230 socios[216].

La AMITI representa a México ante la Alianza Mundial de Servicios de Tecnologías de Información (WITSA) y la Federación de Asociaciones de Latinoamérica, el Caribe y España de Entidades de TI (ALETI).

Dentro de sus iniciativas se encuentra el: a) Incrementar la Inversión de TIC en el sector público y privado; b) Fomentar Exportación de servicios de TI; c) Formación de Capital Humano en las TIC's; d) Gobierno como un serio promotor de las TICs/Plan 2015.

Dentro de su organización, cuentan con varios comités, entre ellos el comité de APPs y Cloud, que se encarga de detonar el uso de aplicaciones móviles y soluciones en la nube ubicándoles como el medio más práctico, rápido, eficiente y económico para acelerar la adopción de las TIs en los sectores productivos de México[217].

1.2.3. AMIPCI

La Asociación Mexicana de Internet (fundada en 1999) es una Asociación Civil que tiene como objetivo fomentar el uso responsable y productivo de internet por parte de organizaciones, empresas, instituciones y usuarios. Realizan estudios y eventos anuales que permiten conocer más sobre las tendencias en línea y la percepción de los usuarios en temas fundamentales alrededor de internet. Actualmente cuenta con más de 200 socios de diversas actividades en

[216] Dato hasta julio del 2014, en la página http://amiti.org.mx/quienes-somos
[217] Ver otros comités y sus funciones en la página: http://amiti.org.mx/quienes-somos/iniciativas

línea[218]. En general, cualquier sitio que realice alguna actividad en línea y cumpla con los códigos de ética, puede ser socio de AMIPCI.

Entre los objetivos de la AMIPCI se encuentra el de agrupar a empresas que ejercen una verdadera influencia en éste sector, procurar que las inversiones realizadas por dicha industria no se vean afectadas por disposiciones y situaciones generadas por terceros; ejercer un frente común ante las decisiones y disposiciones oficiales y privadas en lo concerniente a las operaciones relacionadas con Internet. Promover y cabildear una legislación adecuada para el impulso de la Red en México, etc.

La AMIPCI otorga un distintivo de confianza a sitios web que pertenecen a empresas, organizaciones, instituciones y personas identificadas y comprometidas con la generación de confianza en línea, mediante su sitio: www.sellosdeconfianza.org.mx

1.3. Prácticas internacionales

México ha participado en foros internacionales para promover la adecuación de la normatividad mexicana en materia de comercio electrónico a las mejores prácticas mundiales.

1.3.1. ASPAN

Desde 2005 se ha trabajado para crear un marco común de comercio electrónico en el contexto de la Alianza para la Seguridad y Prosperidad de América del Norte (ASPAN). En 2007, México, Estados Unidos y Canadá apoyaron la adopción y posterior implementación de la Declaración sobre el Flujo Libre de Información y Comercio en América del Norte.

[218] Tales como: farmacéuticas, hoteles, empresas de logística transporte y entrega; buscadores web, medios de pago, empresas de seguridad informática, despachos de auditorías, agencias de viaje, etc. Ver más en la página de AMIPCI: https://www.amipci.org.mx/en/que-es/descripcion-amipci

1.3.2. APEC

En octubre de 2006 fue lanzada una iniciativa conjunta del sector público y privado para fortalecer a la industria mexicana e impulsar el crecimiento del comercio electrónico en México, apoyándose en los lineamientos de privacidad establecidos en APEC. Durante 2007 México apoyó y expresó su determinación de participar en alguno de los 9 proyectos contenidos en el APEC *Data Privacy Pathfinder*.

1.3.3. UNCTAD- ALADI

En el marco del Seminario Regional sobre los Aspectos Legales del Comercio Electrónico (octubre, 2007), promovido por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD por sus siglas en inglés), y la Asociación Latinoamericana de Integración, se impartieron y desarrollaron cursos presenciales y a distancia sobre aspectos legales del comercio electrónico, para funcionarios públicos y privados de los países miembros. Asimismo, se creó el grupo Montevideo, el cual integra a profesionales de derecho para tratar diversos temas legales del comercio electrónico, a fin de promover la armonización normativa de la región; el grupo ya cuenta con algunos proyectos piloto como el Certificado de Origen Digital “E-COD ALADI” y un Sello de Confianza de la Región, reconocido y validado por los Estados miembros de la ALADI[219]

2. Tipología de nubes y servicios

A la tipología de nubes, en cuanto que puede distinguirse entre nubes públicas, privadas, comunitarias e hibridas, así como de los servicios, relativos a infraestructura (IaaS), plataforma (PaaS), software (SaaS) y business process (BPaaS), nos hemos referido de manera extensa con anterioridad, al presentar las clasificaciones en el cómputo

[219] PROSOFT 2.0, diagnóstico y avances publicado en el 2008 http://www.prosoft.economia.gob.mx/doc/prosoft20.pdf

en la nube[220], de manera que aquí haremos únicamente referencia a algunos aspectos concretos y adicionales para evitar así repeticiones innecesarias.

Entre dichos aspectos, uno es el relativo a que desde el punto de vista del cliente es importante prestar atención al tipo de nube cuando se contratan los servicios correspondientes. Es decir, si un cliente, ya sea una organización del sector privado o una entidad del sector público, va a almacenar datos en la nube, es importante que analice qué tipo de nube es la que mejor se adopta a sus necesidades.

Resulta claro que si los datos, sean personales o no y sensibles o no, no son considerados como una información confidencial, la opción de la nube pública puede ser la más adecuada por sus características y costo. Pero, si por el contrario estamos ante un supuesto en el que la información a almacenar y tratar en la nube son datos personales sensibles[221], entonces la nube privada puede ser la opción más adecuada dadas sus características.

Recordemos que entre las características ya analizadas de las nubes privadas se encuentran las relativas a que lleva asociados sistemas y bases de datos locales; está diseñada para ajustarse a las necesidades propias de la empresa contratante y también facilita el control y la supervisión de los requisitos de seguridad y protección de la información almacenada.

Por tanto, el tipo de nube que elija un cliente está relacionado, además de con otros factores, con el hecho de que vaya a tratarse información, sean datos personales o no, que pueda ser más o menos confidencial, de manera que clasificar la información y atender a su naturaleza es importante a la hora de contratar uno u otro tipo de nube.

---

[220] Véase la parte relativa a definición y cuestiones generales sobre el cómputo en le nube.

[221] Que son definidos en la fracción VI, del artículo 2 de la LFPDPPP como *"[a]quellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual."*

Y por lo que se refiere a los tipos de servicios, resulta claro que los clientes contratarán éstos en atención a sus necesidades específicas que se refieran a recursos informáticos de carácter básico (infraestructura), aplicaciones Web escalables (plataforma), aplicaciones completas de usuario final en la Web (software) o servicio de procesos de negocio "*end-to-end"* (Business Processor).

En cualquier caso, los diferentes tipos de nubes y servicios implican que los clientes, ya sean del sector privado o público, cuenten con una amplia oferta que les permite hacer uso de recursos informáticos de una manera que implica la posibilidad de almacenar y procesar grandes cantidades de información, de manera que serán clave para el desarrollo de los grandes tratamientos de datos personales *(big data)*, o el Internet de las Cosas. Además, uno de los aspectos relevantes en el caso de las PYMEs es que el cómputo en la nube significa también que *"puedan competir con las grandes, ya que los diferenciales competitivos que se daban en cuanto al uso tradicional de las tecnologías de la información desaparecen gracias a aquél"*[222].

3. Oportunidades de negocio que ofrece el cómputo en la nube en México

El cómputo en la nube, además de un servicio electrónico que avanza día a día en el caso de México como hemos visto en virtud de la encuesta elaborada en la primera parte de este estudio, es también una posibilidad de ofrecer servicios para las empresas de manera que México no puede perder la oportunidad para ser competitivo a nivel internacional.

[222] Véase VV.AA., La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo. Op. ya citada. Pág. 16.

3.1. De manera directa

La prestación de servicios de nube o relacionados con la nube es una clara oportunidad de negocio. En este sentido, el estudio sobre la nube al que ya hemos hecho referencia[223], citando diversas fuentes, indica que:

> *"Según Gartner, el crecimiento de los servicios basados en nube pública, a nivel mundial, seguirá en aumento hasta 2017. Dicho crecimiento aumentará un 17.4% en comparación con 2011 y pasará de 132 billones de dólares que los usuarios invirtieron en 2011 a casi 250 billones de dólares en 2017, incluyendo publicidad. Es así que los servicios de nube pública seguirán creciendo, ya que para 2013 Gartner12 había pronosticado que lo harían en un 18.5% a nivel mundial, de manera que superarían los 111 billones de dólares alcanzados en 2012."*

Si bien resulta claro que el mercado de prestación de servicios de cómputo en la nube se caracteriza por la existencia de pocos proveedores, lo cual puede responder entre otras razones a la necesidad de contar con una infraestructura compleja y un alto nivel de servicios, hay oportunidades relacionadas con el cómputo en la nube pudiendo ser el BPaaS una de ellas.

Al respecto, uno de los logros importantes de PROSOFT del 2003 al 2007 ha sido que México *"ha logrado posicionarse en la percepción internacional como un país con capacidad de desarrollar tecnología y un destino de la subcontratación de servicios de TI. Analistas internacionales del sector consideran que México cuenta a clima general necesario para ser considerado como un lugar potencial para offshore/nearshore de servicios de TI y externalización de procesos de negocio (BPO por las siglas en inglés de business process outsourcing)."*[224]

---

[223] Véase la nota a pie de página anterior. Pág. 8.

[224] Véase Logros del PROSOFT a cinco años de su implementación, disponible en la dirección de Internet http://www.diputados.gob.mx/expo_foro/docs/proyectos/23_PROSOFT.pdf

Es decir, lo anterior unido al uso de la nube, puede llevar a las empresas mexicanas a ser tanto prestadores de servicios de TI que compitan a un alto nivel así como a las Administraciones Públicas a ser eficientes, lo cual se refleja en los *rankings* internacionales. Y al mismo tiempo la nube es una clara oportunidad para el desarrollo de negocios y generación de empleos[225] que debe ser considerado en el caso de México.

Por tanto, la existencia de políticas públicas que impulsen la adopción de la nube, por empresas y Administraciones Públicas, es una opción adecuada para no perder oportunidades de competitividad, especialmente en una economía globalizada que día a día avanza más en la dirección de la prestación de servicios electrónicos y el uso de tecnologías innovadoras.

3.2. De manera derivada

El cómputo en la nube también está relacionado con las aplicaciones ("apps"), que son una oportunidad para jóvenes y emprendedores a tomar en consideración. Según algunos estudios[226], el mercado de apps en México crecerá entre 2013 y 2017 hasta alcanzar una cifra de 75 mil millones de dólares de ingresos globales hasta 2016.

A nivel internacional, por ejemplo en el caso de la Unión Europea[227] se estima que conforme a un estudio llevado a cabo sobre las "apps", éstas generarán un mercado de 63 millones de euros y casi cinco (5) millones empleos hasta 2018.

---

[225] Al respecto, puede verse por ejemplo una noticia en la que se indica que según un estudio preparado por IDC para Microsoft, el *cloud* generará 214,400 empleos en México entre 2012 y 2015. Véase la noticia en http://eleconomista.com.mx/tecnociencia/2012/03/06/cloud-generara-214400-empleos-mexico-idc

[226] Véase la nota de prensa disponible en http://www.elfinanciero.com.mx/tech/mercado-de-aplicaciones-generara-75-mil-mdd-en-el-mundo-en-2016.html#.U9-IywOjSj4.twitter

[227] Véase la nota de prensa de la Comisión Europea disponible en http://europa.eu/rapid/press-release_IP-14-145_en.htm

También surgen otras oportunidades de negocio, como por ejemplo podría ocurrir en el caso de la certificación. En este sentido, además de la certificación en protección de datos personales prevista en los Parámetros[228] emitidos por la Secretaría de Economía en coadyuvancia con el IFAI y que encuentran su razón de ser en el artículo 44 de la LFPDPPP, la certificación en materia de nube puede ser otra oportunidad.

En concreto, en el caso de la Unión Europea, la certificación es una de las cuestiones clave en la estrategia europea sobre la nube[229].

En el caso de México, la posibilidad de prestar servicios de certificación en materia de protección de datos personales y relacionados con la nube es una clara oportunidad, respaldad por el hecho de que la LFPDPPP impulse en el párrafo segundo de su artículo 44 los esquemas de autorregulación, que *"podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares."* Y correlativamente en el artículo 83 de Reglamento de la LFPDPPP que en el segundo párrafo indica que *"[e]n caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley."*

---

[228] Se trata de los Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el Diario Oficial de la Federación el 29 de mayo de 2014.

[229] Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, la Comité Económico y Social Europeo y al Comité de las Regiones – Liberar el potencial de la computación en la nube en Europa, COM(2012) 529 final, de 27 de septiembre de 2012, en la que se indica que *"El despegue de las actividades en nube se verá favorecido por un mayor uso de las normas, por la certificación de los servicios en la nube para demostrar que cumplen estas normas y por el refrendo de tales certificados por parte de las autoridades normativas para indicar el cumplimiento de las obligaciones jurídicas."* La citada Comunicación puede verse en la dirección de Internet http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012DC0529&rid=1

En definitiva, la posibilidad de prestar servicios relacionados con la nube, tanto tecnológicos como jurídicos, es una realidad que debe ser tomada en consideración con la finalidad de aprovechar los logros alcanzados por México y seguir siendo competitivo con otras regiones y países alrededor del mundo.

4. Aspectos a considerar sobre el cómputo en la nube desde un punto de vista tecnológico

4.1. Estandarización

La estandarización implica que deba garantizarse que tanto la prestación de servicios de cómputo en la nube como el desarrollo de los mismos se haga conforme a estándares tanto nacionales como internacionales que sean compatibles. De otra forma, podrían darse situaciones en las que un cliente de servicios de cómputo en la nube pueda tener problemas a la hora de hacer uso de dichos servicios.

En el caso de estándares nacionales, es importante garantizar que los servicios de cómputo en la nube y la tecnología necesaria para la misma cumplan con las Normas Oficiales Mexicanas aplicables en la materia, así como que la tecnología se desarrolle conforme a dichas normas. Y, a su vez, dichas normas tienen que estar alienadas con las normas internacionales, tales como las normas ISO, entre las que se encuentra la ISO/IEC 17788 *Tecnología de la Información. Servicios y plataformas para aplicaciones distribuidas. Computación en la nube. Generalidades y vocabulario*, así como la ISO/IEC 17789 *Tecnología de la Información. Computación en la nube. Arquitectura de referencia.*

No tomar en consideración la necesidad de estandarización, tanto a nivel nacional como alineada con las normas internacionales, sería un problema para los clientes de servicios de cómputo en la nube, que tendrían importantes problemas en la práctica para poder hacer uso de los servicios. Por tanto, la estandarización, como garantía, tiene que ser también un aspecto a tomar en consideración en los acuerdos de nivel de servicio.

4.2. Interoperabilidad

A la interoperabilidad nos referiremos posteriormente, debiendo tomar en consideración ahora que según la definición dada en el Esquema de Interoperabilidad de Datos Abiertos de la Administración Pública Federal, en la fracción XVIII del artículo segundo, es *"la capacidad de organizaciones y sistemas, dispares y diversos, para interactuar con objetivos consensuados y comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las dependencias y entidades compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicaciones".*

La interoperabilidad requiere que se garantice la neutralidad tecnológica, a la que también nos hemos referido a lo largo del estudio, de manera que una cuestión a tomar en consideración por la Secretaría de Economía, como autoridad competente, es la de adoptar las medidas oportunas para que tanto la interoperabilidad como la neutralidad tecnológica sean los principios a tener en cuenta a la hora de abordar cualquier cuestión relativa al cómputo en la nube.

El hecho de que los servicios y la información sean interoperables es también un aspecto importante a tomar en consideración desde el punto de vista de los clientes de cómputo en la nube, de manera que no se vean cautivos de un prestador de servicios de cómputo en la nube.

Como conclusión, cabe señalar que la interoperabilidad es fundamental en el caso del uso de las TIC así como en relación al *cloud computing* y otros servicios tecnológicos, por lo que debe ser un principio rector o que gobierne el desarrollo de políticas públicas en relación con el cómputo en la nube y, al mismo tiempo, ser una garantía para los clientes de dichos servicios.

4.3. Análisis de las tendencias tecnológicas que requieren especial atención en la seguridad de la información y de datos personales

Considerando que dichas tendencias tecnológicas están relacionadas con el cómputo en la nube por la capacidad tecnológica que ésta ofrece, ya que de otra manera no sería posible contar con los recursos necesarios desde un punto de vista tecnológico para tratar ingentes cantidades de datos personales o, también, cualquier otra información aunque no sean datos personales, es posible atender a algunas de estas tendencias.

Al respecto, algunas de estas tendencias son el internet de las cosas (internet of things), los tratamientos masivos de datos (Big Data), o los Sistemas Operativos Urbanos (smart cities). En concreto, éstas son las tres tendencias tecnológicas que, según los expertos[230], se van a consolidar en América Latina durante el año 2014.

Se trata de tres tendencias que para las empresas representan oportunidades de negocio y también pueden suponer cambios importantes en cuanto a la posibilidad de acceso a la información.

4.3.1. Internet de las cosas

El internet de las cosas es una de las tendencias tecnológicas más relevantes que presenta diversas implicaciones, ya que cualquier empresa, con independencia de su tamaño y área o sector de actividad, puede beneficiarse de las innumerables ventajas que ofrece y que, entre otros aspectos, potencia la posibilidad de un escenario de movilidad y omnipresencia desconocido hasta el momento.

A nivel global, según la empresa de inteligencia de mercados International Data Corporation (IDC), se estima que para 2020 habrá 32,000 millones de dispositivos conectados, lo que representa el 10%

[230] Puede verse la nota de prensa publicada en http://www.forbes.com.mx/tres-tendencias-tecnologicas-y-el-riesgo-para-la-innovacion/

de los datos mundiales[231]. Por su parte, Ericsson estima que para 2020 existirán 50,000 millones de objetos conectados a la red en todo el mundo, de los cuales 5,000 millones estarán en América Latina[232].

También IDC estima que el mercado global de soluciones para el internet de las cosas[233] crecerá de 1,9 trillones de dólares en 2013 hasta 7,1 trillones de dólares en 2020.

Las posibilidades que ofrece el internet de las cosas tiene importantes implicaciones tanto en materia de protección de datos personales como de seguridad, estimando IDC que *"el 40% de los datos en el universo digital requieren algún tipo de protección, desde medidas de privacidad intensificadas hasta datos totalmente encriptados"* y que en *"México sólo el 47% de la información que requiere protección cuenta con ella."*[234]

Citando a Cisco como fuente, según las cifras estimadas por este último, el internet de las cosas podría generar ganancias de hasta 34,4 billones de dólares para México en los próximos diez años[235], estando México entre los 12 países del mundo que más beneficios podrían obtener.

El internet de las cosas ofrece un amplio abanico de aplicaciones y posibilidades en diferentes sectores y materias, lo que supone que deba prestarse atención a los tratamientos de datos personales que se producen en cada caso, los principios y deberes aplicables y la necesidad de revisar si el marco normativo aplicable es el adecuado o si son necesarias modificaciones o acciones tales como impulsar la autorregulación sectorial, así como garantizar la seguridad en un

---

[231] Véase la referencia en http://www.forbes.com.mx/internet-de-las-cosas-dinamizador-de-los-negocios/

[232] Véase la cifra citada en la dirección de Internet http://eleconomista.com.mx/tecnociencia/2014/08/21/medir-desafio-internet-las-cosas

[233] Véase la referencia en la dirección de Internet http://www.idc.com/getdoc.jsp?containerId=prUS24903114

[234] Véase la referencia indicada en http://www.forbes.com.mx/internet-de-las-cosas-dinamizador-de-los-negocios/

[235] Véase la información en http://pulsosocial.com/2014/01/28/internet-de-las-cosas-generaria-us19-billones-a-gobiernos-y-empresas-privadas-en-2022/

escenario digital en el que todo está interconectado y, por tanto, puede ser el objetivo de ataques cibernéticos.

Es decir, el desarrollo tecnológico plantea, de nuevo, cuál ha de ser la interrelación entre derecho y tecnología, prestando atención específica a la protección de datos personales y la seguridad, ya que se trata de conseguir un equilibrio entre innovación y garantía del derecho fundamental a la protección de datos personales y la seguridad.

4.3.2. Big data

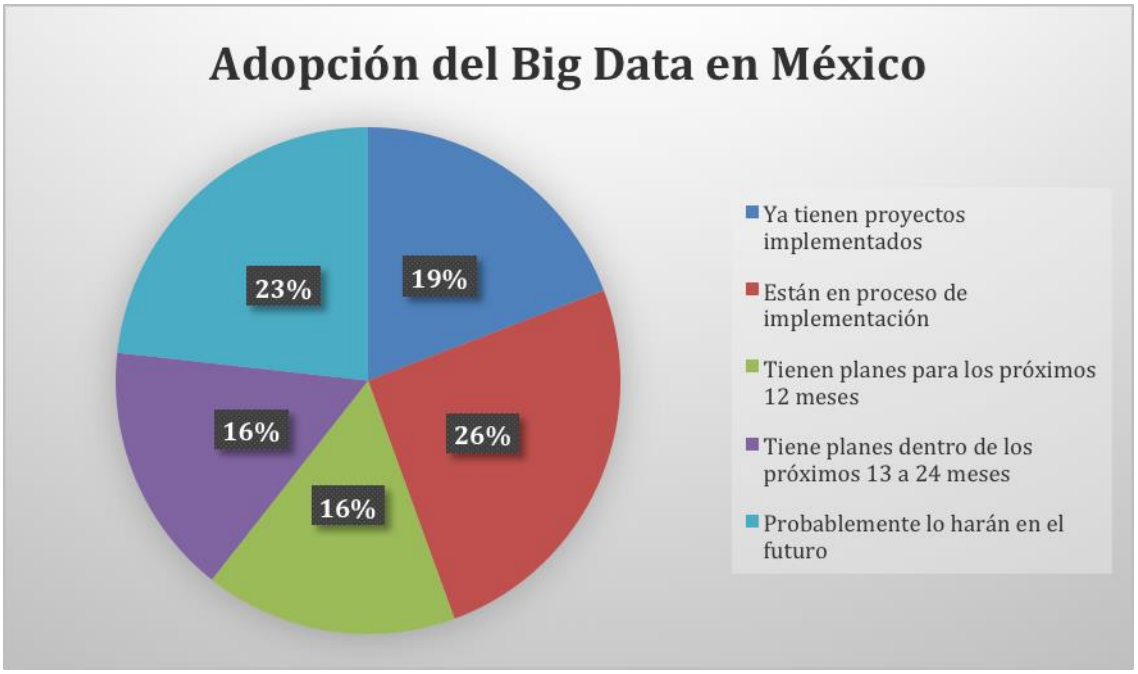
En el caso del *big data*, según IDC, se espera[236] que el mercado de tecnología y servicios represente una cifra de 32.4 mil millones de dólares en 2017, lo que supone un crecimiento anual del 27%.

Al respecto, según un estudio elaborado por IDC[237] entre compañías que han adoptado o están adoptando el *big data*, los resultados son los siguientes:

	Porcentaje
Ya tienen proyectos implementados de Big Data	19%
Están en proceso de implementación (25%)	25%
Tienen planes para desplegarlos en los próximos 12 meses	16%
Tienen planes para desplegarlos dentro de los próximos 13 a 24 meses	16%
Probablemente implementarán proyectos de Big Data en el futuro	23%

[236] Véanse las cifras indicadas en http://www.computerworldmexico.mx/Articulos/31940.htm
[237] Mencionado en el artículo que se indica en la nota a pie anterior

Lo que gráficamente puede representarse de la siguiente manera:



Unido a lo anterior, según un estudio elaborado por Cisco, titulado *Connected World Technology Report* (CCWTR)[238], el *"85% de los gerentes de TI en México considera que los Big Data aumentarán la competitividad global, y 78% de ellos asegura que serán una prioridad estratégica para su compañía en 2013 y en los próximos cinco años."*

También, en relación con el mencionado estudio, se indica que *"los gerentes de TI entrevistados en México indican que su presupuesto para el manejo de estos grandes volúmenes de datos aumentará 64% en 2013, y se prevé que el porcentaje se incremente más de la mitad (52%) en los próximos cinco años. A escala mundial, estos son de 53 y 57%, respectivamente."*

Por lo que se refiere a otras cifras a las que da lugar el *big data*, según un estudio de **Online Business School[239], se estima que en**

[238] El estudio aparece mencionado en la nota de prensa http://www.computerworldmexico.mx/Articulos/28648.htm

[239] Véase una referencia al citado estudio en http://www.obs-edu.com/noticias/2014/05/12/el-volumen-de-datos-generado-por-smartphones-crecera-un-63-los-proximos-cuatro-anos/

todo el mundo se generarán 4,400 millones de empleos y que en el año 2015 se producirá una inversión de 132.000 millones de dólares en servicios de big data en todo el mundo.

Si bien pudiera pensarse que el *big data* está reservado sólo para grandes empresas, no es así, ya que también las PYMES se verán beneficiadas por el uso del *big data*, lo que les permitirá tomar mejores decisiones.

Además, el *big data* tiene también implicaciones sociales[240] que todavía deben ser analizadas[241]. Específicamente en México, en 2014, INFOTEC y el Instituto Nacional de Estadística y Geografía (INEGI) organizaron durante los días 16 y 17 de junio, un seminario internacional sobre *"Big Data para la Información Oficial y la Toma de Decisiones"*, en la que se prestó atención a las posibilidades que ofrece el *big data* en cuanto al luso de información y la toma de decisiones, siendo uno de los aspectos relevantes que *"La generación y disponibilidad de información digital, así como el uso masivo de dispositivos electrónicos, hacen posible su empleo para generar información oficial, estadística y geográfica"*[242].

Y entre los retos que se presentan en este sentido, cabe señalar, en particular, que *"para extraer su potencial, será necesario contar con la legislación y regulación adecuadas que permitan la explotación de bases de datos para fines públicos, asegurar la privacidad y seguridad de la información."*[243]

[240] Véase el artículo publicado en http://www.computerworldmexico.mx/Articulos/25268.htm

[241] En concreto, cabe señalar que la Federal Trade Commission (FTC) de los Estados Unidos de América, ha organizado un evento en Washington, D.C., el 15 de septiembre de 2014, que tiene por objeto prestar atención a estos aspectos. El evento relativo al *Big Data: A Tool for Inclusion o Exclusion?* presta especial atención a al uso del *big data* y su impacto en los consumidores Americanos, incluyendo a quienes tienen ingresos o recursos más bajos. En relación con este evento puede verse la información disponible en http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion

[242] Véase el programa del evento en la dirección de Internet http://www.inegi.org.mx/eventos/2014/big-data/doc/Agenda_es.pdf

[243] Véase el documento citado en la nota a pie anterior.

Por lo que se refiere a las implicaciones en protección de datos personales, el *big data* fue ya mencionado en la Declaración de la Ciudad de México, adoptada durante la 33ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos[244]. En relación con el concepto de *big data*, la citada Declaración hace referencia a que:

> *"el crecimiento expansivo de las computadoras, los medios de comunicación, el análisis de datos, y la velocidad con la que proliferan los datos personales, así como el desarrollo de nuevas formas de almacenamiento de información en bases de datos de gran dimensión que posibilitan el rastreo y la supervisión, así como las tecnologías basadas en sensores, todo esto comúnmente conocido con el término de "big data"."*

Y termina la Declaración indicando:

> *"Acordar que en la 34ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos se expongan y discutan los avances logrados mediante el trabajo conjunto en aras de una más efectiva protección de datos en esta era de globalización y "big data"."*

Durante la 34ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos, los Comisionados adoptaron la Declaración sobre "profiling" o evaluación de perfiles[245], de fecha 26 de octubre de 2012, en la que se hace referencia a las ventajas que puede representar el big data, entre otros, en sectores como la salud, la eficiencia energética y la salud pública, si bien dichos tratamientos de datos personales presentan riesgos para el derecho a la protección de datos personales y la privacidad a los que hay que atender por lo que se hace necesaria la adopción de medidas, tanto regulatorias como no

[244] Disponible en la dirección de Internet http://www.redipd.org/documentacion/common/declaracion_2011_IX_encuentro_es.pdf

[245] Disponible en inglés en la dirección de Internet http://privacyconference2012.org/wps/wcm/connect/7b10b0804d5dc38db944fbfd6066fd91/Uruguay_Declaration_final.pdf?MOD=AJPERES

regulatorias, ya sean estas últimas tecnológicas o metodológicas, con la finalidad de minimizar dichos riesgos.

En particular, en el caso de México, el *big data* se desarrollará debiendo tomar en consideración los principios establecidos en la normatividad sobre protección de datos personales, tanto para el sector privado como para el sector público, de manera que el consentimiento, la calidad de los datos, la minimización del tratamiento de los datos personales y la finalidad del tratamiento, además del resto de principios y deberes aplicables, son el marco que aplica para el tratamiento de datos personales a los que da lugar el *big data*.

En conclusión, cualquier empresa, del tamaño y sector que sea, tiene que actuar con apego a la normatividad sobre protección de datos personales, sin perjuicio de requisitos específicos con los que tenga que cumplir, por ejemplo, en el caso de datos de salud, a la hora de beneficiarse de las ventajas que ofrece el *big data.*

4.3.3. Sistemas Operativos Urbanos (*smart cities*)

Los Sistemas Operativos Urbanos o ciudades inteligentes (*smart cities*) son otra de las tendencias tecnológicas más destacables tanto actuales como futuras.

Sobre las ciudades digitales, cabe señalar que en Mayo de 2014, tuvo lugar una conferencia internacional *"Ciudades inteligentes, gobiernos abiertos: comparaciones entre Francia y México"*, organizada por la Universidad Nacional Autónoma de México (UNAM) en la que se trataron algunos aspectos relativos a las ciudades inteligentes y la protección de datos personales.

Una de las conclusiones que se alcanzaron en dicha conferencia fue la de que *"los cambios en las tecnologías y su influencia en las ciudades inteligentes han incentivado la creación de regulaciones que eviten el uso irresponsable de la información personal de los*

ciudadanos por parte de las autoridades"[246]. Y lo anterior supone que las reformas legislativas o futuras leyes sobre protección de datos contemplen estos avances tecnológicos, siendo necesario que tanto actualmente como en el futuro se garantice la protección de datos personales, lo que se consigue a través de una aplicación efectiva de los principios y deberes de la protección de datos personales.

El desarrollo de las ciudades inteligentes plantea también la *"colusión público-privada en distintos sectores de la vida social y económica"*. Es decir, desde proporcionar infraestructura hasta el desarrollo de aplicaciones o servicios tecnológicos para el desarrollo de las ciudades digitales, son ámbito de oportunidad para cualquier empresa y, por tanto, debe ser un área a tener en consideración.

En relación con lo anterior, es necesario garantizar los principios de la protección de datos personales, debiendo tener en especial consideración el conocido como principio de privacidad desde el diseño ("Privacy by Design"). Y también que en el caso de México, D.F., se trata de una ciudad de 22 millones de habitantes en la que hay, por ejemplo, 8.000 cámaras de vídeo que permiten recabar constantemente información[247].

Y dicho desarrollo avanza debiendo tener en consideración que *"hacia 20150 casi 70% de la población mundial será urbana"*[248], lo que debe servir para dimensionar los retos que se plantean, tanto desde la perspectiva de protección de datos personales como en otras áreas, tales como seguridad, salud, gestión de residuos, uso de tecnologías verdes, etc.

---

[246] Al respecto, puede verse la nota publicada en la dirección de Internet http://www.iis.unam.mx/indexcontent.php?_module=689

[247] Véase la reseña de Thales sobre la *"Integración de transporte y seguridad para una ciudad inteligente"*, en la dirección de Internet https://www.thalesgroup.com/es/espana/case-study/integracion-de-transporte-y-seguridad-para-una-ciudad-inteligente

[248] El dato aparece citado en el documento de la Organización para la Cooperación y el Desarrollo Económicos (OCDE9, Perspectivas ambientales de la OCDE hacia 2050. Véase en http://www.oecd.org/env/indicators-modelling-outlooks/49884278.pdf

En cuanto a la protección de datos personales, lo anterior implica tener en consideración nuevos paradigmas de privacidad y seguridad, de manera que lo importante sea considerar el uso que se da a los datos personales, a la vista de que se recaban a través de múltiples sensores y dispositivos incluso de forma invisible para la persona, así como la necesidad de garantizar la ciberseguridad frente a constantes ataques cibernéticos.

Al igual que en el caso del internet de las cosas y el *big data*, las ciudades inteligentes implica que se desarrollará debiendo tomar en consideración los principios establecidos en la normatividad sobre protección de datos personales, tanto para el sector privado como para el sector público, así como los nuevos paradigmas de privacidad y seguridad para un mundo cada vez más interconectado.

5. Necesidad de identificar riesgos legales y regulatorios para evitar incumplimientos

El uso de cualquier tecnología, no sólo del cómputo en la nube, implica que el usuario, ya sea una empresa del sector privado o una entidad o dependencia del sector público, tengan que identificar si existen riesgos o cuestiones legales o regulatorias para evitar incumplimientos.

En el caso del tratamiento de datos personales, por lo que se refiere en particular al sector privado, el Reglamento de la Ley Federal de Protección de Datos en Posesión de los Particulares[249] incluye en la fracción V del artículo 48, entre las medidas para el principio de responsabilidad la relativa a:

> *"V. Instrumentar un procedimiento para que atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos."*

[249] Publicado en el Diario Oficial de la Federación de 21 de diciembre de 2011. El texto de este Reglamento puede verse en la siguiente dirección electrónica http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Esta medida, así como las demás previstas en el citado artículo corresponde adoptarla al responsable del tratamiento, siendo necesario poner el citado artículo en relación con el artículo 14 de la LFPDPPP, que indica:

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

Es decir, el responsable adoptará las medidas para cumplir con el principio de responsabilidad, si bien en virtud del artículo 14 de la LFPDPPP velará también porque el encargado del tratamiento, como tercero que trata los datos por solicitud del responsable y a su cuenta, cumpla también con los principios de la protección de datos personales.

También el citado Reglamento de la LFPDPPP, en su artículo 60, se refiere a los factores para determinar las medidas de seguridad y entre dichos factores se incluye:

> *"I. El riesgo inherente por tipo de dato personal."*
>
> Y también indica que *"[d]e manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:*
>
> *[…]*
>
> *IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable."*

Adicionalmente, el artículo 61, relativo a las acciones para la seguridad de los datos personales, incluye entre las mismas la consistente en:

> *"III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;"*

En cuanto al riesgo en protección de datos personales, es necesario tomar en consideración que todo tratamiento de datos personales supone un riesgo[250] y que es necesario garantizar también su seguridad. Al respecto, cabe señalar que, como ya sabemos, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), publicó en 2014 una *Tabla de equivalencia funcional de estándares de seguridad y la LFPDPPP, su Reglamento y las Recomendaciones en materia de seguridad de los datos personales*[251] en la que con relación al concepto de gestión del riesgo de los datos personales, define el riesgo con carácter general como:

> *"una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal que al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal."*[252]

También, en su *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*[253], en lo relativo al riesgo para los datos personales, el IFAI indica que:

> *"**El objetivo de implementar medidas de seguridad es que cada una de ellas ayude a reducir el riesgo de que se materialice un incidente y sus consecuencias desfavorables.** Las medidas de seguridad también ayudan a que, en caso de que se presente un incidente, se reduzca el daño a los titulares y a la empresa u organización."*[254]

---

[250] Al respecto, por ejemplo, véase a nivel internacional el documento del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE *titulado Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218, que fue adoptado el 30 de mayo de 2014 y que está disponible en la dirección de Internet http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[251] La tabla de equivalencia, en su versión completa, puede verse en la dirección de Internet http://inicio.ifai.org.mx/_catalogs/masterpage/Documentos-de-Interes.aspx?a=m8

[252] Véase la citada tabla de equivalencia en su página 11.

[253] Publicado en Julio de 2014 y disponible en la dirección de Internet http://inicio.ifai.org.mx/DocumentosdeInteres/Manual_seguridad_mipymes_julio2014.pdf

[254] Pág. 7 del citado Manual.

Específicamente por lo que se refiere al uso de servicios de cómputo en la nube, es posible tomar en consideración que a nivel internacional las buenas prácticas establecidas por las autoridades de protección de datos se concretan en el análisis previo del riesgo para los datos personales. Al respecto, el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, al que hemos hecho ya referencia, en su ya citado Dictamen 5/2012 sobre cómputo en la nube[255], indica que:

> *"Una de las principales conclusiones del presente dictamen es que las empresas y las administraciones que deseen utilizar la computación en la nube deben efectuar, como un primer paso, un análisis de riesgos completo y riguroso."*[256]

Sin perjuicio de lo anterior, los riesgos legales y regulatorios pueden ir, y de hecho así ocurre y ocurrirá, más allá de la protección de datos personales, de manera que es necesario que, en particular, los clientes o potenciales clientes, ya sean estos PYMEs o entidades o dependencias de las Administraciones Públicas, adopten medidas para identificar dichos riesgos previamente a la contratación de servicios de cómputo en la nube o, en su caso, otras soluciones tecnológicas, de manera que se aseguren que la contratación se hace con todas las garantías y que se han evaluado los riesgos existentes en cada caso.

El análisis de dichos riesgos puede llevarse a cabo a través de diferentes instrumentos y metodologías, ya sea trate por ejemplo de una auditoría interna o externa, mediante el uso de *checklists* o cuestionarios[257] o de otra forma, siempre y cuando se garantice que como resultado del análisis es posible identificar riesgos que, posteriormente, permitan adoptar medidas correctivas y de gestión de dicho riesgo para minimizarlo.

---

[255] Se trata del Dictamen 5/2012 sobre la computación en nube (WP 196), adoptado el 1 de julio de 2012 y disponible en la dirección de Internet http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

[256] Pág. 2 del citado dictamen.

[257] En este sentido, es necesario recordar que en el último entregable se incluirá un *checklist* que sirva a los usuarios del estudio para la revisión del cumplimiento, de manera que nos remitimos al mismo.

6. Protección de datos personales

6.1. Normatividad de protección de datos personales

6.1.1. Sector Privado

Más atrás en este mismo estudio nos hemos referido con amplitud al marco regulatorio de la protección de datos personales en México. Nos remitimos a lo ya dicho, sin perjuicio de reiterar ahora y en algún caso complementar lo que ya se ha analizado.

La regulación básica sobre protección de datos personales en posesión de los particulares se contempla, como sabemos, en los siguientes ordenamientos[258]:

1. Artículos 16 y 73, fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos[259].
2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares[260].
3. El Reglamento de la ley Federal de protección de datos personales en posesión de los particulares, en específico, lo relativo a la nube está en el artículo 52, el cual se describe en la siguiente sección[261].

---

[258] Gran parte del marco regulatorio mexicano de protección de datos personales (e internacional en relación con México) puede consultarse en PIÑAR MAÑAS, José Luis y RECIO GAYO, Miguel, *Código de protección de datos personales México*, Tirant Lo Blanch, México, (2013)

[259] **Artículo 16**: "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de los mismos los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros…"

Artículo 73. El Congreso tiene Facultad: … XXIX-O Para legislar en materia de protección de datos personales en posesión de particulares

Conforme a la última reforma publicada el 07/07/2014 en la página De la Cámara de Diputados http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

[260] Ley Federal de Protección de Datos Personales en Posesión de los particulares publicada en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[261] Ver Reglamento en http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

4. Parámetros de autorregulación vinculante en materia de protección de datos personales[262]. Tiene la finalidad de crear bases para que los particulares cuenten con elementos para la elaboración, conformación y aplicación de esquemas de autorregulación en materia de protección de datos personales. Sus disposiciones son de observancia obligatoria[263]. Lo que no esté estipulado en los parámetros, la ley Federal de Procedimiento Administrativo[264] se utilizará de forma supletoria.
5. Recomendaciones del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), en materia de seguridad de datos personales[265]. La recomendación general se encuentra señalada en el artículo 19 de la ley Federal de protección de datos personales en posesión de los particulares, y puede resumirse en que, el IFAI recomienda la adopción de un Sistema de Gestión de Seguridad de Datos Personales, basado en un ciclo de Planear-Hacer-Verificar-Actuar.
6. Lineamientos del aviso de privacidad[266]. Estos Lineamientos fueron emitidos por la Secretaría de Economía en coadyuvancia con el IFAI.
7. Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos[267].

---

[262] Parámetros publicados por la Secretaria de Economía en: http://www.economia.gob.mx/files/marco_normativo/PAR1.pdf Los citados Parámetros, en virtud de su artículo transitorio segundo, abrogan los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos en Posesión de los Particulares, que habían sido publicados en el Diario Oficial el 17 de enero de 2013.

[263] El artículo 44 de la ley Federal de protección de datos personales en posesión de los particulares, prevé que las personas físicas o morales pueden convenir entre ellas, con organizaciones civiles o gubernamentales nacionales o extranjeras, esquemas de autorregulación vinculante que complementen lo dispuesto por la ley, por tanto si deciden crear dichos esquemas, deberán atenerse a los parámetros estipulados por la secretaria de economía.

[264] Ley Federal de Procedimientos Administrativos se encuentra publicada en la página de la Cámara de Diputados: http://www.diputados.gob.mx/LeyesBiblio/pdf/112.pdf

[265] Dichas recomendaciones fueron publicadas el 30.10.2013 en el diario oficial de la federación en la página: http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013

[266] Ver http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

[267] Ver http://dof.gob.mx/nota_detalle.php?codigo=5244229&fecha=18/04/2012

Esta normatividad es la que puede considerarse como general en materia de protección de datos personales en posesión de los particulares, lo que significa que deba entenderse sin perjuicio de otra normatividad específica aplicable en su caso, como por ejemplo la Ley Federal de Protección al Consumidor[268] que en su artículo 17 incluye disposiciones sobre el uso de datos personales con fines mercadotécnicos o publicitarios o el Registro Público de Consumidores previsto en la Ley Federal de Protección al Consumidor y el Registro Público de Usuarios previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros, a los que se refiere, respectivamente, el artículo 111 del Reglamento de la LFPDPPP. Por último, puede tenerse también en consideración la nueva Ley Federal de Telecomunicaciones y Radiodifusión[269] que, por ejemplo, en materia de colaboración de los concesionarios de telecomunicaciones con la justicia, indica en el último párrafo de la fracción II, del artículo 190, que *"[s]in perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares."* [270]

6.1.2. Sector Público

En cuanto al sector público, la regulación de datos personales es de nivel federal y estatal. La normatividad básica, como ya sabemos, se encuentra en los siguientes ordenamientos:

---

[268] Publicada en el Diario Oficial de la Federación el 24 de diciembre de 1992 y disponible, con las reformas que se han hecho al texto original, en la siguiente dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/pdf/113_040614.pdf

[269] Publicada en el Diario Oficial de la Federación el 14 de julio de 2014.

[270] En relación con la cuestión relativa a la colaboración con la justicia, cabe señalar que la prensa hace referencia a las declaraciones de la comisionada Areli Cano, del IFAI, que apuntan a que la Ley podría vulnerar la privacidad y que "el IFAI aún está en el proceso de análisis sobre los artículos de las leyes secundarias de la reforma en telecomunicaciones que abordan la geolocalización y la creación de una base de datos para resolver si se solicita o no a la Suprema Corte de Justicia una revisión de inconstitucionalidad." Véase la nota de prensa publicada en http://www.cnnexpansion.com/negocios/2014/08/08/ley-telecom-vulneraria-privacidad-cano

1. El artículo 6 sección A.III, A.VIII y el artículo 73 fracción XXIX-S[271] de la Constitución Política Federal.
2. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal[272].
3. Acuerdo que tiene por objeto emitir 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 establecer el manual administrativo de aplicación general en dichas materias[273].
4. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[274].
5. El capítulo VIII del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[275].
6. Lineamientos de protección de datos personales[276].
7. Acuerdo que tiene por objeto emitir 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 establecer el Manual Administrativo de

[271] **Articulo 6 sección A.III** "Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos."
Articulo 6 sección A.VIII. "La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio… responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley… El organismo garante tiene competencia para conocer de los asuntos relacionados con el acceso a la información publica y la protección de datos personales de cualquier autoridad, entidad, órgano y organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial…"
Articulo 73 fracción XXIX-S El Congreso tiene facultad … Para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno
[272] http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011
[273] Acuerdo publicado en: http://dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014
[274] Ver http://www.diputados.gob.mx/LeyesBiblio/ref/lftaipg.htm
[275] El Reglamento se encuentra en
http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf
[276] Ver http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf

Aplicación General en dichas materias[277], sobre todo en lo señalado en los artículos 5, fracción I, 13 y 28[278].

Se trata de una amplia lista de normatividad, tanto a nivel federal[279], como estatal y local, que es necesaria tomar en consideración, así como el hecho de que están pendiente la Ley General reglamentaria en materia de protección de datos personales en posesión de los sujetos obligados del sector público, a la que ya hemos hechos referencia.

6.1.3. Regulaciones existentes a nivel mundial que contemplan requisitos de protección de datos personales para el cómputo en la nube

Anteriormente se ha hecho referencia a las distintas normativas y lineamientos internacionales en materia de datos personales y aquellos con enfoque a la protección de los datos personales en el Cloud Computing, lo que incluía, entre otros, Estados Unidos, la Unión Europea, China, India, Japón, así como la inclusión de una relación de todas las leyes y reglamentos de protección de datos aprobados en

---

[277] Ver http://dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

[278] Artículo 5.- El PETIC se integrará con las Iniciativas y Proyectos de TIC que determinen las Instituciones, sujetándose al artículo anterior, para lo cual atenderán lo siguiente:
I. Favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, teniendo en consideración la seguridad de la información;
Artículo 13.- En el caso de servicios de Centros de Datos, las Instituciones, deberán observar lo siguiente:…
II. 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;…
IV. Analizar el alojamiento de su infraestructura de operación 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;
V. Almacenar y administrar en los Centros de Datos que se encuentren en las instalaciones de las Instituciones, los datos considerados de seguridad nacional, seguridad pública e información reservada y confidencial, conforme a la normatividad aplicable;…
El artículo 28 clasifica la información de acuerdo al grado de sensibilidad de ésta.

[279] Al respecto, puede verse también el marco normativo en la materia, disponible en la dirección de Internet del IFAI http://inicio.ifai.org.mx/_catalogs/masterpage/marcoNormativo.aspx

América Latina, siendo el común denominador que en la medida en que el uso del cómputo en la nube suponga un tratamiento de datos personales, quedará sujeto a la normatividad aplicable.

Es decir, si bien no se han identificado regulaciones específicas en materia de protección de datos personales para el cómputo en la nube, cabe señalar que las normas sobre protección de datos personales existentes son aplicables al cómputo en la nube, en la medida en que el uso de dichos servicios implica un tratamiento de datos personales.

Teniendo en consideración lo anterior, las regulaciones existentes señaladas anteriormente son las que aplican al cómputo en la nube en cada caso, en la medida en que la prestación de servicios de cómputo en la nube implique un tratamiento de datos personales, si bien no se encuentran referencias específicas y/o expresas al cómputo en la nube. Es decir, no se han identificado leyes específicas en materia de protección de datos personales sobre el cómputo en la nube, ya que con carácter general los diferentes marcos reguladores actuales de la protección de datos personales aplican a los servicios de cómputo en la nube.

Además de toda la normatividad sobre protección de datos personales ya indicada en este documento, sería posible señalar algunos recursos disponibles actualmente y que pueden servir para identificar país por país las diferentes normas de protección de datos personales, y que son los que se indican a continuación:

a) Data Protection Laws of the World: (repertorio de leyes de protección de datos en el mundo)[280], preparado por el despacho de abogados DLA Piper[281], que incluye información sobre diferentes aspectos (definiciones, autoridad de protección de datos, oficiales de protección de datos, obtención y tratamiento, transferencia, seguridad, notificaciones de brechas de seguridad, cumplimiento y privacidad

[280] El repertorio está disponible en el vínculo de Internet http://www.dlapiperdataprotection.com/#handbook/world-map-section/c1_AR

[281] Sobre DLA Piper puede verse más información en http://www.dlapiper.com/

online), pero que no incluye un apartado específico como tal relativo al cómputo en la nube[282].

Los diferentes aspectos en materia de protección de datos personales a los que se refiere el repertorio citado son los que resultan aplicables, en cada país, al cómputo en la nube.

b) Lista global sobre cómputo en la nube de BSA (2013 BSA Global Cloud Computing Scorecard)[283]: Preparada por BSA[284] y en la que se analiza el marco normativo, no sólo en materia de protección de datos personales sino también en materia de seguridad, cibercrimen, propiedad intelectual, estándares y normas de armornización internacional, libre comercio e infraestructura, de un total de veinticuatro (24) países[285].

En materia de protección de datos personales, BSA dedica un apartado específico a esta cuestión prestando atención a cuestiones tales como la existencia de normativa sobre protección de datos personales, si hay una autoridad de protección de datos o autoridad, si aplica algún requisito de registro del responsable del tratamiento, si hay requisitos aplicables a la transferencia internacional de datos así como si hay normas específicas de notificación de brechas o violaciones de seguridad[286].

En cualquier caso, la guía no hace referencia a ninguna norma específica sobre protección de datos personales para el cómputo en la nube, salvo por lo que se refiere al caso de Corea, sobre el que se incluye una mención a una propuesta de Ley sobre el cómputo en la

---

[282] El repertorio completo puede encontrarse en la siguiente dirección de Internet

[283] A la que puede accederse a través de la dirección de Internet http://cloudscorecard.bsa.org/2013/index.html

[284] En relación con BSA, puede verse más información en la dirección de Internet http://www.bsa.org/?sc_lang=es-MX

[285] La lista de países es la siguiente: Alemania, Argentina, Australia, Brasil, Canadá, China, Corea, España, Estados Unidos, Francia, India, Indonesia, Italia, Japón, Malasia, México, Polonia, Reino Unido, Rusia, Singapur, Sudáfrica, Tailandia, Turquía y Vietnam.

[286] La lista completa de BSA puede verse en la dirección de Internet http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf

nube[287]. Se trata de la *Proposed Bill for the Development of Cloud Computing and Protection of Users*[288].

Por lo tanto, tampoco en esta lista de países se encuentran regulaciones específicas en materia de protección de datos personales para el cómputo en la nube, más que la lista de normas sobre protección de datos personales aplicables al cómputo en la nube en los términos que ya hemos indicado.

c) GSR 2012 Discussion paper: The cloud: Data Protection and Privacy, Whose cloud is it Anyway? *(GSR 2012 documento para el debate: La nube: Protección de datos y Privacidad: ¿De quién es la nube en cualquier caso?)*[289]: Se trata de un documento[290] relevante ya que hace referencia a la normatividad sobre protección de datos personales en Europa, Estados Unidos, Canadá, Brasil, Sudáfrica, Arabia Saudí, Emiratos Árabes Unidos, India y Japón.

De nuevo, por lo que se refiere a protección de datos personales, el documento se centra en aspectos relacionados con el cómputo en la nube, tales como las transferencias internacionales de datos, pero no en el cómputo en la nube específicamente ya que la normativa sobre protección de datos personales aplica en general y no se prevén requisitos específicos sobre el cómputo en la nube en dichas normativas.

Este mismo documento cita[291], a su vez, que son un total de 89 países los que han adoptado leyes de protección de datos y

[287] Véase la referencia específica en el caso de Corea en la lista, indicada en la nota a pie anterior. Página 6.
[288] Cabe señalar que salvo la referencia incluida en la lista de BSA no se encuentra ninguna referencia adicional a dicha propuesta que permita confirmar que finalmente haya sido aprobada.
[289] GSR son las siglas en inglés de *Global Symposium for Regulators*. En español, se trata del Simposio Mundial para Organismos Reguladores que constituye un foro de reunión para los jefes de los organismos nacionales de reglamentación de las telecomunicaciones/TIC de todo el mundo.
[290] El citado documento, en inglés, puede verse en la dirección de Internet http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Privacy_Liston_6.pdf
[291] Véase al respecto la referencia que se incluye en la página 8 del documento, ya citado.

privacidad, haciendo referencia al documento titulado *Global Data Privacy Laws: 89 Countries, and Accelerating*[292].

En concreto, entre los aspectos a los que se refiere el documento para el debate de la Unión Internacional de las Telecomunicaciones (UIT), debe prestarse atención a las recomendaciones relativas a la protección de datos personales en el cómputo en la nube[293], siendo una de dichas recomendaciones que se busque un equilibrio entre el desarrollo del cómputo en la nube y la protección de datos personales, en el sentido de atender, por una parte, a que se produzca dicho desarrollo así como un libre flujo de la información y, por otra parte, el conocimiento informado y un control efectivo por parte de los titulares de los datos personales, para garantizar así su derecho fundamental.

Al respecto, el documento resalta la importancia de consultar activamente a la industria sobre el desarrollo de políticas relevantes para la prestación de servicios de cómputo en la nube[294], pudiendo extender dicha recomendación a que se atienda también a las cuestiones que se plantean para responsables y encargados del tratamiento que hacen uso de los servicios de cómputo en la nube y pudiendo desempañar la Secretaría de Economía un papel relevante al respecto como autoridad reguladora en materia de protección de datos personales.

Como conclusión, a lo largo del presente análisis se ha hecho referencia a la normativa sobre protección de datos personales de diferentes países que representan las diferentes aproximaciones a la materia que pueden encontrarse en varias regiones del mundo, debiendo destacar el hecho de que ninguna de ellas regule específicamente requisitos aplicables al cómputo en la nube, sino que se aplica con carácter general al cómputo en la nube. Además, se ha

---

[292] Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Disponible, en inglés, en la dirección de Internet http://ssrn.com/abstract=2000034

[293] En particular, páginas 29 y 30 del documento, apartados 5.1 y 5.2.

[294] En concreto, en el documento se indica que “CSPs and businesses should be actively consulted and involved in the development of policies relevant to the provision of cloud services.” Página 29.

hecho referencia a varios documentos elaborados por organizaciones internacionales o, en su caso, asociaciones, que también parten de prestar atención a diversos aspectos e implicaciones en materia de protección de datos personales relacionados con el cómputo en la nube, pero no a la regulación específica de requisitos sobre el cómputo en la nube. Es así que la lista de regulaciones existentes en el mundo en materia de protección de datos personales, aplicables al cómputo en la nube o a cualquier otro servicio tecnológico, queda incluida tanto por los países a los que se ha prestado atención específica como a las referencias hechas a otros documentos que se han incluido y que permiten llegar a la conclusión anteriormente indicada.

6.2. Principios de la protección de datos personales

Para tratar los principios de la protección de datos personales tenemos que partir de la diferencia en la regulación que se produce en los sectores público y privado a nivel federal[295], que básicamente en cuanto a los principios de la protección de datos personales es la siguiente:

Sector público	Sector privado
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental –LFTAIPG- (DOF de 11 de junio de 2002).	Ley Federal de Protección de Datos Personales en Posesión de los Particulares –LFPDPPP- (DOF de 5 de julio de 2010).
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental –Reglamento	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares –Reglamento de la

[295] En el caso del sector público a nivel estatal y municipal es necesario recordar que también hay normatividad específica sobre protección de datos personales, si bien el ámbito y alcance del presente estudio se centran en el nivel federal. No obstante, sobre la normatividad estatal en materia de protección de datos personales, puede verse la información disponible en la siguiente dirección de Internet http://inicio.ifai.org.mx/_catalogs/masterpage/otrasInstituciones/Legislación-Estatal-en-Materia-de-Transparencia.aspx y sobre la normatividad municipal, puede verse también la información disponible en http://inicio.ifai.org.mx/_catalogs/masterpage/otrasInstituciones/Legislación-Municipal-en-Materia-de-Transparencia.aspx

de la LFTAIPG- (DOF de 11 de junio de 2003)	LFPDPPP- (DOF de 21 de diciembre de 2011).
Lineamientos de Protección de Datos Personales (DOF de 30 de septiembre de 2005).	—

Ya que actualmente se espera que se tramite una Ley General de Protección de Datos Personales para el sector público a nivel federal, en virtud de la reforma al artículo 6 constitucional[296], se prestará atención a los principios de la protección de datos personales en virtud de la normatividad para el sector privado.

En concreto, el segundo párrafo de la fracción VIII del artículo 6 constitucional, en virtud de la reforma operada en el mismo por el Decreto referido, indica que:

> *"El organismo autónomo previsto en esta fracción, se regirá por la ley en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho."*

Atendiendo a las previsiones normativas en la Ley y el Reglamento es posible incluir el siguiente cuadro de resumen de los principios y deberes de la protección de datos personales:

[296] Véase el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia. El Decreto fue publicado en el Diario Oficial de la Federación el 7 de febrero de 2014 y puede verse en la siguiente dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

Principio	Art(s) de la LFPDPPP	Art(s) del Reglamento
Licitud	6 y 7	9, 10 y 44
Consentimiento	3, fracción IV, 6, 8 a 10, 36 y 37	9 y 11 a 22
Información	8, 12, 14 a 18, 23, 32 a 36, 43, fracción III, y transitorio tercero	9, 23 a 35, 40, 41, 43, 50, 90, 102 y transitorio segundo
Calidad	6 y 11	9 y 36 a 39
Finalidad	6, 12 y 13	9 y 40 a 43
Lealtad	6 y 7	9 y 44
Proporcionalidad	6 y 11	9, 45 y 46
Responsabilidad	6 y 14	9, 47 y 48

6.2.1. Licitud

Como establece el artículo 7 de la LFPDPPP, en virtud del principio de licitud *"los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas"* por la Ley y demás normatividad aplicable.

Y el Reglamento de la LFPDPPP, en su artículo 10, establece que *"el principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional."*

Entendiendo que la expectativa razonable de privacidad y la prohibición de obtención de datos personales por medios engañosos o fraudulentos quedan incluidas dentro de este principio.

Y en el caso de las fuentes de acceso público, el artículo 7 del Reglamento de la LFPDPPP indica que el tratamiento de los datos *"respetará la expectativa razonable de privacidad."*

Por tanto, la licitud obliga al responsable del tratamiento a velar porque los datos sean tratados cumpliendo con los principios previstos

en la normativa y en particular observando la expectativa razonable de privacidad y prohibiendo la obtención de datos personales por medios engañosos o fraudulentos.

Por último, como señalan Piñar Mañas y Ornelas Nuñez[297], *"el legislador ha previsto como infracción el incumplimiento de este principio, al indicar en la fracción IV, del artículo 63 de la LFPDPPP que supone la comisión de una infracción de "dar tratamiento a los datos personales en contravención a los principios establecidos en la" Ley, siendo sancionable con multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal."*

En conclusión, el cliente de servicios de cómputo en la nube, como responsable del tratamiento, tiene que velar por el cumplimiento de este principio de licitud, y conforme al ya citado artículo 14 de la LFPDPPP velará también porque así lo haga el prestador de servicios de cómputo en la nube, como encargado del tratamiento.

6.2.2. Consentimiento

Sobre el principio del consentimiento, Piñar Mañas y Ornelas Nuñez[298], indican que:

> *"el contenido del derecho fundamental a la protección de datos personales consiste en un poder de control sobre los datos personales que se concreta jurídicamente en varias facultades.*
> *El principio del consentimiento se encuentra en el primer artículo de la LFPDPPP, ya que se encuentra imbuido cuando se menciona que uno de los objetivos de la ley es otorgar la autodeterminación informativa."*

Por consentimiento, según la definición dada en la fracción IV, del artículo 3 de la LFPDPPP, se entiende la: *"Manifestación de la voluntad*

---

[297] Véase Piñar Mañas, José Luis y Ornelas Nuñez, Lina, *Los principios de la protección de datos personales,* en La Protección de Datos Personales en México, edit. Tirant Lo Blanch, México, 2013. Pág. 62.
[298] Op. ya citada. Pág. 62.

del titular de los datos mediante la cual se efectúa el tratamiento de los mismos."

El consentimiento, como manifestación de voluntad del titular de los datos, según indica el artículo 12 del Reglamento de la LFPDPPP, debe reunir las siguientes características:

Aspecto	**Previsiones en el art. 12 del Reglamento de la LFPDPPP**		
Consentimiento	Obtención del consentimiento tácito o expreso.		
Características	Libre	Fracc. I	*"Sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular."*
	Específica	Fracc. II	*"Referida a una o varias finalidades determinadas que justifiquen el tratamiento."*
	Informada	Fracc. III	*"Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento."*

Además, en el caso del consentimiento expreso, el último párrafo del artículo 12 del Reglamento de la LFPDPPP indica que: *"deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento."*

En relación con las formas del consentimiento en protección de datos personales, hay que distinguir entre el consentimiento expreso y tácito, de manera que tal y como resume Recio Gayo[299] puede indicarse lo siguiente:

[299] Recio Gayo, Miguel, *Esquemas de la Ley Federal de Protección de Datos Personales y su Reglamento*, edit. Tirant Lo Blanch, México, 2013. Pág. 31.

— Consentimiento tácito

Consentimiento tácito	Art(s).	Previsiones
Obtención de los datos personales **directa o personalmente de su titular**	14, párrafo primero de la LFPDPPP	El responsable deberá: • Poner a disposición del titular el aviso de privacidad previamente a su obtención; • El aviso de privacidad deberá contener un mecanismo para que, en su caso, el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.
Obtención de los datos personales **de manera indirecta**	14, párrafo segundo de la LFPDPPP	**Y tenga lugar un cambio de finalidades que fueron consentidas en la transferencia:** • El responsable deberá poner a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales.
El aviso de privacidad no se haga del conocimiento del titular de manera directa o personal		El titular tendrá un **plazo de cinco días** (hábiles) para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.

— Consentimiento expreso

Consentimiento expreso	Art(s).	Previsiones
En general	16 del Reglamento	Cuando el consentimiento expreso sea exigido en términos de una disposición legal o reglamentaria, el responsable deberá facilitar al titular un medio sencillo y gratuito para que, en su caso, lo pueda manifestar.
Consentimiento verbal	18 del Reglamento	(Véanse las definiciones y lo ya indicado anteriormente).
Consentimiento tácito	19 del Reglamento	

Y es el responsable quien tiene que asegurarse de obtener el consentimiento necesario en su caso, para tratar lícitamente los datos personales. En este sentido, tal y como indica el artículo 8 de la LFPDPPP, en su primer párrafo: *"Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley."*

En concreto, por lo que se refiere a las excepciones a la necesidad del consentimiento para el tratamiento de datos personales, el artículo 10 de la LFPDPPP indica que:

> *"No será necesario el consentimiento para el tratamiento de los datos personales cuando:*
> *I. Esté previsto en una Ley;*
> *II. Los datos figuren en fuentes de acceso público;*
> *III. Los datos personales se sometan a un procedimiento previo de disociación;*
> *IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;*
> *V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;*

VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o
VII. Se dicte resolución de autoridad competente."

En su *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[300], el IFAI se refiere al principio del consentimiento y, a modo de resumen, hace referencia a las siguientes obligaciones ligadas al principio del consentimiento[301]:

*"**1.** Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 10 de la LFPDPPP;*
***2.** Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad;*
***3.** Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito;*
***4.** Solicitar el consentimiento expreso para los datos personales financieros o patrimoniales, en los casos que no se actualice alguna de las causales del artículo 10 de la LFPDPPP;*
***5.** Solicitar el consentimiento expreso y por escrito para los datos personales sensibles, en caso de que no se actualice alguno de los supuestos del artículo 10 de la LFPDPPP;*
***6.** Solicitar el consentimiento expreso o expreso y por escrito cuando así lo requiera una ley o reglamento, se acuerde con el titular o lo determine conveniente el responsable;*
***7.** Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento;*

[300] Publicada en Julio de 2014 y disponible en la dirección de Internet http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf
[301] Págs. 24 y 25 de la citada Guía.

8. *Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular y no se actualiza alguno de los supuestos previstos en el artículo 10 de la LFPDPPP;*
9. *Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta y no se actualiza alguno de los supuestos previstos en el artículo 10 de la LFPDPPP;*
10. *Implementar medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y por escrito);*
11. *Llevar un control para identificar a los titulares que negaron su consentimiento y a las finalidades concretas para las cuales no se podrán tratar los datos personales;*
12. *Esperar el plazo de cinco días hábiles que señala el artículo 14 del Reglamento de la LFPDPPP, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito;*
13. *Generar pruebas para acreditar que se cumplió con el principio de consentimiento, y*
14. *Solicitar el consentimiento si hubo cambios en las finalidades informadas en el aviso de privacidad y éstas lo requieren por no actualizarse alguno de los supuestos previstos en el artículo 10 de la LFPDPPP.”*

En el caso del uso de servicios de cómputo en la nube, partiendo de que el cliente, como responsable del tratamiento, hace uso de los servicios que le proporciona el prestador de servicios de cómputo en la nube, como responsable del tratamiento, dicho tratamiento no requiere del consentimiento del titular de los datos personales, ya que el acceso a los datos personales por el encargado del tratamiento, para prestar un servicio al responsable, no requiere de dicho consentimiento.

No obstante, si en lugar de un acceso a los datos personales del responsable del tratamiento, el cliente, para prestarle un servicio por el

encargado del tratamiento, el prestador de servicios de computación en la nube, lo que hubiera entre ambos fuera una transferencia de datos personales, ésta sí puede requerir del consentimiento del titular de los datos personales, salvo que concurra alguna de las excepciones previstas en el artículo 37 de la LFPDPPP[302].

6.2.3. Información

Como indica la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares* del IFAI[303] en relación con el principio del consentimiento:

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

Y el citado aviso de privacidad es definido en la fracción I, del artículo 3 de la LFPDPPP como el: *"documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley."*

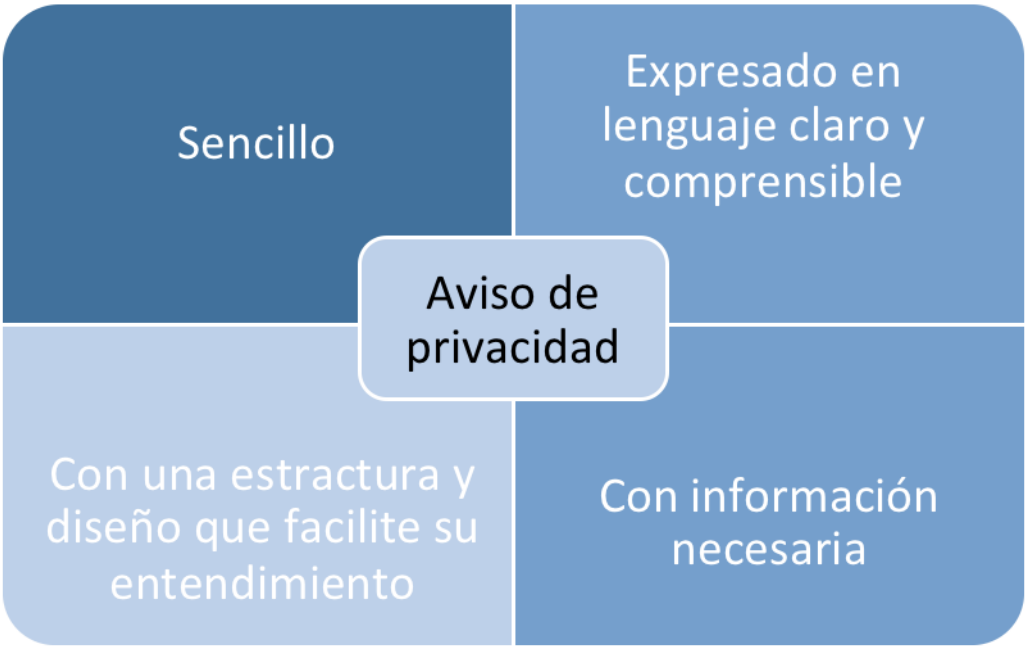
---

[302] En concreto, el artículo 37 de la LFPDPP indica lo siguiente:

> *"Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:*
> *I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;*
> *II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;*
> *III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;*
> *IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;*
> *V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;*
> *VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y*
> *VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular."*

[303] Ya citada. Pág. 32.

En relación con las características del aviso de privacidad, el artículo 24 del Reglamento de la LFPDPPP indica que éste deberá caracterizarse por ser:



En relación con el aviso de privacidad, es necesario tomar en consideración los Lineamientos del Aviso de Privacidad[304], emitidos por la Secretaría de Economía en su carácter de autoridad reguladora y en coadyuvancia con el IFAI.

Como indica la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares* del IFAI[305], *"[e]s importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad."*

Respecto al aviso de privacidad, como instrumento para cumplir con el principio de información, es conveniente tomar en consideración que el IFAI ha elaborado y ha puesto a disposición de los sujetos

[304] Fueron publicados en el Diario Oficial de la Federación el 17 de enero de 2013.
[305] Ya citada. Pág. 32.

obligados, a través de su sitio web[306], las siguientes herramientas y modelos[307]:

1. El Generador de Avisos de Privacidad (GAP);
2. La guía El ABC del Aviso de Privacidad;
3. El formato de auto-evaluación de avisos de privacidad para responsables;
4. Modelo de aviso de privacidad corto para video vigilancia; y
5. Modelo de aviso de privacidad simplificado en video.

Además, la citada *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, incluye una detallada explicación de los elementos informativos que debe contener cada una de las modalidades del aviso de privacidad; la explicación de cuándo hacer uso de cada una de estas modalidades y en qué momento poner a disposición del titular el aviso de privacidad, de manera que el responsable del tratamiento puede tomar en consideración la misma a efecto de cumplir con dicho principio.

En cuanto a las obligaciones ligadas al principio de información, también el IFAI, en la citada Guía, las resume de la siguiente manera[308]:

> *"**1.** Poner a disposición de los titulares el aviso de privacidad en los términos que fije la LFDPPP, su Reglamento y los Lineamientos del Aviso de Privacidad, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales;*
>
> ***2.** Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular;*
>
> ***3.** Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no*

[306] Véase http://www.ifai.org.mx

[307] Véase la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, ya citada, en la página 32.

[308] Véase la Guía, ya citada, en sus páginas 39 y 40.

requiera el consentimiento, o bien de una fuente de acceso público;

4. *Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para la finalidad para la que se obtuvieron (aprovechamiento), cuando éstos no se hayan obtenido de manera directa del titular, el tratamiento no requiera del contacto con él y se cuente con datos para contactarlo;*

5. *Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente;*

6. *Redactar el aviso de privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento, y atendiendo lo siguiente: no usar frases inexactas, ambiguas o vagas; tomar en cuenta los perfiles de los titulares; no incluir textos o formatos que induzcan al titular a elegir una opción en específico; no pre-marcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles;*

7. *Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice;*

8. *Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales;*

9. *Demostrar el cumplimiento del principio de información, en caso de que así se requiera;*

10. *Cuando se utilice la modalidad* ***integral*** *del aviso de privacidad, incluir todos los elementos informativos previstos en el Vigésimo de los Lineamientos del Aviso de Privacidad, con las características establecidas en los lineamientos Vigésimo primero a Trigésimo tercero;*

11. *Cuando se utilice la modalidad* ***simplificado*** *del aviso de privacidad, incluir todos los elementos informativos previstos en el Trigésimo cuarto al Trigésimo séptimo de los Lineamientos;*

12. *Cuando se utilice la modalidad* ***corto*** *del aviso de privacidad, incluir todos los elementos informativos previstos por el Trigésimo octavo al Cuadragésimo primero de los Lineamientos;*
13. *Utilizar la versión integral del aviso de privacidad cuando los datos personales sean obtenidos* ***personalmente*** *de los titulares;*
14. *Utilizar la versión simplificada del aviso de privacidad cuando los datos personales sean obtenidos* ***directamente*** *de los titulares. En este caso, el responsable podrá optar por poner a disposición de los titulares el aviso de privacidad integral, según lo considere conveniente;*
15. *Utilizar la versión corta del aviso de privacidad corto, únicamente cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales obtenidos también sean mínimos;*
16. *Elaborar y tener disponible para su consulta el aviso de privacidad integral, con independencia de que se ponga a disposición de los titulares el aviso de privacidad en su versión simplificada o corta previo a la obtención o aprovechamiento de los datos personales;*
17. *No establecer cobros para la consulta del aviso de privacidad;*
18. *Cuando así ocurra, informar en su portal de Internet, a través de una comunicación o advertencia colocada en un lugar visible y a la cual se pueda acceder desde el momento en que se ingresa a dicho portal, que están siendo utilizadas tecnologías de rastreo, que a través de éstas se pueden recabar datos personales y la forma en cómo se pueden deshabilitar, y*
19. *Poner a disposición de los titulares* ***un nuevo*** *aviso de privacidad en los siguientes casos: (i) cambie la identidad del responsable; (ii) se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular; (iii) se requiera tratar los datos personales para nuevas finalidades que requieran el consentimiento del titular, y (iv) se requiera realizar nuevas transferencias que requieran el consentimiento del titular."*

Al igual que ocurre con el resto de principios de la protección de datos personales, corresponde al responsable del tratamiento, que será

con carácter general el cliente de los servicios de cómputo en la nube, cumplir y velar por el cumplimiento del principio de información, de manera que tendrá que adoptar las medidas necesarias a tal fin.

Es necesario recordar que cuando se firma un contrato u otro instrumento jurídico, el artículo 50 del Reglamento de la LFPDPPP, indica que *"Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente."*

6.2.4. Calidad

Conforme al Dictamen de la Comisión de Gobernación sobre el Proyecto con Decreto de la LFPDPPP[309], cabe señalar que *"el principio de calidad del dato ha de entenderse específicamente vinculado con la veracidad y exactitud en la que se mantienen los datos personales, de forma que aquél refleje realmente de forma fiel, la realidad de la información tratada. Ello conlleva un doble esfuerzo para los particulares responsables: por un lado deberán asegurarse en el momento de la recogida de la información, sobre todo cuando la misma no procede directamente del titular, de que aquella resulta exacta y actualizada; por otro debería, siempre que ello sea posible, adoptar las medidas razonables para que la información responda a esa veracidad mientras persiste en su tratamiento."*

Como indican Piñar Mañas y Ornelas Nuñez[310] en relación con el principio de calidad, cabe señalar que *"[l]a falta de calidad de los datos no es un asunto menor ya que puede acarrear distintos grados de afectación en la esfera de otros derechos y libertades de los individuos,*

[309] Se trata de la versión final del Dictamen con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, disponible en la dirección de Internet
http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf

[310] Op. ya citada. Pág. 78.

ya que un dato inexacto, equivale a un dato falso. Asimismo, de cara a la industria, las afectaciones pueden traducirse en un mal servicio a los clientes y fala de competitividad."

El principio de calidad se concreta, tal y como se menciona el IFAI en su *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, en que los datos personales tratados sean[311]:

> *"• Los datos personales son **exactos** cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Por ejemplo, un dato no sería exacto si se registra en la base de datos que una persona cuenta con Doctorado en derecho, si el título que en realidad tiene es una Maestría en derecho.*
> *• Los datos personales están **completos** cuando no falta ninguno de los que se requiera para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Por ejemplo, los datos de salud del titular están completos cuando el expediente médico contiene todos los documentos clínicos e información que debe estar integrada al mismo.*
> *• Los datos personales son **pertinentes** cuando corresponden efectivamente al titular. Por ejemplo, los datos del adeudo son pertinentes cuando corresponden al deudor y no a una homonimia.*
> *• Los datos están **actualizados** cuando están al día y corresponden a la situación real del titular. Por ejemplo, el número telefónico que se tiene registrado en la base de datos está actualizado cuando, efectivamente, corresponde al titular con el que está vinculado.*
> *• Los datos personales son **correctos** cuando cumplen con todas las características anteriores, es decir, son exactos, completos, pertinentes y actualizados."*

[311] Véase la citada Guía en su página 58.

Y en relación con las obligaciones ligadas a este principio, la citada Guía del IFAI a la que hacemos referencia, indica lo siguiente[312]:

> *"**1.** Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, pertinentes, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación;*
> ***2.** Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo;*
> ***3.** Eliminar los datos personales relacionados con incumplimiento de obligaciones contractuales en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento;*
> ***4.** Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales;*
> ***5.** Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación;*
> ***6.** Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales, y*
> ***7.** En caso que se requiera, demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación."*

De nuevo, en el caso de los servicios de cómputo en la nube, el cliente, como responsable del tratamiento es quien tiene que asegurarse del cumplimiento de este principio así como de velar de que

[312] Guía ya citada. Pág. 61

el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumple con el mismo.

6.2.5. Finalidad

El principio de finalidad, según establece la Comisión de Gobernación en su Dictamen sobre el Proyecto de Decreto, es *"la manifestación esencial de la protección de la privacidad en relación con el tratamiento de los datos personales se funda en que el tratamiento únicamente sea llevado a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del responsable. Junto con esta regla general, se ha venido reconociendo la posibilidad de proceder a este tratamiento para otros fines, siempre que los mismos* ***no sean incompatibles*** *con los que motivaron el tratamiento inicial del dato."*

Piñar Mañas y Ornelas Nuñez[313] indican que *"[e]ste principio debe ponerse en relación con otros principios ya que la calidad de los datos pasa porque sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados, tal y como señala el párrafo primero del artículo 11 de la LFPDPPP. Se encuentra también relacionado con el principio del consentimiento, ya que éste, cuando sea necesario, se obtendrá del titular de los datos personales en atención a la finalidad o finalidades indicadas en el aviso de privacidad, lo que supone que dicho principio esté relacionado también con el de información."*

En relación con este principio, el IFAI en su Guía[314], indica que: *"La finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad."*

[313] Op. ya citada. Págs. 79 y 80.
[314] Ya citada. Pág. 52.

En cuanto a la finalidad o finalidades del tratamiento es necesario distinguir entre finalidades primarias y secundarias del tratamiento, indicando también el IFAI en su Guía que[315]: *"De acuerdo con el Reglamento de la LFPDPPP hay dos tipos de finalidades: (i) aquéllas que dan origen y son necesarias para la relación jurídica entre el titular y el responsable, a las cuales identificamos como primarias, y (ii) todas las demás que no cumplan con esta condición, a las que llamaremos secundarias o accesorias."*

Por lo que se refiere a las obligaciones ligadas al cumplimiento del principio de finalidad del tratamiento, en su Guía[316], el IFAI indica que son las siguientes:

> *"**1.** Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste;*
> ***2.** Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas;*
> ***3.** Identificar y distinguir en el aviso de privacidad entre las finalidades primarias y secundarias;*
> ***4.** Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias;*
> ***5.** Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información para finalidades secundarias;*
> ***6.** No condicionar el tratamiento para finalidades primarias, a que se puedan llevar a cabo las finalidades secundarias;*
> ***7.** Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos."*

[315] Véase la nota a pie de página anterior.
[316] Guía ya citada. Págs. 53 y 54.

En definitiva, el responsable del tratamiento tiene que adoptar las medidas necesarias para cumplir con este principio y en el caso de que el responsable sea cliente de servicios de cómputo en la nube, es también quien tiene que asegurarse y velar porque el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, cumpla con dicho principio cuando trate los datos personales por cuenta del responsable.

6.2.6. Lealtad

Tal y como indica el Dictamen de la Comisión de Gobernación en su Dictamen sobre el Proyecto de Decreto por el que se aprobó el Reglamento de Protección de Datos en posesión de los particulares, este principio supone *"impedir la creación de bases de datos que contengan datos personales sensibles, sin que esta acción se justifique atendiendo a su finalidad y que ésta sea legítima, concreta y acorde con las actividades o fines explícitos que procura el sujeto regulado."*

Además de la prohibición de crear bases de datos que contengan datos personales sensibles, la lealtad en el tratamiento debe entenderse como la obligación del responsable de tratar los datos observando los principios de licitud, proporcionalidad, calidad, finalidad, consentimiento e información. Es decir, la lealtad está interrelacionada con el resto de los principios.

Es así que el artículo 44 del Reglamento de la LFPDPPP indica que *"el principio lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad"*, habiendo sida analizada ésta ya en el principio de licitud al que nos remitimos.

Será, de nuevo, el cliente de servicios de cómputo en la nube quien, como responsable del tratamiento, tenga que velar por el cumplimiento de este principio y porque el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, cumpla también con el mismo.

6.2.7. Proporcionalidad

El Dictamen de la Comisión de Gobernación sobre el Proyecto de Decreto[317] indicaba que este principio *"se encuentra directamente relacionado con el de finalidad"* y atendiendo al análisis efectuado por los derechos regionales o nacionales cabe analizarlo *"desde dos perspectivas distintas, aunque complementarias: Por una parte, los datos sólo deberían ser los adecuados o necesarios para la finalidad que justifica el tratamiento (principio de proporcionalidad en sentido estricto); por otra, quien procede al tratamiento de los datos deberá analizar las finalidades que justifican el tratamiento, de modo que sólo debería tratar la mínima cantidad de información necesaria para conseguir la finalidad perseguida (principio de minimización)."*

Sobre el principio de proporcionalidad, el artículo 13 de la LFPDPPP indica que: *"El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad."*

En relación con este principio, como indican Piñar Mañas y Ornelas Núñez[318]: *"Cabría, por tanto, preguntarse cuándo son proporcionales los datos personales, lo que tiene que ponerse en relación con la finalidad del tratamiento. Es decir, los datos serán proporcionales si son los necesarios, adecuados y relevantes en atención a la finalidad con la que vayan a ser tratados. De esta manera, pedir más datos personales que los que sean necesarios o pedir datos personales que nada tienen que ver con la finalidad para la que van a ser tratados, supone que el tratamiento no resulte proporcional, incumpliendo así con dicho principio lo que determina que el tratamiento sea ilícito."*

El IFAI, en relación con las obligaciones ligadas con este principio, indica en su Guía[319] que son las relativas a:

---

317 Ya citado.
318318 Op. ya citada. Págs. 86 y 87.
319 Ya citada. Pág. 50.

> *"**1.** Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron;*
> ***2.** Tratar el menor número posible de datos personales;*
> ***3.** Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles, y*
> ***4.** Crear bases de datos con datos personales sensibles sólo cuando (i) obedezca a un mandato legal; (ii) se justifique para la seguridad nacional, el orden, la seguridad y la salud públicos, así como derechos de terceros, o (iii) el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga."*

Y al igual que ocurre en el caso de los demás principios de la protección de datos personales, cuando el cliente, como responsable del tratamiento, haga uso de servicios de cómputo en la nube que le sean proporcionados por un proveedor, que actúa como encargado del tratamiento, le corresponde cumplir con dicho principio, velando que este último también lo haga y evitando así un tratamiento ilícito de los datos personales.

6.2.8. Responsabilidad

El reiterado Dictamen de la Comisión de Gobernación sobre el Proyecto de Decreto indica que el principio de responsabilidad *"debe entenderse en el sentido de que corresponderá a la entidad o persona responsable el deber de velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento. Este principio es la verdadera garantía para el titular de los datos quien deposita su confianza en el responsable, mismo que deberá tomar todas las previsiones para que los datos sean tratados de acuerdo con la voluntad del dueño de la información y bajo las medidas de seguridad que se prevean por la vía contractual. Así, dado que existe un tráfico de datos intenso y en muchas ocasiones este se da fuera de las fronteras de nuestro país, el ciudadano tendrá la tranquilidad de que si su*

información ha trascendido a manos de terceros en otras latitudes, éste estará enterado de las cautelas con que debe tratar su información."

En la LFPDPPP, este principio se plasma en el artículo 14 que establece lo siguiente: *"El responsable velará por el cumplimiento de los principios de protección de datos personales."*

De manera que el responsable, para cumplir con la obligación que le impone la LFPDPPP tendrá que adoptar las medidas necesarias para su aplicación y lo hará también cuando los *"datos fueran tratados por un tercero a solicitud del responsable".*

Este tercero tiene que entenderse como un encargado del tratamiento, indicando al respecto el Reglamento de la LFPDPPP en su artículo 47 que el principio de responsabilidad obliga al responsable a velar y responder por el tratamiento de datos personales *"por aquéllos que haya comunicado a un encargado, ya sea que éste último se encuentre o no en territorio mexicano."*

Es decir, el principio de responsabilidad se concreta en la obligación del responsable de velar y responder por el tratamiento de los datos personales que estén bajo su custodia o posesión o que sean tratados por un encargado al que los haya remitido.

En relación con este principio, indica el IFAI en su *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[320] que *"cierra el círculo con relación a los principios que regulan la protección de los datos personales. A este principio se le conoce también como el principio de "rendición de cuentas", ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales."*

[320] Ya citada. Pág. 65.

Es necesario tomar en consideración que el artículo 48 cita algunas medidas que el responsable podrá adoptar para cumplir con este principio.

Por su parte, el IFAI, en la Guía a la que venimos haciendo referencia, resume las obligaciones de este principio de la siguiente manera[321]:

> *"**1.** Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados;*
> ***2.** Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y*
> ***3.** Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento."*

En relación con los servicios de cómputo en la nube, la observancia de este principio implica que, entre otros aspectos, el cliente, como responsable del tratamiento, adopte las medidas necesarias para identificar riesgos en materia de protección de datos personales; medidas para minimizar dichos riesgos y a su vez otras medidas para velar porque el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumple con sus obligaciones.

Por lo tanto, el cliente, como responsable del tratamiento, tendrá que verificar que el encargado del tratamiento cumple con sus obligaciones, bien sea a través de supervisar cómo presta sus servicios o recurrir a terceros, ya sean auditores o certificadores, para proceder a dicha verificación. Al respecto, las certificaciones emitidas por terceros pueden ser un instrumento adecuado para llevar a cabo dicha verificación o al menos tener una prueba de que se han adoptado medidas[322]. Y en este sentido la autorregulación puede jugar un papel

---

[321] Páginas 66 y 67 de la citada Guía.

[322] Sobre esta cuestión, además de certificaciones ya existentes, es posible hacer referencia a la ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection

fundamental en el caso de prestación de servicios de cómputo en la nube, por lo que es una cuestión a tomar en consideración a la hora de desarrollar políticas públicas en la materia.

6.3. Roles de usuario como responsable del tratamiento y del prestador de servicios como encargado del tratamiento

A este tema ya nos hemos referido con cierto detalle en este estudio, y nos remitimos a lo ya dicho. No obstante podemos hacer ahora alguna consideración complementaria.

En la prestación de servicios de cómputo en la nube, desde el punto de vista de la normatividad sobre protección de datos personales, como regla general, ya que podrían darse otras relaciones, el usuario o cliente de los servicios es responsable del tratamiento y el prestador o proveedor de servicios actúa como encargado del tratamiento.

Al respecto, si tomamos en consideración las definiciones de responsable y encargado del tratamiento de la LFPDPPP y su Reglamento[323], es posible presentar la siguiente tabla:

Figura	Rol o papel	Definición	Referencia
Responsable del tratamiento	Cliente o usuario	*"Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales".*	Art. 3, fracción XIV de la LFPDPPP
Encargado del tratamiento	Prestador o proveedor de servicios	*"La persona física o jurídica que sola o conjuntamente con otras trate datos*	Art. 3, fracción IX de la

of personally identifiable information (PII) in public clouds acting as PII processors, de la que pueden verse algunos detalles disponibles en la siguiente dirección de Internet http://www.iso.org/iso/home/search.htm?qt=ISO+27018&sort=rel&type=simple&published=on

[323] El articulado de la LFPDPPP y su Reglamento pueden consultarse también en Piñar Mañas, José Luis y Recio Gayo, Miguel, *Código de Protección de Datos Personales México*, edit. Tirant Lo Blanch, México, 2013.

	de cómputo en la nube	*personales por cuenta del responsable."*	LFPDPPP
		"[E]s la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio."	Art. 49 del Reglamento de la LFPDPPP

Se atiende a las definiciones incluidas en la normatividad sobre protección de datos personales para el sector privado ya que en el caso del sector público, la vigente Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[324] no incluye estas definiciones y, en el caso de los Lineamientos de Protección de Datos Personales[325], la definición de encargado del tratamiento en el Lineamiento Tercero, fracción II como "El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales", no resulta acertada ya que dicho encargado del tratamiento es, como indica el artículo 49 del Reglamento de la LFPDPPP, una persona física o moral, pública o privada, ajena a la organización del responsable que trata datos personales por cuenta del mismo. Es decir, tiene que ser alguien ajeno a la organización del responsable que trate datos personales por su cuenta, sin tomar decisión alguna en el tratamiento de dichos datos personales.

[324] Publicada en el Diario Oficial de la Federación de 11 de junio de 2002.
[325] Publicados en el Diario Oficial de la Federación de 30 de septiembre de 2005.

Que el cliente de los servicios de cómputo en la nube sea responsable del tratamiento y el prestador de dichos servicios sea considerado como encargado del tratamiento es la norma también a nivel internacional. Al respecto, el ya citado Dictamen 5/2012 sobre el cómputo en la nube, del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[326], indica que: *"El dictamen se centra en la situación de una relación entre el responsable y el encargado, considerándose al cliente responsable y al proveedor, encargado."*

No obstante, podría haber otras situaciones en las que el proveedor de servicios actúe también como responsable, decidiendo sobre la finalidad del tratamiento de los datos personales, de manera que habría que atender de manera específica a dicha situación. Al respecto, el Dictamen 5/2012 que citamos, indica que: *"En los casos en que el proveedor actúa también como responsable del tratamiento, este debe cumplir requisitos adicionales."*

Por lo que se refiere a las figuras del responsable y el encargado del tratamiento, el responsable remite al encargado del tratamiento datos personales, sin que sea necesario a tal fin obtener el consentimiento del titular de los datos personales, de manera que el encargado se limita a prestar un servicio al responsable del tratamiento, sin decidir sobre el tratamiento de los datos personales.

Sobre el responsable del tratamiento, como señalan Del Conde Ugarte y Martínez Rojas[327], esta figura *"ha sido reconocida en diversas legislaciones como la persona física o moral que decide sobre la finalidad, contenido y uso de la información personal, en términos generales."*

---

[326] Ya citado.

[327] Del Conde Ugarte, Alejandro y Martínez Rojas, Edgardo; *Sujetos que intervienen en la relación jurídica que se genera derivado del tratamiento de los datos personales: caso del responsable, encargado y tercero* en *La Protección de Datos Personales en México*, obra coordinada por Piñar Mañas, José Luis y Ornelas Nuñez, Lina; edit. Tirant Lo Blanch, México, 2013.

Y continúan diciendo que *"[e]sta figura es de particular importancia dentro de los ordenamientos de protección de datos."*[328] En el caso del encargado del tratamiento, los autores citados indican que: *"Una figura diferente al titular de los datos y al responsable del tratamiento es la del encargado. Actualmente, esta figura tiene una amplia difusión y reviste una importancia notable en el tratamiento de los datos personales. Sin omitir mencionar que su complejidad se ha incrementado debido a la evolución de las Tecnologías de la Información y Comunicación, incluyendo el vertiginoso desarrollo del comercio electrónico."*[329]

Lo anterior implica que sea necesario tomar en consideración la diferente posición que tienen el responsable y el encargado del tratamiento, de manera que las relaciones que se establezcan entre las mismas y que impliquen un tratamiento de datos personales queden determinadas claramente, de manera que sus obligaciones y responsabilidades también estén claras y se evite cualquier tratamiento ilícito de datos personales como consecuencia del incumplimiento de sus obligaciones y/o de las garantías que son exigibles en virtud de que estemos ante una transferencia o una remisión de datos personales.

En conclusión, a la hora de contratar servicios de cómputo en la nube es necesario que las partes, de un lado el cliente y de otro lado el prestador de los servicios de cómputo en la nube, tengan claro su rol o papel desde el punto de vista de la normatividad sobre protección de datos personales, ya que ello determinará las obligaciones que les corresponden a uno y a otro así como, en su caso, la responsabilidad aplicable en caso de infracción. Y, por último, con carácter general se considera al cliente como responsable del tratamiento y al proveedor de servicios de cómputo en la nube como encargado del tratamiento, si bien en la práctica podrían darse otras situaciones que es necesario tomar en consideración.

[328] Op. ya citada. Pág. 146.
[329] Op. ya citada. Pág. 151.

6.4. El establecimiento del responsable y la ley aplicable al contrato

En cuanto a la ley aplicable al contrato, tomando en consideración que, tal y como venimos comentando, el cliente de servicios de cómputo en la nube será considerado como responsable del tratamiento y el proveedor de dichos servicios como encargado del tratamiento, el artículo 4 del Reglamento de la LFPDPPP, relativo al ámbito territorial de aplicación, indica que:

> *"El presente Reglamento será de aplicación obligatoria a todo tratamiento cuando:*
> *[…]*
> ***II.** Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano".*

Esto supone que el establecimiento del responsable del tratamiento en México, determine que las disposiciones del Reglamento, y específicamente las que se refieren en su caso al encargado del tratamiento, sean aplicables al prestador de servicios de cómputo en la nube con independencia del país en el que se encuentre situado éste.

Por tanto, aunque el prestador de servicios de cómputo en la nube, que actúa como encargado del tratamiento, esté establecido en Estados Unidos la Unión Europea o en Asia, al prestar servicios de *cloud* a un responsable del tratamiento establecido en México, tendrá que cumplir con la normatividad mexicana en materia de protección de datos personales y al responsable del tratamiento, en virtud de los artículos 14 de la LFPDPPP y 47 de su Reglamente, le corresponde cumplir con *"la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano."*

Es importante tomar en consideración si el responsable del tratamiento está establecido en México y dónde está establecido, en su caso, el encargado del tratamiento, ya que ello determinará qué ley o leyes son aplicables al contrato de servicios de cómputo en la nube. Igualmente, si el prestador de servicios de cómputo en la nube fuera un nuevo responsable del tratamiento, habrá que atender a las disposiciones aplicables a la transferencia, nacional o internacional, de datos personales y de nuevo el establecimiento de las partes determinará, en su caso, qué ley es aplicable al contrato correspondiente.

Por lo tanto, es importante contar con reglas claras, especialmente en el caso de MIPYMEs que, como clientes de grandes proveedores de servicios, pueden quedar desprotegidas en el caso de que el proveedor incluya cláusulas que establezcan una ley o jurisdicción a su favor, haciendo que el cliente renuncie por dicho contrato a su propio fuero. En definitiva, pueden plantarse cuestiones relativas a derecho de los contratos y prácticas comerciales que deben ser tomadas en consideración por la Secretaría de Economía, como autoridad reguladora.

6.5. Necesidad de un contrato que regule el acceso a los datos personales

Si bien nos hemos referido ya al hecho de que la prestación de servicios de *cloud* requiere de la celebración de un contrato[330], cabe señalar aquí que la LFPDPPP y su Reglamento requieren que la relación jurídica entre el responsable y el encargado del tratamiento conste, según indica específicamente el artículo 51 del Reglamento, en: *"cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido."*

[330] Véase al respecto lo ya dicho en el apartado relativo al artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que forma parte de la etapa 2 del presente análisis.

Es decir, la relación jurídica puede ser parte de un contrato (un acuerdo, convenio, cláusulas contractuales, anexos al contrato, etc.) que tenga por objeto regular la prestación de servicios u otras cuestiones entre el responsable y el encargado del tratamiento, o ser un contrato en sí mismo. Esto supone que, entre el cliente, como responsable del tratamiento, y el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, tenga que haber firmado un contrato u otro instrumento jurídico, ya que de otra forma no se cumpliría con las obligaciones que ambas partes tienen en virtud de la normatividad sobre protección de datos personales.

De lo que se trata en cualquier caso es de poder probar la existencia y alcance de la relación jurídica entre ambos por lo que se refiere al tratamiento de los datos personales que el responsable encomienda al encargado del tratamiento y, en caso de que fuera necesario, poder acreditar las instrucciones dadas a efectos de determinar la responsabilidad que pudiera surgir del tratamiento de los datos personales.

Al respecto, el artículo 53 del Reglamento de la LFPDPPP indica que: *"El encargado será considerado responsable con las obligaciones propias de éste, cuando:*

I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o

II. Efectúe una transferencia, incumpliendo las instrucciones del responsable.

Es decir, el contrato o relación jurídica existente entre las partes del mismo permite atribuir a cada una de las mismas la responsabilidad que les es exigible y que además consta en dicho documento, ya se encuentre este en papel o electrónico.

Además, el encargado tiene que cumplir con las obligaciones que le son exigibles, conforme a lo indicado en el artículo 50 del Reglamento de la LFPDPPP, que deberían constar en las cláusulas contractuales o instrumento jurídico que regule su relación jurídica con el responsable y a las que prestamos atención a continuación:

Fracción	Obligación del encargado del tratamiento
I	Tratar únicamente los datos personales conforme a las instrucciones del responsable.
II	Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
III	Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables.
IV	Guardar confidencialidad respecto de los datos personales tratados.
V	Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
VI	Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

En relación con las obligaciones que tiene el responsable respecto del encargado del tratamiento que trate datos personales a su cuenta y nombre, el IFAI, en su Guía de obligaciones de la LFPDPPP[331], indica que son las siguientes:

> *"**1.** Establecer la relación con el encargado a través de un instrumento jurídico que permita acreditar la existencia de la relación jurídica, su alcance y contenido;*
> ***2.** Fijar los acuerdos con el encargado con base en lo previsto en el aviso de privacidad que definió las condiciones del tratamiento de los datos personales;*
> ***3.** Contemplar en el instrumento que establezca la relación jurídica con el encargado, al menos, las obligaciones que prevé el artículo 50 de la LFPDPPP;*
> ***4.** Autorizar las subcontrataciones que realice el encargado, que involucren el tratamiento de datos personales;*

[331] Ya citada. Pág. 81.

5. *Contratar servicios de cómputo en la nube que cumplan, al menos, con las condiciones descritas en el artículo 52 del Reglamento de la LFPDPPP, y*
6. *Verificar que el encargado cumpla con sus obligaciones."*

Además, en virtud de lo dispuesto en los artículos 14 de la LFPDPPP y 50 de su Reglamento, *"los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente."*

No obstante, el encargado no incurrirá en responsabilidad cuando *"previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable"* (art. 53, último párrafo, del Reglamento de la LFPDPPP).

6.6. Subcontratación

Como ya sabemos, el Reglamento de la LFPDPPP dedica sus artículos 54 y 55, respectivamente, a la subcontratación y a la autorización de subcontratación. Es así que dichos artículos constituyen el régimen jurídico de la subcontratación[332].

En su Guía de obligaciones de la LFPDPPP[333], en relación con la subcontratación, el IFAI indica que: *"En la práctica se dan habitualmente casos en los que hay una subcontratación de servicios, cuando el encargado del tratamiento tiene que recurrir a su vez a otras personas físicas o empresas que le prestan algún servicio que implica el acceso a los datos personales del responsable. De acuerdo con el Reglamento de la LFPDPPP, el encargado puede llevar a cabo subcontrataciones, siempre que cuente con la autorización del responsable."*

[332] Es necesario recordar que a esta cuestión nos hemos referido ya, si bien queremos concretar aquí algunos aspectos del régimen de la subcontratación.
[333] Ya citada. Págs. 79 y 80.

Dicha autorización para la subcontratación, de acuerdo con lo previsto en el artículo 54 del Reglamento de la LFPDPPP, deberá cumplir con el requisito de realizarse en nombre y por cuenta del responsable. Y conforme al artículo 55 del citado Reglamento, la autorización podrá ser obtenida:

Supuesto	Autorización
Se haya previsto en la relación entre el responsable y el encargado del tratamiento	En este caso la autorización se entenderá como otorgada a través de lo estipulado en éstos.
No esté prevista en dicha relación	El encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

En cualquiera de estos dos supuestos, es importante tomar en consideración que tal y como indica el artículo 54 del Reglamento de la LFPDPPP *"[l]a persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado en la Ley, el presente Reglamento y demás disposiciones aplicables."*

Además, será el encargado del tratamiento, conforme a lo que indica el artículo 54 del Reglamento de la LFPDPPP quien *"deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido."* Y también le corresponde a dicho encargado, según indica el artículo 54 del citado Reglamento, cumplir con la obligación de *"acreditar que la subcontratación se realizó con autorización del responsable."*

En el caso de los servicios de cómputo en la nube, en la práctica dichas subcontrataciones son habituales y conocidas, de manera que es importante que el cliente, como responsable del tratamiento, se asegure de que el prestador de servicios de cómputo en la nube, como

encargado del tratamiento, sea transparente en relación con la cadena de subcontratación y debiendo considerarse como una buena práctica que el proveedor de servicios de cómputo en la nube.

Se trata de transparentar las subcontrataciones, cuestión a la que ya nos hemos referido al analizar el artículo 52 del Reglamento de la LFPDPPP, si bien queremos incluir aquí un ejemplo concreto de acción que suponga transparentar la cadena de subcontratación. En concreto, puede tratarse de que el encargado del tratamiento ponga a disposición de sus clientes, que son los responsables del tratamiento, una dirección de Internet donde informe de dichos subcontratistas, sin perjuicio de que además se dirija de alguna otra forma al cliente para informarle de los subencargados que puedan prestarle algún servicio y que tengan acceso a los datos personales.

Estos subcontratistas, en su caso, pueden ser personas que presten a su vez servicios al encargado del tratamiento, relacionados con el servicio de cómputo en la nube que preste con éste, y en la práctica es necesario tomar en consideración que dichos subcontratistas pueden encontrarse en cualquier lugar del mundo. Para garantizar que se cumpla con lo previsto en el artículo 54 del Reglamento de la LFPDPPP en cuanto a que *"[l]a persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado en la Ley, el presente Reglamento y demás disposiciones aplicables"*, sería conveniente, por ejemplo, que se exija al encargado del tratamiento que firme con dichos subcontratistas un contrato, cláusula contractual u otro instrumento jurídico, que permita extender dichas obligaciones a los mismos y tener un control sobre ellos en caso de incumplimiento. Se trata, por lo tanto, de que el proveedor de servicios de cómputo en la nube ofrezca garantías a sus clientes, de manera que pueda ser considerado también como una buena práctica de negocio y en materia de protección de datos personales.

6.7. Ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO)

El responsable del tratamiento, según indica el artículo 22 de la LFPDPPP, tiene que tratar los datos personales de manera que *"deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos"*, refiriéndose a los derechos de acceso, rectificación, cancelación y oposición (también conocidos como derechos ARCO).

En relación con los derechos ARCO, cabe señalar que el IFAI ha publicado dos guías prácticas dirigidas a los responsables del tratamiento así como, en su caso, a los titulares de los datos personales. Se trata, por una parte, de la *Guía práctica para ejercer el derecho a la Protección de Datos Personales*[334] y, por otra parte, la *Guía práctica para la atención al ejercicio de las solicitudes de los Derechos ARCO*[335]*.*

Respecto a los derechos ARCO, es necesario recordar que el párrafo segundo del artículo 16 de la Constitución indica lo siguiente: *"toda persona tiene derecho a la protección de sus datos personales,* ***al acceso, rectificación y cancelación*** *de los mismos, así como a manifestar su* ***oposición,*** *en los términos que fije la ley."*

Por lo que se refiere al desarrollo normativo de los derechos ARCO, la Ley dedica su Capítulo III, artículos 22 a 26, a los derechos de los titulares de los datos personales y su Capítulo IV, artículos 28 a 35, al ejercicio de estos derechos. Además, la Ley también dedica el Capítulo VII, artículos 45 a 58, al procedimiento de protección de derechos. Por su parte, el Reglamento dedica el Capítulo VII, artículos 87 a 112, a los derechos y su ejercicio, y el Capítulo VIII, artículos 113 a 127, al procedimiento de protección de derechos ante el IFAI.

---

[334] Disponible en la siguiente dirección de Internet
http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf
[335] Disponible en la siguiente dirección de Internet
http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

Por lo que se refiere al ejercicio de los derechos ARCO hay que tomar en consideración, con carácter general, que[336]:

Aspecto	Art(s).	Previsiones normativas
Sencillez	93 del Reglamento	El ejercicio de los derechos ARCO será sencillo.
Gratuidad del ejercicio		El ejercicio de los derechos ARCO será gratuito.
Costos a cubrir por el titular		El titular deberá cubrir únicamente los gastos de: • Envío; • Reproducción, y • En su caso, certificación de documentos
Costos de reproducción		No podrán ser mayores a los costos de recuperación del material correspondiente.
Costos por el derecho de acceso		En el caso del derecho de acceso, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.
Medios para la presentación de las solicitudes		El responsable no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio con costo.

[336] Véase, Recio Gayo, Miguel, op. ya citada, en cuanto a las características generales de los derechos ARCO. Págs. 51 y 52

Por lo que se refiere al contenido de cada uno de estos derechos de acceso, rectificación, cancelación y oposición, las siguientes tablas[337]:

(A) Acceso

Cuestión	Art(s).	Previsiones normativas
Medios para el cumplimiento	33 de la LFPDPPP y 102 del Reglamento	La obligación de acceso se dará por cumplida: • Cuando el responsable: o Ponga a disposición del titular los datos personales en sitio; o Respetando el periodo previsto al efecto (no podrá ser menor a quince días). • Mediante la expedición de copias simples, medios magnéticos, ópticos sonoros, visuales u holográficos • Utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular.
Otros medios de reproducción de la información		El responsable podrá acordar con el titular: • Medios de reproducción de la información distintos a los informados en el aviso de privacidad. • Cuando así lo considere conveniente.

[337] Véase la nota a pie de página anterior. Págs. 54 a 57.

Solicitud dirigida a quien no es el responsable	33 de la LFPDPPP	Se tendrá por cumplida la solicitud cuando: • El titular solicite el acceso a los datos una persona que presume es el responsable y ésta resulta no serlo o Bastará con que así le indique al titular por cualquiera de los medios previstos para el cumplimiento.
Acceso a los datos personales en sitio	99 del Reglamento	El responsable deberá: • Determinar el periodo durante el cual el titular puede presentarse a consultarlos o No será menor a quince días Transcurrido el plazo sin que el titular haya acudido a tener acceso a sus datos personales, será necesaria la presentación de una nueva solicitud.

(R) Rectificación

Cuestión	Art(s).	Previsiones normativas
Requisitos del derecho de rectificación	104 del Reglamento	La solicitud deberá: • Indicar: o A qué datos personales se refiere, y o La corrección que haya de realizarse • Ir acompañada de la documentación que ampare la procedencia de lo solicitado.
		El responsable podrá ofrecer

		mecanismos que faciliten el ejercicio del derecho de rectificación en beneficio del titular.
Transmisión de los datos con anterioridad a la rectificación	25 de la LFPDPPP	El responsable deberá hacer de conocimiento de los terceros a los que hubiera transmitido los datos personales cuando: • Hubiesen sido transmitidos con anterioridad a la fecha de rectificación, y • Sigan siendo tratados por terceros. Para que los terceros procedan también a efectuarla.

(C) Cancelación

Cuestión	Art(s).	Previsiones normativas
Supuestos en los que procede	106 del Reglamento	Cuando el titular considere que los datos personales no están siendo tratados conforme a los principios y deberes que establece la Ley y el Reglamento.
Alcance de la solicitud		Según lo haya solicitado, respecto de: • La totalidad de los datos personales contenidos en una base de datos, o • Sólo parte de ellos.
Bloqueo	107 del Reglamento	De resultar procedente la cancelación, el responsable deberá: I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual, y

		notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación; II. Atender las medidas de seguridad adecuadas para el bloqueo; III. Llevar a cabo el bloqueo en el plazo de quince días; IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad establecidas por el mismo.
Propósito del bloqueo	108 del Reglamento	El bloque tiene como propósito: • Impedir el tratamiento o A excepción del ▪ Almacenamiento o ▪ Posible acceso por personal alguna • Salvo que alguna disposición legal prevea lo contrario.
Aviso al titular	25 de la LFPDPPP	Una vez cancelado el dato se dará aviso al titular.
Transmisión de los datos con anterioridad a la cancelación		El responsable deberá hacer de conocimiento de los terceros a los que hubiera transmitido los datos personales cuando: • Hubiesen sido transmitidos con anterioridad a la fecha de cancelación, y • Sigan siendo tratados por terceros. Para que los terceros procedan también a efectuarla.
Inexistencia	26 de la	Además de los supuestos de denegación

de obligación de cancelar los datos personales	LFPDPPP	de los derechos ARCO, el responsable no está obligado a cancelar los datos personales cuando: I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento; II. Deban ser tratados por disposición legal; III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas; IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular; V. Sean necesarios para realizar una acción en función del interés público; VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

(O) Oposición

Cuestión	Art(s).	Previsiones normativas
Supuestos en los que procede	109 del Reglamento	El titular podrá, en todo momento, oponerse al tratamiento de sus datos personales cuando: I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.
Improcedencia del derecho de oposición		No procederá cuando: • El responsable puede negar el ejercicio de los derechos ARCO, el derecho de oposición, y • El tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.
Listados de exclusión	110 del Reglamento	Para el ejercicio del derecho de oposición, los responsable podrán gestionar listados de exclusión: • Propios o En los que incluyan los datos de las personas que han manifestado su negativa para que se trate sus datos personales o Ya sea para sus productos

		o de terceras personas. • Comunes o Por sectores o generales.
Inclusión del titular en los listados de exclusión		En ambos casos (listados de exclusión propios o comunes) la inclusión del titular deberá: • Ser gratuita; • Otorgar al titular una constancia de su inscripción al mismo, o A través de los mecanismos que el responsable determine.
Registro Público de Consumidores y Registro Público de Usuarios	111 del Reglamento	Los Registros Públicos de: • Consumidores: previsto en la Ley Federal de Protección al Consumidor • Usuarios: previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros • Continuarán vigentes y se regirán de conformidad con lo que establezca su normativa y demás disposiciones aplicables.

Es así que los derechos ARCO se ejercerán ante el responsable por el titular o su representante, legal o voluntario.

No obstante, es necesario tener en consideración que los derechos ARCO no son absolutos, sino que hay supuestos en los que no procederán, por ejemplo, por aplicación de una disposición legal, y otros en los que el responsable los podrá denegar por las causas que correspondan.

Tal y como indica el artículo 88 del Reglamento de la LFPDPPP: *"El ejercicio de los derechos ARCO podrá restringirse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud*

públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución e la autoridad competente debidamente fundada y motivada."

Es así que, dado que el responsable del tratamiento tiene que resguardarlos de manera que permitan el ejercicio sin dilación de estos derechos, esto supone que incluso en el caso de que sean tratados por un proveedor de servicios de cómputo en la nube, tendrá que asegurarse de que puede atender al ejercicio de los mismos en los términos previstos en la normatividad sobre protección de datos personales.

Es decir, el cliente, como responsable del tratamiento, tendrá que asegurarse de que el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, permite que se pueda atender al ejercicio de los derechos ARCO en tiempo y forma ya que de lo contrario el responsable del tratamiento podría estar incumpliendo con sus obligaciones, lo cual además podría llegar a ser sancionable. En este sentido, es necesario tomar en consideración que la fracción I, del artículo 63 de la LFPDPPP prevé como infracción *"No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley"*, siendo objeto de apercibimiento conforme a lo previsto en la fracción I, del artículo 64 de la LFPDPPP. Sin perjuicio de lo anterior, en caso de que conforme a la fracción II, del citado artículo 63, el responsable del tratamiento actúe *"con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales"*, entonces podría ser sancionado con multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, conforme a lo previsto en la fracción II, del artículo 64 de la LFPDPPP y en virtud del correspondiente procedimiento de verificación.

En conclusión, el responsable del tratamiento tendrá que asegurarse de que en caso de que haga uso de servicios de cómputo en la nube, puede atender el ejercicio de los derechos ARCO a pesar

de que los datos personales estén siendo tratados por el proveedor de servicios de cómputo en la nube como tratamiento.

6.8. Potestades de la autoridad garante y las autoridades

En protección de datos personales, la condición de autoridad garante la tiene el IFAI, siendo la Secretaría de Economía una de las autoridades reguladoras previstas en la LFPDPPP. Al respecto, son respectivamente los artículos 39, relativo al IFAI, y 43, relativo a la Secretaría de Economía, los que se refieren a las atribuciones o potestades que tienen cada una de dichas autoridades.

En el caso del IFAI, como autoridad garante, éste tiene atribuidas funciones informativas, normativas, de verificación, resolutorias y sancionadoras que pueden resumirse así[338]:

> *"**1. Atribuciones informativas***
> *El IFAI tiene la atribución de proporcionar apoyo técnico a los responsables que lo soliciten para el cumplimiento de las obligaciones establecidas en la ley; además de rendir al Congreso de la Unión un informe anual de sus actividades; desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares, así como brindar capacitación a los sujetos obligados.*
>
> ***2. Atribuciones normativas***
> *Aunado a lo anterior, el IFAI cuenta con atribuciones normativas relativas a interpretar en el ámbito administrativo la ley; emitir los criterios y recomendaciones para garantizar el pleno derecho a la protección de datos personales, y divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información.*

[338] Conforme a la explicación de dichas funciones dada por el IFAI y disponible en la dirección de Internet http://inicio.ifai.org.mx/_catalogs/masterpage/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m3

3. Atribuciones de verificación

Adicionalmente, el Congreso Federal confirió al IFAI atribuciones de supervisión enfocadas a vigilar y verificar el cumplimiento de las disposiciones contenidas en la ley y elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.

4. Atribuciones resolutorias

El IFAI cuenta con atribuciones resolutorias referentes a conocer y resolver los procedimientos de protección de derechos y de verificación e imponer las sanciones según corresponda, así como funciones en materia de cooperación como son acudir a foros internacionales y cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.

5 Atribuciones sancionadoras

El IFAI también está facultado para imponer sanciones pecuniarias. Al respecto, la ley prevé una serie de conductas consideradas como infracciones y sus sanciones correspondientes, que van desde el apercibimiento hasta la imposición de multas máximas, bajo un sistema de modulación de la penalidad, de acuerdo con la gravedad de las conductas."

Y en el caso del sector público, el IFAI tiene las siguientes funciones o atribuciones[339]:

"— Emisión de regulación secundaria: Lineamientos y recomendaciones.

— Verificaciones a sistemas de datos personales.

— Seguimiento al registro de sistemas de datos (3,034).

— Notificación de la Guía para la elaboración del documento de seguridad.

[339] Véase la explicación de funciones del IFAI en la dirección de Internet indicada en la nota a pie de página anterior.

- *Elaboración de Impacto a la Privacidad (PIA´s): NOM-024 Expediente clínico electrónico y Cédula de Identidad Ciudadana.*
- *Elaboración de las recomendaciones al proyecto de al proyecto de implementación del SNIP y eventual expedición de la Cédula de Identidad.*
- *Comentarios al Proyecto de reglamento de la Ley Federal de Telecomunicaciones en materia del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT).”*

Por lo que se refiere a las potestades o funciones de otras autoridades, en concreto por lo que se refiere a la Secretaría de Economía como autoridad reguladora, la LFPDPPP le atribuye en su artículo 43 las siguientes:

Función	Art. 43	Función
Difundir conocimiento sobre protección de datos personales	I	*“Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial.”*
Fomentar buenas prácticas	II	*“Fomentar las buenas prácticas comerciales en materia de protección de datos personales.”*
Emitir Lineamientos sobre el aviso de privacidad	III	*“Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley.”*
Expedir regulación secundaria	IV	*“Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto.”*
Fijar parámetros de autorregulación	V	*“Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se*

en protección de datos personales[340]		*refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto."*
Llevar registros de consumidores y verificar su cumplimiento	VI	*"Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento."*
Colaboración con cámaras de comercio y otras organizaciones	VII	*"Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales."*
Diseñar e implementar políticas públicas y realizar estudios	VIII	*"Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales."*
Acudir a foros nacionales e internacionales	IX	*"Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial."*
Apoyar la realización de estudios	X	*"Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales."*

[340] En relación con la autorregulación vinculante, véanse los Parámetros de Autorregulación en materia de Protección de Datos Personales. Dichos Parámetros fueron publicados en el Diario Oficial de la Federación el 29 de mayo de 2014 y en virtud de su artículo transitorio segundo abrogan los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que fueron publicados en el Diario Oficial de la Federación el 17 de enero de 2013.

6.9. Cooperación internacional

La cooperación internacional hace referencia al hecho de que la Secretaría de Economía, en su papel de autoridad reguladora, coopere con otras autoridades a nivel internacional.

En este sentido, hay que tomar en consideración que una de las funciones que la LFPDPPP atribuye a la Secretaría de Economía, conforme a la fracción IX, del artículo 43 es la de "*Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial."*

Unido a lo anterior, el cómputo en la nube es un *"fenómeno global y que implica una revolución tecnológica, cualquier solución a los retos que se plantean tiene que ser considerada en favor de la adopción de las nuevas tecnologías, con una regulación mínima razonable y adecuada a la vista de las buenas prácticas seguidas en derecho comparado y la autorregulación de la industria. Se trata así de no obstaculizar los beneficios que conlleva la innovación, a través de su adopción y uso intensivo."*[341]

Además, es necesario tomar en consideración que en su Resolución sobre el cómputo en la nube (en inglés, Resolution on Cloud Computing), adoptada por las autoridades de protección de datos y privacidad[342], éstas concluyeron que: *"Todas las partes – proveedores y clientes de CC así como reguladores – deberían cooperar para asegurar un alto nivel de privacidad y protección de datos así como seguridad tecnológica"*[343]*.*

---

[341] Véase, VV.AA., *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo.* Op. ya citada. Pág. 6.

[342] Adoptada en la 34ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, reunidas en Punta del Este (Uruguay), el 26 de Octubre de 2012 y disponible en la siguiente dirección de Internet http://privacyconference2012.org/wps/wcm/connect/92d083804d5dbb9ab90dfbfd6066fd91/Resolution_Cloud_Computing.pdf?MOD=AJPERES

[343][343] Traducción del original en inglés: *"All stakeholders – providers and customers of CC as well as regulators – should cooperate in order to ensure a high level of privacy and data protection and IT security."*

Por tanto, como autoridad reguladora, la Secretaría de Economía puede y debe desempeñar un papel fundamental tanto a nivel nacional como internacional en relación con el cómputo en la nube, como servicio tecnológico que implica o conlleva, en su caso, el tratamiento de datos personales y que, en definitiva, requiere promover buenas prácticas y un marco regulador adecuado para garantizar el derecho fundamental a la protección de datos personales. Se debe tratar así de fomentar el uso tecnológico, de manera que México pueda ser competitivo, al mismo tiempo que se vela porque tanto responsables como encargado del tratamiento adoptan medidas para garantizar el derecho fundamental a la protección de datos personales.

6.10. Acceso de autoridades gubernamentales y judiciales a los datos

Una cuestión que se plantea en relación con el cómputo en la nube y con otros servicios tecnológicos a nivel internacional es la relativa al acceso por autoridades gubernamentales y judiciales a datos personales.

A nivel nacional, hay que tomar en consideración que la LFPDPPP, en su artículo 10 indica, en su fracción VII, que no será necesario el consentimiento del titular de los datos personales cuando *“se dicte resolución de autoridad competente”*.

El citado artículo se limita a hacer referencia a una “autoridad competente”, de manera que ésta podría ser tanto administrativa o gubernamental como judicial. El Reglamento de la LFPDPPP no se refiere a esta cuestión. En cualquier caso, se entiende que la previsión de la LFPDPPP se refiere a las autoridades nacionales, de manera que no se trataría de una previsión relativa a autoridades de otros países.

En el caso de transferencias internacionales, lo que se produciría en el caso de solicitudes hechas por autoridades de otros países, el artículo 37, en su fracción I, indica que no será necesario el consentimiento del titular de los datos *“[c]uando la transferencia esté*

prevista en una Ley o Tratado en los que México sea parte". No obstante, es necesario tomar en consideración que el acceso a los datos personales debe producirse con todas las garantías jurídicas, legales y procesales, aplicables al caso y que pueden tener implicaciones tanto para el clientes de servicios de cómputo en la nube como para el prestador de dichos servicios.

Sin perjuicio de lo anterior, hay que tener en cuenta la regulación de la retención o conservación de datos en la nueva Ley Federal de Telecomunicaciones y Radiodifusión[344] (en adelante, LFTR), que dedica su Título Octavo, artículos 189 y 190, a la colaboración de los concesionarios de telecomunicaciones y, en su caso, los autorizados y los proveedores de servicios de aplicaciones y contenidos, con la Justicia.

En concreto, el artículo 189 de la nueva LFTR indica, en su primer párrafo, que dichos sujetos están obligados a *"atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes".*

Y también, en su segundo párrafo, que *"Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación."*

Por último, habría que tomar también en consideración los artículos relativos a la comunicación entre autoridades, tanto por lo que se refiere a requerimientos entre autoridades nacionales como a los exhortos de tribunales extranjeros, del nuevo Código Nacional de Procedimientos Penales[345].

---

[344] Publicada en el Diario Oficial de la Federación el 14 de julio de 2014 y disponible en la dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_140714.pdf Esta Ley abroga, entre otras, a la hasta ahora vigente Ley Federal de Telecomunicaciones, publicada en el Diario Oficial de la Federación el 7 de junio de 1995.

[345] Publicado en el Diario Oficial de la Federación el 5 de marzo de 2014 y disponible en la dirección de Internet http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

En cualquier caso, resulta claro que en relación con los servicios de cómputo en la nube pueden presentarse casos en los que las autoridades competentes, ya sean nacionales e internacionales, requiere, por una parte, que los proveedores de servicios de computación en la nube sean transparentes de manera que los clientes sepan, salvo que exista una obligación de mantener en secreto dicha solicitud, cuando se produce el acceso a los datos personales que se tratan en la nube. Y, por otra parte, requiere que las autoridades competentes adopten medidas de manera que los proveedores de servicios de cómputo en la nube no se vean sujetos a situaciones en las que tengan que permitir el acceso a autoridades de otros países sin poder contar con un procedimiento administrativo o, en su caso, procesal que se lleve a cabo a través de las autoridades implicadas. Es decir, dichas solicitudes de acceso tendrían que hacerse a través de las autoridades competentes, de manera que el proveedor de servicios de cómputo en la nube quede también protegido, especialmente en el caso de solicitudes de acceso emitidas por otros países[346]. Se trata de los artículos 73 a 81del citado Código Nacional de Procedimientos Penales.

Sobre esta cuestión, es recomendable adoptar las garantías jurídicas y procesales adecuadas que, por una parte, permitan a los proveedores de servicios de computación en la nube poder responder y, en su caso, atender con las garantías necesarias las solicitudes de acceso a datos personales o contenidos por parte de autoridades nacionales o de otros países y, por otra parte, garantizar a los clientes de estos servicios que el acceso cumple con dichas garantías. Al respecto, es importante tomar en consideración que los proveedores de servicios de cómputo en la nube enfrentan costos en virtud de dichas solicitudes de acceso que es necesario tomar en consideración y que,

[346] Al respecto, a nivel internacional, puede verse por ejemplo el Dictamen 5/2012 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, ya citado. En dicho Dictamen, las autoridades europeas de protección de datos personales han indicado, como conclusión y recomendación relativa a las garantías contractuales, que *"El contrato también deberá exigir al proveedor que notifique toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que dicha divulgación esté prohibida por otras razones. El cliente deberá garantizar que el proveedor rechazará cualquier solicitud de divulgación jurídicamente no vinculante."* Pág. 24.

cuando las mismas son de otros países, es necesaria la cooperación internacional para evitar situaciones de desprotección de los mismos y de sus clientes[347].

En definitiva, se trata de una cuestión en la que se plantean cuestiones comerciales y de seguridad nacional que pueden entrar en conflicto, de manera que la Secretaría de Economía, como autoridad reguladora y en el ámbito de sus competencias, podría aportar recomendaciones o argumentos que permitan que tanto los usuarios de servicios de cómputo en la nube como los proveedores de dichos servicios queden protegidos y, al mismo tiempo, se pueda atender las solicitudes que cumplan con las garantías procesales o procedimentales oportunas y, al mismo tiempo, se garantice el derecho fundamental a la protección de datos.

Con respecto al supuesto concreto en el que los datos personales estuvieran almacenados fuera de México, se trata de una cuestión sobre la que en su momento se pronunció la Comisión Permanente del Congreso de la Unión, que *"rechazó categóricamente toda acción que vulnere la intimidad, la protección de los datos personales o la seguridad de la población mexicana y atente contra la soberanía que protege a las representaciones diplomáticas"*[348].

También, la Comisión Permanente requirió *"Ejecutivo Federal para que, por conducto de la Secretaría de Relaciones Exteriores, solicite al gobierno norteamericano una explicación precisa y urgente respecto al espionaje sobre funcionarios y representaciones diplomáticas mexicanas y pida el cese de esas actividades de forma permanente e inmediata."*

---

[347] Además de lo ya indicado en la nota a pie de página anterior, sobre la cuestión relativa al acceso a los datos personales con fines de seguridad nacional y de aplicación de la ley, el Dictamen 5/2012 ya citado, indica que: *"es primordial que el futuro Reglamento prevea la prohibición, para los responsables del tratamiento que operan en la UE, de revelar datos personales a un país tercero si así lo solicita una autoridad judicial o administrativa de dicho país tercero, salvo autorización expresa derivada de un acuerdo internacional o de tratados de asistencia jurídica mutua, o salvo autorización de la autoridad de supervisión."* Pág. 26.

[348] Véase el Boletín-2004 del Senado, de 31 de julio de 2013, disponible en http://comunicacion.senado.gob.mx/index.php/informacion/boletines/7931-boletin-2004-rechaza-comision-permanente-espionaje-de-eu-.html

Y sobre el caso Snowden, se puso de manifiesto que *"el programa revelado por el ex contratista de la ASN, Edward Snowden, representa "una intromisión injustificada de los servicios de inteligencia norteamericanos en la vida civil", así como una falta a las normas de la diplomacia internacional."*

En el marco de la Comisión Permanente, también hubo una diputada que "consideró que el espionaje estadounidense demuestra *"el grado de intromisión y de amenaza a la seguridad nacional" de México."Las dudas que rodean al programa de espionaje masivo siguen sin esclarecerse, pese a que Barack Obama ha insistido en que ese programa garantiza libertades", apuntó."*

Se trata, por tanto, de una cuestión que requiere de acciones por parte de las autoridades competentes para proteger tanto a los ciudadanos mexicanos, entre quienes deben entenderse incluidas las empresas que hacen uso a diario de servicios electrónicos, como por ejemplo, Internet, el correo electrónico, el cómputo en la nube, etc., así como a quienes proporcionan dichos servicios. En concreto, según se indica en la nota ya citada, *"los legisladores consideraron que el programa representa "una intrusión injustificada de los servicios de inteligencia norteamericanos en la vida civil, así como una falta a las normas escritas y consuetudinarias de la diplomacia internacional"."*

Son, precisamente, los legisladores, quienes deben adoptar medidas, ya que como finaliza la nota del Congreso, esta acción de espionaje *"lesiona los derechos humanos a la intimidad y a la secrecía de los datos personales violentando numerosos instrumentos internacionales, como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos."*

Al respecto y a nivel internacional, la Unión Europea también ha dedicado sus esfuerzos a exigir explicaciones sobre el caso Snowden y ha emitido una Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos

Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior[349], que finaliza con la presentación de *"un «Habeas corpus digital europeo – proteger los derechos fundamentales en una era digital» con las ocho acciones siguientes, cuya aplicación supervisará:*

- *Acción 1: Adopción del paquete de protección de datos en 2014;*
- *Acción 2: Conclusión del acuerdo marco entre la UE y los Estados Unidos que garantice el derecho fundamental de los ciudadanos a la intimidad y a la protección de datos y los mecanismos de recurso adecuados para los ciudadanos de la UE, incluso en caso de que se produzcan envíos de datos de la UE a los Estados Unidos con fines coercitivos;*
- *Acción 3: Suspensión del puerto seguro hasta que se haya efectuado un análisis completo y se hayan enmendado las lagunas actuales para garantizar que el envío de datos personales con fines comerciales desde la Unión a los Estados Unidos solo pueda llevarse a cabo de conformidad con los máximos estándares de la UE;*
- *Acción 4: Suspensión del acuerdo TFTP hasta que i) se hayan cerrado las negociaciones del acuerdo marco; ii) se haya efectuado una investigación exhaustiva sobre la base de un análisis de la UE y se hayan abordado debidamente todos los problemas planteados por el Parlamento en su Resolución de 23 de octubre de 2013;*
- *Acción 5: Evaluación de todo acuerdo, mecanismo o intercambio con terceros países que implique datos personales a fin de garantizar que no se infringe el derecho a la intimidad y a la protección de los datos personales debido a las actividades de vigilancia, y adopción de las medidas de seguimiento necesarias;*
- *Acción 6: Protección del Estado de Derecho y los derechos fundamentales de los ciudadanos de la UE (también de las*

[349] Publicada en la dirección de Internet http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES

amenazas a la libertad de prensa), el derecho del público a recibir información objetiva y acogerse al secreto profesional (incluidas las relaciones entre abogados y clientes), así como la garantía de una mejor protección de los denunciantes de irregularidades;

- *Acción 7: Desarrollo de una estrategia europea para una mayor independencia informática (un «nuevo acuerdo digital» que incluya la asignación de recursos adecuados a nivel nacional y de la UE), a fin de potenciar la industria informática y permitir que las empresas europeas exploten la ventaja competitiva de la UE en términos de intimidad;*
- *Acción 8: Desarrollo de la UE como actor de referencia para una gobernanza democrática y neutral de internet".*

Desde un punto de vista tecnológico y comercial, las revelaciones del espionaje han tenido también importantes consecuencias, en particular en el caso del cómputo en la nube y también en otros ámbitos, indicando que las *"empresas que presten nuevos servicios utilizando datos masivos y nuevas aplicaciones, como el «Internet de las Cosas», que elaboren medidas de protección de datos desde la fase de desarrollo a fin de mantener un nivel de confianza elevado entre los ciudadanos."*

Lo anterior supone que las cuestiones de seguridad nacional y espionaje deban tratarse entre los países implicados a través de Tratados o Convenios, ya sean bilaterales o multilaterales, sin que perjudiquen el desarrollo de tecnológico y la prestación de servicios tecnológicos por proveedores que podrían sufrir las consecuencias de las acciones del gobierno y, específicamente, de los correspondientes servicios de inteligencia.

6.11. Principios mínimos con los que debe cumplir el proveedor de servicios en la nube

6.11.1. Sector privado

El artículo 52 del reglamento para Ley de Protección de Datos Personales en Posesión de los Particulares, sobre el que ya hemos hecho anteriormente un completo análisis, señala:

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

***I.** Cumpla, al menos, con lo siguiente:*

***a)** Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;*

***b)** Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;*

***c)** Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y*

***d)** Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y*

***II.** Cuente con mecanismos, al menos, para:*

***a)** Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;*

***b)** Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;*

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

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

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

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

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

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

6.11.2. Sector Público

Como ya sabemos, el cómputo en la nube, se define como el modelo de prestación de servicios digitales que permite a las Instituciones acceder a un catálogo de servicios digitales estandarizados, los cuales pueden ser: de infraestructura como servicios, de plataforma como servicios y de software como servicios[350].

[350] Artículo 2 del Acuerdo que tiene por objeto emitir 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 establecer el manual administrativo de aplicación general en dichas materias. Publicado en: http://dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

Dado que el acuerdo refiere las políticas y disposiciones de la Estrategia Digital Nacional en materia de tecnologías de la información, los responsables de aplicar dichas políticas son los titulares de las unidades administrativas o áreas responsables de las tecnologías de información y comunicaciones (TIC) en las instituciones, así como los servidores públicos cuyas atribuciones o funciones estén relacionadas con la planeación, contratación y administración de bienes y servicios de TIC y con la seguridad de la información (artículo 3 del Acuerdo).

En el artículo 5 fracción I, se establece que las políticas para la Estrategia Digital Nacional (PETIC) deberán favorecer el uso del cómputo en la nube para el aprovechamiento de la economía de escala, eficiencia en la gestión gubernamental y estandarización de las TIC, siempre que se tenga en consideración la seguridad de la información.

Siguiendo con las políticas para la Estrategia Digital Nacional, el artículo 13 habla de que en el caso de servicios de Centros de Datos, las Instituciones deberán:

a) Primero, identificar la infraestructura del centro de datos con el que cuentan, la capacidad de procesamiento y almacenamiento.
b) Evaluar la conveniencia de contratar servicios de centro de datos, tomando en cuenta el beneficio económico, eficiencia, privacidad, seguridad de los datos y la información en comparación con utilizar un centro de datos propio o compartido con otra institución.
c) Establecer en las convocatorias a la licitación pública, la invitación a cuando menos tres personas.
d) Analizar el alojamiento de la infraestructura de operación 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.
e) Almacenar y administrar en los Centros de Datos que se encuentren en las instalaciones de las Instituciones, los datos considerados de seguridad nacional, seguridad pública e

información reservada y confidencial, conforme a la normatividad aplicable;

f) Mantener en la infraestructura de los Centros de Datos una arquitectura que permita la portabilidad, de forma tal que las aplicaciones de cómputo puedan migrar entre distintos centros de datos y sean interoperables.
g) Establecer la infraestructura y administración de la seguridad de la información en zonas de seguridad física y lógica, considerando identidad, perfiles y privilegios, incluyendo en éstas las necesarias para el personal involucrado.

En el capítulo IV del Acuerdo, se establecen las disposiciones generales que las Instituciones de gobierno deberán seguir.

En lo relativo a las cuestiones contractuales con prestadores del servicio de la nube en el sector público, ver la sección correspondiente en el apartado correspondiente a las cuestiones específicas de la contratación de cómputo en la nube en el sector público.

7. Propiedad intelectual

7.1. Cuestiones relativas a la protección de la propiedad intelectual

El cómputo en la nube, para un adecuado desarrollo, requiere que el país cuente con normas claras y eficientes en materia de derechos de autor así como propiedad industrial. De lo contrario, se desincentivarían las inversiones por parte de los desarrolladores tanto de *software* necesario para el cómputo en la nube, como de aplicaciones *(“apps”)* u otras creaciones.

En el seno de una economía digital o electrónica, donde el *software* se convierte en un instrumento fundamental, es necesario contar con un sólido marco regulador que proteja al titular del mismo.

Al respecto, cabe señalar que México ha venido progresando durante los últimos años por lo que se refiere a combatir la piratería del software, a pesar de que todavía queda bastante por hacer. En este sentido, si se toma en consideración el ranking elaborado por *BSA | The Software Alliance* y publicado en junio de 2014, bajo el título *Encuesta Global sobre Software*[351], es posible ver que México sigue estando entre las 20 economías principales con software sin licencia que alcanza un valor comercial, en 2013, de USD 1,211 millones.

Si bien en 2013 México ha bajado su índice de piratería del software un 3%, pasando del 57% de 2011 al 54% en 2013, todavía se encuentra lejos de otros países alrededor del mundo que tienen un índice mucho más bajo, tales como Alemania (24%), Australia (21%) o Japón (19%). No obstante, es necesario tomar en consideración que se va alejando también de la media en Latinoamérica que en 2013 fue del 59%, si bien sigue por encima de la media mundial, que fue del 43%.

Además, México también sigue en la lista de países bajo "vigilancia" (en inglés, *Watch List*) que anualmente elabora la Oficina del Representante Comercial de los Estados Unidos (*United States Trade Representative*, USTR) en materia de derechos de propiedad intelectual, bajo el nombre *Special 301 Report*[352].

En definitiva, además de políticas públicas dirigidas a atraer inversión de desarrolladores de software y aplicaciones, es necesario que México siga reforzando su marco de protección de la propiedad intelectual e industrial, de manera que ello permita, por una parte, que los jóvenes y emprendedores estén protegidos y, por otra parte, que la inversión de otros países y de la industria sea posible, ya que así será posible consolidar día a día una industria que permita a México ser un país competitivo y, en su caso, líder con respecto a otros países o

---

[351] Disponible en la dirección de Internet http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_es.pdf

[352] El informe relativo a 2013 y publicado el 30 de abril de 2014 está disponible en la dirección de Internet http://www.ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf

potencias económicas[353] en cuanto a la economía digital, basada en servicios electrónicos, las aplicaciones y otras creaciones que requieren de una protección efectiva.

Por su relevancia, en los siguientes apartados se analiza, de manera específica, la normatividad aplicable a las licencias de software, así como las instituciones de gobierno que tienen alguna función en relación con la protección de la propiedad intelectual. En particular se trata de INDAUTOR y el IMPI. Finamente se hace referencia a alguna jurisprudencia relevante en la materia.

7.2. Licencias de *software*

7.2.1. Leyes que rigen las licencias de *software*

Los contratos de licencia de *software*, se encuentran regulados principalmente en los siguientes ordenamientos:

[353] Como ejemplo, en el caso de la Unión Europea, al analizar el concepto de cómputo en la nube, según un estudio llevado a cabo por el Parlamento Europeo, hay que tomar en consideración que *"el tema es complejo y amplio, y tiene sinergias con muchas esferas del mercado único digital de la UE, desde las cuestiones de propiedad intelectual hasta la penetración de la banda ancha y la denominada Internet de los objetos".* Véase, Parlamento Europeo, *Computación en Nube*, Dirección General de Políticas Interiores, Mercado Interior y Protección del Consumidor, 2012. Pág. 13 Y también que *"en el ámbito de los contenidos digitales, solo se ha logrado un nivel limitado de armonización a raíz de la Directiva sobre los derechos de autor y, por tanto, preocupan especialmente los servicios en nube que dependen de un régimen de derechos de propiedad intelectual (DPI) uniforme a la hora de cruzar fronteras. Asimismo, los Estados miembros carecen de un método armonizado de gestión de los derechos de autor. Pero, como indicaron muchos de nuestros entrevistados, este no es un problema específico de los servicios en nube, ya que todos los servicios en línea que permiten, por ejemplo, la transmisión de contenidos de música y vídeo — como YouTube o el servicio en nube de Spotify— se ven afectados por esta fragmentación: debido a los diferentes regímenes de DPI, a menudo es posible bloquear los contenidos en distintos Estados miembros."* Pág. 76. Disponible en la siguiente dirección de Internet http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_ES.pdf

7.2.1.1. Ley Federal de Derechos de Autor[354] y su reglamento[355].

En el capítulo IV de la Ley Federal de Derechos de Autor (LFDA) se definen las cuestiones relativas a la protección de los programas de computación y las bases de datos. Se entiende por programa de computación: *"la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica"* (artículo 101 de la LFDA).

Protección de los programas de cómputo

Conforme al artículo 102 de la LFDA, los programas de computación se protegen en los mismos términos que las obras literarias, y dicha protección se extiende tanto a los programas operativos como a los programas aplicativos (en forma de código fuente o de código objeto). Se exceptúan de ésta protección, aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

Además, los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por la LFDA en los elementos primigenios que contengan (artículo 111 de la LFDA).

Está prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo 111 (artículo 112 de la LFDA).

---

[354] La Ley Federal de Derecho de autor conforme a la última reforma del 10.06.2013 se encuentra publicada en la página de la Cámara de Diputados: http://www.diputados.gob.mx/LeyesBiblio/pdf/122.pdf

[355] El reglamento de la ley federal del derecho de autor, se encuentra publicado en la página de la Cámara de diputados: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFDA.pdf

Así mismo, las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley (artículo 113 de la LFDA).

La transmisión de obras protegidas por la LFDA mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia (artículo 114 de la LFDA).

Se considera una **infracción en materia de comercio** el usar, reproducir o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular (artículo 231, fracción VII de la LFDA). Dicha infracción es sancionada por el Instituto Mexicano de la propiedad Industrial con multa de cinco mil hasta cuarenta mil días de salario mínimo (artículo 232, fracción I de la LFDA).

Facultades patrimoniales del dueño del programa computacional

Conforme al artículo 106 de la LFDA, el derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

a) La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma
b) La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante,
c) Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler, y
d) La descompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje.

Protección sobre las bases de datos

a) Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones (art 107 de la LFDA).
b) La protección a las bases de datos u otros materiales no se extiende a los datos y materiales en sí mismos (artículo 107 de la LFDA)
c) Las bases de datos que **no** sean originales quedan protegidas para su uso exclusivo por quien las haya elaborado, durante un lapso de cinco (5) años (artículo 108 de la LFDA)[356]
d) El acceso a información de carácter privado contenida en las bases de datos no originales, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requiere la autorización previa de las personas de cuya información se trate (artículo 109 de la LFDA)
e) Queda exceptuado de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos (artículo 109 de la LFDA).
f) El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir: la reproducción permanente o temporal, total, parcial por cualquier medio y de cualquier forma; su traducción, adaptación, reordenación y cualquier otra modificación; la distribución del original o copias de la base datos; la comunicación al público y la reproducción, distribución o comunicación pública de los resultados de las operaciones de traducción, adaptación, reordenación u otra modificación

[356] Esto conforme a las recomendaciones de la OMPI, para mayor referencia ver “Protección de bases de datos no originales” en la página de la OMPIÑ http://www.wipo.int/copyright/es/activities/databases.html

Regulación de Licencias de Software

En cuanto a las licencias de *software*, la ley estipula lo siguiente:

a) El titular de los derechos es quien puede libremente otorgar licencias de uso exclusivas o no exclusivas (artículo 30 de la LFDA).
b) Además, las licencias deben de celebrarse por escrito, o de lo contrario serán nulas de pleno derecho (artículo 30 de la LFDA).
c) De darse una licencia exclusiva deberá otorgarse expresamente con tal carácter y atribuirá al licenciatario, salvo pacto en contrario, la facultad de explotar la obra con exclusión de cualquier otra persona y la de otorgar autorizaciones no exclusivas a terceros (artículo 3 de la 5 LFDA). La licencia exclusiva obliga al licenciatario a poner todos los medios necesarios para la efectividad de la explotación concedida, según la naturaleza de la obra y los usos y costumbres en la actividad profesional, industrial o comercial de que se trate (artículo 36 de la LFDA).
d) El titular de los derechos de autor sobre un programa de computación o sobre una base de datos, conservará aún después de la venta de ejemplares de los mismos, el derecho de autorizar o prohibir el arrendamiento de tales ejemplares. Sin embargo, esto no se aplicará cuando el ejemplar del programa de cómputo no constituya en sí mismo un objeto esencial de la licencia de uso (artículo 104 LFDA).
e) El usuario legítimo de un programa de computación puede realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, siempre y cuando sea indispensable para la utilización del programa o sea para resguardo y sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación (artículo 105 de la LFDA).

De la transmisión de derechos patrimoniales

Las disposiciones relativas a la transmisión de derechos patrimoniales, están en el título III de la Ley Federal de derechos de autor:

a) El titular del derecho es quien puede transferir sus derechos patrimoniales (artículo 30 de la LFDA).

b) La transmisión de derechos patrimoniales debe ser onerosa y temporal. En ausencia de acuerdo sobre el monto de la remuneración o del procedimiento para fijarla, así como sobre los términos para su pago, la determinarán los tribunales competentes (artículo 30 de la LFDA). Así pues, en la transmisión de derechos patrimoniales deberá preverse una participación proporcional en los ingresos de la explotación de que se trate, o bien una remuneración fija y determinada. Éste derecho es irrenunciable (artículo de la LFDA 31).

De existir una copia o reproducción de la obra hecha sin autorización del autor y sin estar amparada por alguna de las limitaciones expresas en la ley[357], el titular del derecho podrá exigir una remuneración compensatoria (artículo 40 de la LFDA). Entre las limitaciones al derecho de software se encuentra el que no va a constituir violación siempre y cuando se realice sin fines de lucro y con el objeto exclusivo de hacerla accesible a invidentes o sordomudos, y dado que no se cause perjuicio a los titulares de los derechos (artículos 44 y 45 del Reglamento de la LFDA).

c) Los contratos de transmisión de derechos patrimoniales, deben hacerse por escrito, de lo contrario se consideran nulos de todo derecho (artículo 30 de la LFDA). Tales contratos deberán de inscribirse en el Registro Público del derecho de Autor para que pueda surtir efectos contra terceros (artículo 32 de la LFDA). Por último, como indica la LFDA *“Los actos, convenios y contratos sobre derechos patrimoniales que se formalicen ante notario, corredor público o*

[357] Las limitaciones se encuentran determinadas en los artículos 148 y 151 de la misma ley y se refieren a las obras literarias y artísticas.

cualquier fedatario público y que se encuentren inscritos en el Registro Público del Derecho de Autor, traerán aparejada ejecución" (artículo 37 de la LFDA).

d) En cuanto a la duración de la transmisión de derechos, de no haber estipulación expresa, se considera por el término de cinco (5) años. Por otro lado, solo se podrá pactar de manera excepcional por más de 15 años cuando la naturaleza de la obra o la magnitud de la inversión requerida así lo justifique[358] (artículo 33 de la LFDA).

e) Por lo que se refiere a la producción de obra futura, como indica la LFDA ésta *"sólo puede ser objeto de contrato cuando se trate de obra determinada cuyas características deben quedar establecidas en él. Son nulas la transmisión global de obra futura, así como las estipulaciones por las que el autor se comprometa a no crear obra alguna*" (artículo 34 de la LFDA).

f) Tal y como indica la LFDA en cuanto a la propiedad del objeto material en el que la obra esté incorporada, *"El derecho de autor no está ligado a la propiedad del objeto material en el que la obra esté incorporada. Salvo pacto en contrario, la venta del soporte material, no transfiere ninguno de los derechos patrimoniales del titular sobre la obra"* (artículo 38 de la LFDA). En el mismo contexto, la autorización para difundir una obra protegida, no comprende el derecho a explotarla o a re-difundirla (artículo 39 de la LFDA)

h) Por lo que se refiere a la posibilidad de embargar derechos de autor, la LFDDA indica que *"Los derechos patrimoniales no son embargables ni ignorables aunque pueden ser objeto de embargo o prenda los frutos y productos que se deriven de su ejercicio"* (artículo 41 de la LFDA).

[358] El artículo 17 del reglamento de la ley federal del derecho de autor, señala que las razones del convenio mayor a 15 años debe expresar la causa específica que lo justifique, e inscribirse en el Registro. En la fracción V se señala que se puede pactar un término mayor a 15 años cuando se trata de obras que por su naturaleza o magnitud de la inversión , no se permita recuperar la inversión en ese plazo.

i) El Reglamento de la LFDA refiere a la Ley Federal de Telecomunicaciones[359] para definir "espectro electromagnético" (artículo 36 del Reglamento). Además define medios electrónicos como *"aquellos que hagan posible el acceso remoto al público de obras literarias y artísticas por medio del espectro radioeléctrico o las redes de telecomunicación"* (artículo 37 del Reglamento).

Por último, en materia de licencias de *software*, tanto en el caso de empresas como de entidades y dependencias de las Administraciones Públicas, una buena práctica es la gestión de dichas licencias, pudiendo tomar como guía o referente sobre esta cuestión la norma internacional ISO/IEC 19770 sobre gestión de activos de software (en inglés, *Software Asset Management*, SAM). Se trata de una norma internacional cuya finalidad es ayudar a las organizaciones, tanto del sector privado como del público, a establecer procesos y procedimientos para un control efectivo de activos de software, lo que permite también minimizar los riesgos derivados del uso de software sin licencia o, incluso, el sobre-licenciamiento que tiene un impacto económico para las organizaciones como consecuencia de haber adquirido más licencias de las necesarias.

Además, es posible que las empresas y las entidades y dependencias de la Administración Pública puedan estar interesadas en obtener la certificación correspondiente en materia de SAM, lo que puede ayudarles a reducir riesgos.

7.2.1.2 Ley de Propiedad Industrial[360] y su reglamento[361].

En general en éstas leyes no se protege el contrato de *software* en sí, pero sí se protegen elementos que acompañan a los programas de cómputo, tales como: marcas, dibujos e íconos distintivos. Cabe la

[359] No obstante, es necesario tomar en consideración que esta referencia tendrá que ser actualizada como consecuencia de la entrada en vigor de la nueva Ley Federal de Telecomunicaciones y Radiodifusión.

[360] Ley de la propiedad industrial, con la última reforma del 09/04/2012 publicada en la página de la Cámara de diputados en: http://www.diputados.gob.mx/LeyesBiblio/pdf/50.pdf

[361] Reglamento de la propiedad industrial, con la última reforma del 10/06/2011 publicada en la página de la Cámara de diputados: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LPI.pdf

aclaración de que en México los programas de computación no se consideran invenciones, y por tanto no son patentables[362].

7.2.1.3. Código Penal Federal[363] y Código Federal de Procedimientos Penales[364].

Sancionan la producción masiva de copias no autorizadas de programas de cómputo o su venta. Cabe hacer la anotación de que los siguientes delitos se persiguen de oficio:

a) A quien en forma dolosa, con fin de lucro y sin la autorización correspondiente use obras protegidas por la Ley Federal del Derecho de Autor, se le impondrá prisión de 6 meses a 6 años y de 300 a 3,000 días de multa (artículo 424 código penal).

b) A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación, se le impondrá prisión de 3 a 10 años y de dos mil a veinte mil días de multa (artículo 424 bis código penal). Es importante destacar que éste delito es considerado como “delito grave” al afectar de manera importante valores fundamentales de la sociedad[365].

Las sanciones pecuniarias descritas, se impondrán sin perjuicio de la reparación del daño, cuyo monto no será menor al 40% del precio de venta al público de cada producto tutelado por la ley Federal de derecho de autor (artículo 428 del código penal federal).

Más adelante nos referimos con más detalle al marco regulatorio de los delitos informáticos.[366]

---

[362] Artículo 19, fracción V de la Ley de Propiedad Industrial.

[363] El Código penal federal con reformas del 03 de junio del 2014 publicado en la página de la cámara de diputados: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_030614.pdf

[364] Código Federal de Procedimientos Penales, con reformas publicadas el 13 de junio del 2014: http://www.diputados.gob.mx/LeyesBiblio/pdf/7_130614.pdf

[365] Artículo 194 fracción I, inciso 33

[366] Epígrafe 9 de este Estudio.

7.3. Una referencia específica al SaaS

Aunque en los apartados anteriores nos hemos referido al *software* y a su protección jurídica en la normatividad mexicana aplicable, hay que tomar en consideración que el cómputo en la nube implica un cambio conceptual, ya que ahora el *software* es considerado como un servicio (en inglés, Software as a Service, SaaS) por lo que además de la licencia hay que tomar en consideración que el modelo se basa, fundamentalmente, en la prestación de un servicio.

Esto implica que sea necesario tomar en consideración la necesidad de protección del SaaS y otros bienes objeto de propiedad intelectual ya que del mismo pueden depender muchas personas que encuentren en el software y en las aplicaciones *("apps")* una oportunidad profesional y de negocio.

Al respecto, como ya hemos señalado más atrás, en 2013 *BSA | The Software Alliance*, publicó una clasificación global sobre cómputo en la nube, bajo el título *2013 BSA Global Cloud Computing Scorecard*[367] en la que México aparecía en la posición 15ª de un total de 24 países, por detrás de países como Japón (1º), Alemania (4º), España (11º) o Rusia (14º). En la elaboración de dicho estudio, BSA tuvo en consideración aspectos como la protección de datos personales, la ciberseguridad y la propiedad intelectual, siendo el peso total de esta última cuestión un 20%, en comparación con el 10% dado, respectivamente, a la protección de datos o a la ciberseguridad.

Por tanto, es necesario que México siga trabajando para mejorar su posición en los *rankings* internacionales, además de que la adopción de medidas para proteger a los titulares de derechos de propiedad intelectual implica que los jóvenes y los emprendedores puedan tener más oportunidades y ello favorezca una industria nacional de *software*, aplicaciones y otras creaciones que puedan ser exportadas a otros países, además de ser la base de una creciente economía digital.

---

[367] Disponible en la dirección de Internet http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf

Lo anterior supone también que pueda tener un efecto llamada sobre la industria del software, en el sentido de que los prestadores de servicios de cómputo en la nube podrán ver al país como seguro a la hora de hacer inversiones.

7.4. Instituciones de gobierno

7.4.1. Instituto Nacional del Derecho de Autor (INDAUTOR)

Opera el Registro Público del derecho de autor, se registran programas, documentación y bases de datos, orienta a autores, procura resolver controversias según la LFDA y su reglamento. Es un organismo desconcentrado de la Secretaría de Educación Pública.

El INDAUTOR es la autoridad administrativa en materia de derechos de autor y derechos conexos, brinda servicios a la comunidad autora y artística nacional y extranjera, realiza trámites entre los que destacan[368]:

- El registro de obras y contratos de cesión y licencias de uso
- Autorizaciones a las sociedades de gestión colectiva
- Reservas de derechos al uso exclusivo de: títulos de revistas o publicaciones periódicas, difusiones periódicas, nombres de personas o grupos dedicados a actividades artísticas, personajes humanos de caracterización ficticios o simbólicos.
- Obtención del número internacional normalizado del libro (ISBN) y el número internacional normalizado para publicaciones periódicas (ISSN).
- Celebración de juntas de avenencia
- Consultas y asesorías legales
- Resolución de infracciones en materia de derechos de autor
- Procedimientos de arbitraje
- Impartición de cursos de capacitación y orientación para sensibilizar a la sociedad de la importancia del respeto a los derechos de autos para crear una cultura de la legalidad en la era del conocimiento y la tecnología de la información.

[368] Ficha descriptiva del INDAUTOR, en la página: http://www.indautor.gob.mx/ficha.html

Medios alternativos de resolución de conflictos administrados por el INDAUTOR

El INDAUTOR prevé un procedimiento de avenencia y un procedimiento de arbitraje. En cuanto al procedimiento de avenencia, la regulación estipula lo siguiente:

a) El procedimiento de avenencia se lleva a cabo ante el Instituto, a petición de alguna de las partes para dirimir de manera amigable un conflicto surgido con motivo de la interpretación o aplicación de la LFDA (artículo 217).
b) El procedimiento de avenencia se inicia a petición de parte, se notificará la parte contra de la que se interpone para que conteste la queja. Se cita a ambos a una junta de avenencia (dentro de los 20 días siguientes a la presentación de la queja), en la cual el Instituto tratará de avenir a las partes para que lleguen a un arreglo. El Instituto en sí, no hace determinación sobre el fondo pero sí participa activamente en la conciliación (fracción V del artículo 218 de la LFDA).
c) Las actuaciones dentro del procedimiento son de carácter confidencial y por tanto las constancias sólo podrán ser consultadas por las partes del conflicto, o cuando las autoridades competentes las soliciten[369] (artículo 218 de la LFDA).
d) Si del procedimiento de avenencia se firmarse un acuerdo entre las partes, éste tendrá carácter de cosa juzgada y título ejecutivo (fracción IV del artículo 218 de la LFDA).
e) En caso de que la avenencia no se logre, el instituto instará a las partes a que acojan el procedimiento de arbitraje administrado por el instituto (fracción VI del artículo 218 de la LFDA).

El procedimiento de arbitraje está regulado de los artículos 219 al 228 de la LFDA. Para poder entrar en el procedimiento de arbitraje, se requiere que las partes cuenten con una cláusula compromisoria o que firme un compromiso arbitral (artículo 220 de la LFDA):

[369] La ley no hace referencia sobre quiénes son las autoridades competentes

a) El conflicto será resuelto por un grupo arbitral que se conformará de 2 árbitros designados por cada una de las partes y un presidente que será electo por éstos dos árbitros.
b) A partir de la fecha en que los árbitros acepten su cargo, el arbitraje deberá de durar un máximo de 60 días (artículo 224 de la LFDA).
c) El procedimiento arbitral terminará cuando se dicte el laudo, o bien, por acuerdo entre las partes antes de que se dicte (artículo 225 de la LFDA).
d) El laudo arbitral deberá darse por escrito, deberá de estar fundado y motivado y será definitivo, inapelable y obligatorio para las partes, teniendo carácter de cosa juzgada y título ejecutivo (art 226 LFDA). Aunque cualquiera de las partes podrá pedir por escrito al instituto que aclare los puntos resolutivos, rectifique algún error de cálculo, tipográfico o cualquier otro de naturaleza similar, siempre que no se modifique el sentido del laudo (artículo 227 de la LFDA).
e) Los gastos que se originen con motivo del procedimiento arbitral, corren a cargo de las partes. El pago de honorarios será cubierto conforme al arancel que expida anualmente el Instituto (artículo 228 de la LFDA).

En el documento informativo sobre el uso de medios alternativos de solución de conflictos en materia de derecho de autor en México, el director general del INDAUTOR informa que en el año 2013 se recibieron un total de 1,150 quejas para solucionar conflictos por estos medios[370].

Además señala que el INDAUTOR tiene como objetivo mejorar el procedimiento de avenencia, usando medios tecnológicos para organizar juntas de avenencia en línea[371].

[370] Guerra Zamarro, Manuel, "Medios alternativos de solución de controversias en materia de derecho de autor en México", 20 de Diciembre 2013 a consulta en página: http://www.wipo.int/meetings/es/doc_details.jsp?doc_id=262778 p.7
[371] Ibid p. 8

7.4.2. Instituto Mexicano de la Propiedad Industrial (IMPI)

Implementa el registro y la protección de patentes, modelos de utilidad, diseños industriales y marcas de acuerdo a la Ley de Propiedad Industrial (LPI). Es importante que tanto las empresas como, en su caso, las Administraciones Públicas, conozcan la importante labor que desarrolla el IMPI en cuanto a la protección de derechos de autor, especialmente en el caso de las licencias de *software*, y derechos de propiedad industrial.

La LFDA delega al IMPI la función de investigar, ordenar y practicar visitas de inspección, requerir información y datos para determinar si alguna empresa o institución usa programas sin cumplir con la licencia correspondiente (artículo 234 de la LFDA).

En el título séptimo (artículos del 204 al 211) de la LPI se determina la forma de hacer la inspección, infracciones y sanciones administrativas que llevará a cabo el IMPI, tales como:

- **Solicitar informes y datos** (copia de la factura de compra de licencias de aplicaciones o sistemas operativos propietarios para tantas PCs existentes en un establecimiento)

- **Realizar visitas de inspección** (para examinar qué programas están instalados en cada PC, conforme al artículo 205). Durante las visitas de inspección, el personal comisionado por el instituto podrá tomar fotografías, hacer videos o recabar cualquier otro instrumento admisible como prueba en la Ley Federal de procedimiento administrativo y el código Federal de Procedimientos Civiles. Dichos instrumentos pueden ser utilizados por el Instituto como elementos con pleno valor probatorio (artículo 205 de la LPI). Es importante destacar que los propietarios o encargados de los establecimientos tienen la obligación de permitir el acceso al personal del IMPI comisionado para las visitas de inspección, y que de negarles el acceso, se hará constar en el acta respectiva y se presumirán ciertos los

hechos que se le imputen en los procedimientos correspondientes (artículo 206 de la LPI). Las actas derivadas de las visitas de inspección deberán contar con la firma de testigos, y los visitados podrán ofrecer pruebas en relación a los hechos contenidos en el acta (artículos 209 y 210 de la LPI)

- **Asegurar equipos**. Si durante la diligencia (de inspección) se comprueba fehacientemente la comisión de cualquiera de los actos o hechos considerados como infracción administrativa o delitos, el inspector puede asegurar, de forma cautelar los productos con los que se está cometiendo dichas infracciones o delitos. Se levantará un inventario de los bienes asegurados, que constará en el acta de inspección y se designa como depositario al encargado o propietario del establecimiento en donde se encuentre (artículo 211 de la LPI). Se aseguran cosas como: equipo, instrumentos, maquinaria, dispositivos, diseños, especificaciones, planos, manuales, moldes, clisés, placas o cualquier otro medio utilizado para la realización de hechos considerados como infracciones o delitos. A su vez se pueden asegurar libros, registros, documentos, modelos, muestras, etiquetas, papelería, material publicitario, facturas y en general cualquier otro del que se puedan inferir elementos de prueba; finalmente, mercancías, productos y cualesquiera otros bienes en los que se materialice la infracción a los derechos protegidos (artículo 212BIS de la LPI).

- **Decidir el destino de los bienes asegurados**. En caso de que la resolución definitiva de la controversia declare que se ha cometido una infracción administrativa, el Instituto pondrá a disposición de la autoridad judicial competente, o bien del árbitro, los bienes que se hubiesen asegurado. De no ser el caso, entonces cada uno de los interesados deberá presentar una propuesta (dentro de los 5 días siguientes al en que se les dé vista) sobre el destino de los bienes; de no recibirse propuestas, el Instituto podrá decidir si los bienes se donarán (a entidades de la administración pública Federal, o estados municipios, o

instituciones de beneficencia) o bien si se deberán de destruir (artículo 212BIS-2 LPI).

7.5. Jurisprudencia en materia de licencias de *software*

Los principales criterios jurisprudenciales sobre licencias de software son los siguientes:

a) Cuando la controversia sobre que versó el juicio arbitral se refiera a intereses particulares de orden exclusivamente patrimonial, como lo son los derechos de autor, la Federación no es parte y en tal virtud las acciones deben fundarse, tramitarse y resolverse conforme a lo establecido en la LFDA y sus reglamentos, siendo supletoria la legislación común, es decir el Código de Procedimientos Civiles para el Distrito y Territorio Federales, de conformidad con lo dispuesto por el artículo 146 de dicha ley 372.

b) Los elementos que integran el delito previsto por el artículo 135, fracción I, de la abrogada Ley Federal de Derechos de Autor son: a) Que una persona, con fines de lucro, explote una obra protegida por la ley; y b) Que dicha explotación se realice sin el consentimiento del titular del derecho de autor. Ahora bien, existiendo un convenio para la explotación de una obra creada por el pasivo, en el que se pactó el uso de sus derechos con fines de lucro, mediante el pago de cierta suma, es inexacto que por el solo hecho de que el activo omita pagar esa cantidad, se tipifique la figura delictiva señalada, pues la sola existencia de dicho convenio excluye el elemento correspondiente a la falta de consentimiento exigida por el tipo penal descrito373.

---

372 Semanario Judicial de la Federación, Séptima Época, Instancia: Tercer Tribunal Colegiado en materia administrativa del primer circuito, Tomo 90, sexta parte bajo el rubro: DERECHOS DE AUTOR, ARBITRAJE EN ACCIONES SOBRE. SUPLETORIEDAD DEL CÓDIGO DE PROCEDIMEINTOS CIVILES DEL DISTRITO Y TERRITORIOS FEDERALES.

373 Semanario Judicial de la Federación y su Gaceta, Novena Época, Instancia: Tribunales Colegiados de Circuito, Tomo V mayo 1997 bajo el rubro: AUTOR, DERECHOS DE. LA OMISIÓN DE PAGAR LO CONVENIDO POR SU EXPLOTACIÓN NO TIPIFICA LA CONDUCTA ILÍCITA CONTENIDA EN EL ARTÍCULO 135 FRACCIÓN I, DE LA LEY RESPECTIVA.

c) Aun cuando el IMPI no es un tribunal jurisdiccional, sino un organismo descentralizado con personalidad jurídica y patrimonio propios, tiene la facultad de sustanciar los procedimientos de declaración de infracción administrativa[374], lo cual implica un acto materialmente jurisdiccional suficiente y eficaz para constituir base y prueba firme de la existencia de la infracción. Al ser un elemento altamente especializado, puede utilizarse posteriormente en el ejercicio de la acción de indemnización por daños y perjuicios en la vía civil. Dado que la responsabilidad civil se prueba siempre que concurra la comisión de un hecho, la producción de un daño moral o material en perjuicio de otra persona y una relación de causa y efecto entre los dos elementos, el juez –que conozca de la reclamación de daños y perjuicios- debe ponderar si fueron producto directo de la infracción declarada por el IMPI[375].

8. El documento electrónico y la firma electrónica

8.1. Firma electrónica

En México la firma electrónica ha seguido un camino diferente, desde el punto de vista normativo, por lo que se refiere al sector privado y al público, ya que con respecto al primero, el uso de la firma electrónica fue regulado en virtud del Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica[376].

---

[374] Conforme al artículo 231 de la LFDA constituyen infracciones en materia de comercio, fracción VII “usar, reproducir, o explotar una reserva de derechos protegida o un programa de cómputo sin el consentimiento del titular” ver p. 5 y ss

[375] Seminario Judicial de la Federación y su Gaceta, Novena Época, Instancia Primera Sala SCJ, Tomo XXVIII, agosto 2008, bajo el rubro: DERECHOS DE AUTOR. LAS RESOLUCIONES ADMINISTRATIVAS DICTADAS POR EL INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL CON MOTIVO DEL PROCEDIMIENTO DE INFRACCIÓN ADMINISTRATIVA PREVISOT EN LOS ARTÍCULOS 231 Y 232 DE LA LEY FEDERAL RELATIVA, AL SER ACTOS MATERIALAMENTE JURISDICCIONALES QUE CONSTITUYEN BASE Y PRUEBA FIRME DE LA EXISTENCIA DE UNA INFRACCIÓN, PUEDEN UTILIZARSE EN EL EJERCICIO DE LA ACCIÓN INDEMNIZATORIA POR DAÑOS Y PERJUICIOS EN LA VÍA CIVIL.

[376] Publicado en el Diario Oficial de la Federación el 29 de agosto de 2003 y disponible en la dirección e Internet http://www.diputados.gob.mx/LeyesBiblio/ref/ccom/CCom_ref29_29ago03.doc.

El Código de Comercio se vería complementado posteriormente, en materia de firma electrónica, por un Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación[377]; las Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación[378], así como por la Norma Oficial Mexicana NOM-151-SCFI-2002, Prácticas comerciales-Requisitos que deben observarse para la conservación de mensajes de datos[379].

Y en el caso del sector público, a nivel federal, la normatividad básica en la materia se encuentra en la Ley de Firma Electrónica Avanzada[380] (en adelante, LFEA) y en el Reglamento de la Ley de Firma Electrónica Avanzada[381]. Además, en el sector público hay que tomar en consideración las normas publicadas por diferentes órganos, tales como la Secretaría de la Función Pública, la Suprema Corte de Justicia de la Nación, el Consejo de la Judicatura Federal, o el Servicio de Administración Tributaria. Al respecto, por lo que se refiere a normas anteriores a la LFEA, como acabamos de indicar, se considerarán abrogadas aquéllas que se opongan a la LFEA.

En cualquier caso, tanto el documento electrónico como la firma electrónica son claves ya que, en el primer caso, constituyen el soporte de los negocios hechos por medios electrónicos, igual que el papel en el entorno no electrónico y, en el segundo caso, sirven para cumplir con las mismas funciones que la firma manuscrita que aparece en el papel. Es decir, cumple entre otras, las funciones de autenticación, integridad y no repudio, que son básicas para la realización de transacciones, públicas o privadas, en el entorno electrónico, de manera que el uso

---

377 Publicado en el Diario Oficial de la Federación el 19 de julio de 2004 y disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/ccom/CCom_ref29_29ago03.doc

378 Publicadas y disponibles en el Diario Oficial de la Federación del 10 de agosto de 20004, en la dirección de Internet http://www.dof.gob.mx/nota_detalle.php?codigo=666281&fecha=10/08/2004

379 Publicadas en el Diario Oficial de la Federación el 4 de junio de 2002 y disponibles en http://www.dof.gob.mx/nota_detalle.php?codigo=727725&fecha=04/06/2002

380 Expedidas mediante Decreto publicado en el Diario Oficial de la Federación el 11 de enero de 2012 y disponible en http://dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012 Es importante tomar en consideración que, en virtud de lo dispuesto en su artículo transitorio segundo *"[s]e derogan todas aquellas disposiciones legales y administrativas que se opongan a lo previsto en esta Ley."*

381 Publicado en el Diario Oficial de la Federación el 21 de marzo de 2014 y disponible en http://dof.gob.mx/nota_detalle.php?codigo=5337860&fecha=21/03/2014

del documento electrónico y la firma electrónica está presente de manera constante en nuestras vidas y en el caso del cómputo en la nube es clave para aportar garantías jurídicas a través de procesos y procedimientos tecnológicos.

En este sentido, por ejemplo, la criptografía de clave pública puede ser utilizada para cifrar datos, personales o no, que se almacenan en la nube lo que, en parte, puede servir también para minimizar riesgos.

8.1.1. Tipos de firma electrónica

En el Código de Comercio artículo 89, se definen dos tipos, la firma electrónica simple (NIP, CIEC[382]) y la firma electrónica avanzada o fiable (Fiel). Ambas conviven en el ámbito fiscal, comercial y bancario y seguirán siendo jurídicamente válidas[383].

La firma electrónica es simplemente definida como: *"los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio."*[384]

Por otro lado, la Firma Electrónica Avanzada o Fiable es aquella firma electrónica que cumpla con los requisitos del artículo 97:

a) Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

---

[382] NIP: Número de Identificación Personal

[383] Sobre esta cuestión, cabe recordar que la LFEA, ya citada, indica en el segundo párrafo de su artículo 4 que: *"En los actos de comercio e inscripciones en el Registro Público de Comercio, el uso de la firma electrónica avanzada se regirá de conformidad con lo previsto en el Código de Comercio y demás ordenamientos aplicables en la materia, sin perjuicio de la aplicación de lo dispuesto en esta Ley en lo que resulte procedente."*

[384] Código de Comercio. Última reforma publicada el 13.06.2014, http://www.diputados.gob.mx/LeyesBiblio/pdf/3_130614.pdf

b) Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
c) Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y
d) Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma

La Firma Electrónica Avanzada (Fiel) es un archivo digital que identifica al individuo al realizar trámites por internet y ante el Servicio de Administración Tributaria (SAT)[385] e incluso en otras dependencias del Gobierno de la República. Su diseño se basa en estándares internacionales de infraestructura de claves públicas (*Public Key Infrastructure*, PKI) en donde se utilizan dos claves o llaves para el envío de mensajes:

- La llave o clave privada que únicamente es conocida por el titular de la Fiel, que sirve para cifrar datos; y
- La "llave o clave pública", disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran datos[386].

En general, la Fiel se usa para que los ciudadanos puedan realizar trámites administrativos y gubernamentales a través de internet; se pretende facilitar la interacción entre el gobierno y los ciudadanos que no tendrán que realizar desplazamientos innecesarios a las instituciones públicas[387].

---

[385] El SAT es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, que tiene la responsabilidad de aplicar la legislación fiscal y aduanera, con el fin de que las personas físicas y morales contribuyan proporcional y equitativamente al gasto público; de fiscalizar a los contribuyentes para que cumplan con las disposiciones tributarias y aduaneras; de facilitar e incentivar el cumplimiento voluntario, y de genera y proporcionar la información necesaria para el diseño y la evaluación de la política tributaria. Además administra los procesos de recaudación de las contribuciones federales y de entrada – salida de mercancías del territorio nacional, controlando el riesgo y promoviendo el cumplimiento correcto y voluntario de las obligaciones fiscales. En: Qué es el SAT? Página oficial del SAT http://www.sat.gob.mx/que_sat/Paginas/default.aspx

[386] Izquierdo Enciso, León, "La implementación de la firma electrónica en México" Economía Informa núm. 369, julio 2011, disponible en la página: http://www.economia.unam.mx/publicaciones/econinforma/369/08leonizquierdo.pdf

[387] Ibid. p. 100

8.1.2. Instituciones de gobierno encargadas del manejo de la Firma Electrónica

La Secretaría de la Función Pública[388] es la dependencia facultada para interpretar la legislación y emitirá junto con la Secretaría de Economía y el Sistema de Administración Tributaria las disposiciones generales sobre el tema de la Firma Electrónica Avanzada (artículo 5 de la Ley de Firma Electrónica Avanzada[389]).

Además, estas mismas secretarías son consideradas autoridades certificadoras para emitir certificados digitales en términos de la LFEA (artículo 23). Sin embargo, es posible que otras dependencias y entidades distintas, que estén interesados en tener el carácter de autoridad certificadora en términos de la LFEA puedan hacerlo siempre y cuando cuenten con el dictamen favorable de la Secretaría de la Función Pública (artículo 24 LFEA).

Adicionalmente, los notarios y corredores públicos y las personas morales de carácter privado deberán presentar el documento emitido por la Secretaría de Economía que los acredite como prestadores de servicios de certificación, en virtud de haber cumplido con los requisitos establecidos en el Código de Comercio y su Reglamento (artículo 24 LFEA).

---

[388] La Secretaría de la Función Pública, dependencia del Poder Ejecutivo Federal, vigila que los servidores públicos federales se apeguen a la legalidad durante el ejercicio de sus funciones, sanciona a los que no lo hacen así; promueve el cumplimiento de los procesos de control y fiscalización del gobierno federal, de disposiciones legales en diversas materias, dirige y determina la política de compras públicas de al Federación, coordina y realiza auditorías sobre el gasto de recursos federales, coordina procesos de desarrollo administrativo, gobierno digital, opera y encabeza el Servicios Profesional de Carrera, coordina las labores de los órganos internos de control en cada dependencia del gobierno federal y evalúa la gestión de las entidades también a nivel federal. http://www.funcionpublica.gob.mx/

[389] Ley de Firma Electrónica Avanzada disponible en
: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf

8.1.3. Atribuciones y obligaciones de las autoridades certificadoras

a) Emitir, administrar y registrar certificados digitales, así como prestar servicios relacionados con la firma electrónica avanzada;
b) Llevar un registro de los certificados digitales que emitan y de los que revoquen, así como proveer los servicios de consulta a los interesados;
c) Adoptar las medidas necesarias para evitar la falsificación, alteración o uso indebido de certificados digitales, así como de los servicios relacionados con la firma electrónica avanzada;
d) Revocar los certificados de firma electrónica avanzada, cuando se actualice alguno de los supuestos previstos en el artículo 19 de la LFEA[390] conforme a los procedimientos a que se refiere el artículo 18 de la misma;
e) Garantizar la autenticidad, integridad, conservación, confidencialidad y confiabilidad de la firma electrónica avanzada, así como de los servicios relacionados con la misma;
f) Preservar la confidencialidad, integridad y seguridad de los datos personales de los titulares de los certificados digitales en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, su Reglamento y demás disposiciones aplicables, y
g) Las demás que les confieran las disposiciones jurídicas aplicables.
h) Lo anterior, sin perjuicio de las atribuciones que, en su carácter de autoridad certificadora, corresponden al Servicio de Administración Tributaria en términos de la legislación fiscal y

[390] El artículo 19 previene que el certificado digital quedará sin efectos o será revocado por la autoridad certificadora que lo emitió, cuando se actualice alguno de los supuestos siguientes: por expiración de vigencia; cuando se compruebe que los documentos que presentó el titular del certificado digital para acreditar su identidad son falsos; cuando así lo solicite el titular del certificado digital a la autoridad certificadora que lo emitió; por fallecimiento del titular del certificado digital; cuando se extravíe o inutilice por daños el medio electrónico que contenga los certificados digitales; cuando se ponga en riesgo la confidencialidad, integridad o seguridad de los datos de creación de la firma electrónica avanzada y Por resolución de autoridad judicial o administrativa que así lo determine.

aduanera.

8.1.4. Obtención de firma electrónica

De conformidad con el acuerdo de la Secretaría de la Función Pública[391], las Dependencias o Entidades de la Administración Pública Federal que Requieran integrarse como AC[392] en la ITFEA[393], con el fin de obtener el reconocimiento de sus Certificados Digitales, deberán ajustar sus procedimientos y formas de operación a efecto de cumplir con los lineamientos dados por la propia SFP[394].

La FIEL debe obtenerse mediante trámite ante las oficinas del SAT, con una identificación oficial vigente y el CURP[395] certificado. En caso de no contar con la CURP certificada en el Registro Nacional de Población, se debe de presentar un acta de nacimiento original.

En caso de personas morales, el representante legal debe contar con Fiel activa y presentar el poder general para actos de dominio o de administración, así como el acta constitutiva de la persona moral.

---

[391] Más sobre el acuerdo, en la página 27

[392] Se entiende por AC, las Dependencias, Entidades, Organizaciones, Instituciones y Proveedores de Servicios de Certificación que cuentan con la infraestructura tecnológica para la emisión y registro de Certificados Digitales de Firma Electrónica Avanzada. Esta infraestructura Tecnológica también será entendida como Agencia o Autoridad Certificadora. En: SEGUNDO, Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la administración pública Federal. http://cidge.gob.mx/cidge_hist/doc/Lineamientos.pdf

[393] ITFEA es la Infraestructura Tecnológica que permite la interoperabilidad y el reconocimiento de Certificados Digitales de Firma Electrónica Avanzada entre las Autoridades o Agencias Certificadoras que la integran. Ibid

[394] Ibid en TERCERO

[395] La Clave Única de Registro de Población, mejor conocida como CURP, es un instrumento que sirve para registrar en forma individual a todos los habitantes de México, nacionales y extranjeros, así como a los mexicanos que radican en otros países. Se conforma de 18 elementos de un código alfanumérico (los primeros 16 elementos se conforman por la primer letra y primer vocal interna del primer apellido, primer letra del segundo apellido, primer letra del primer nombre, año, mes y día de la fecha de nacimiento, género, dos letras del lugar de nacimiento de acuerdo al código de la Entidad Federativa y los últimos dos dígitos son asignados por el Registro Nacional de la Población). En: ”Qué es la CURP?” página de la Presidencia de la República: http://www.presidencia.gob.mx/que-es-la-curp/

Las citas para todas las oficinas del SAT en toda la República se gestionan a través de la página de dicho organismo[396]. Además, para agilizar el trámite se recomienda descargar el programa de solicitud de certificado digital de Fiel, en donde se puede proporcionar la RFC, la CURP y una cuenta de correo electrónico[397]. Al concluir el trámite, el SAT regresa los archivos de la Fiel, junto con la solicitud sellada[398].

8.1.5. Validez y eficacia probatoria

La Ley de Firma Electrónica Avanzada[399] (LFEA) regula el uso de la Fiel y la expedición de certificados digitales a personas físicas; los servicios relacionados con la Fiel, y la homologación de la Fiel con las firmas electrónicas avanzadas regulados por otros ordenamientos legales. En el título segundo de la LFEA se establece el uso y validez de la misma[400]:

Conforme al Artículo 7 de la LFEA, la Fiel podrá ser utilizada en documentos electrónicos y, en su caso, en mensajes de datos. Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán **los mismos efectos que los presentados con firma autógrafa** y, en consecuencia, tendrán **el mismo valor probatorio** que las disposiciones aplicables a éstos.

Para tener el efecto mencionado en el artículo 7 de la LFEA**,** el artículo 8 señala que **la firma electrónica avanzada deberá cumplir con los principios** rectores siguientes:
I. Equivalencia Funcional: Consiste en que la firma electrónica avanzada en un documento electrónico o en su caso, en un mensaje

396 https://citas.sat.gob.mx/citasat/home.aspx
397 Dicho programa se encuentra disponible para descarga en la página: http://www.sat.gob.mx/fichas_tematicas/fiel/Paginas/sugerencias_agilizar_tramite.aspx.
398 En "Cómo obtener tu FIEL" página del SAT http://www.sat.gob.mx/fichas_tematicas/fiel/Paginas/obtener_fiel.aspx
399 Diario Oficial de la Federación, 11/01/2012 http://www.dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012
400 http://www.dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012

de datos, satisface el requisito de firma del mismo modo que la firma autógrafa en los documentos impresos;
II. Autenticidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que el mismo ha sido emitido por el firmante de manera tal que su contenido le es atribuible al igual que las consecuencias jurídicas que de él deriven;
III. Integridad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, permite dar certeza de que éste ha permanecido completo e inalterado desde su firma, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene como resultado del proceso de comunicación, archivo o presentación;
IV. Neutralidad Tecnológica: Consiste en que la tecnología utilizada para la emisión de certificados digitales y para la prestación de los servicios relacionados con la firma electrónica avanzada será aplicada de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular;
V. No Repudio: Consiste en que la firma electrónica avanzada contenida en documentos electrónicos garantiza la autoría e integridad del documento y que dicha firma corresponde exclusivamente al firmante, y
VI. Confidencialidad: Consiste en que la firma electrónica avanzada en un documento electrónico o, en su caso, en un mensaje de datos, garantiza que sólo pueda ser cifrado por el firmante y el receptor.

En el caso del Código de Comercio, en cuanto a los principios que rigen la aplicación de las actividades previstas en el mismo en materia de firma electrónica, el artículo 89 hace referencia a los *"de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa."*

Así mismo, para que los sujetos obligados puedan utilizar la Fiel en los actos a que se refiere la LFEA, deberán contar con un certificado

digital vigente, emitido u homologado, y una clave privada, generada bajo su exclusivo control (articulo 9 de la LFEA).

Es importante señalar que la LFEA también previene sobre la validez de los documentos electrónicos y de los mensajes de datos (título segundo). Además, de define la estructura y procedimientos del certificado digital (título tercero), los que pueden ser emitidos por la secretaría de la función pública, la secretaría de economía, y el servicio de administración tributaria, y otras dependencias y entidades.

Por último, cabe señalar que la nueva Ley de Amparo, en su artículo tercero, establece que el uso optativo de la firma electrónica para la presentación de escritos en un juicio de amparo[401].

[401] *"… Los escritos en forma electrónica se presentarán mediante el empleo de las tecnologías de la información, utilizando la Firma Electrónica conforme la regulación que para tal efecto emita el Consejo de la Judicatura Federal.*

La Firma Electrónica es el medio de ingreso al sistema electrónico del Poder Judicial de la Federación y producirá los mismos efectos jurídicos que la firma autógrafa, como opción para enviar y recibir promociones, documentos, comunicaciones y notificaciones oficiales, así como consultar acuerdos, resoluciones y sentencias relacionadas con los asuntos competencia de los órganos jurisdiccionales.

En cualquier caso, sea que las partes promuevan en forma impresa o electrónica, los órganos jurisdiccionales están obligados a que el expediente electrónico e impreso coincidan íntegramente para la consulta de las partes.

El Consejo de la Judicatura Federal, mediante reglas y acuerdos generales, determinará la forma en que se deberá integrar, en su caso, el expediente impreso.

Los titulares de los órganos jurisdiccionales serán los responsables de vigilar la digitalización de todas las promociones y documentos que presenten las partes, así como los acuerdos, resoluciones o sentencias y toda información relacionada con los expedientes en el sistema, o en el caso de que éstas se presenten en forma electrónica, se procederá a su impresión para ser incorporada al expediente impreso. Los secretarios de acuerdos de los órganos jurisdiccionales darán fe de que tanto en el expediente electrónico como en el impreso, sea incorporada cada promoción, documento, auto y resolución, a fin de que coincidan en su totalidad. El Consejo de la Judicatura Federal, en ejercicio de las facultades que le confiere la Ley Orgánica del Poder Judicial de la Federación, emitirá los acuerdos generales que considere necesarios a efecto de establecer las bases y el correcto funcionamiento de la Firma Electrónica.

No se requerirá Firma Electrónica cuando el amparo se promueva en los términos del artículo 15 de esta Ley".

Sobre juicio de amparo y nuevas tecnologías es pertinente revisar: Ferrer Mc-Gregor, Eduardo y Sánchez Gil, Rubén (2014), *El nuevo juicio de amparo. Guía de la Reforma Constitucional y la Nueva Ley de Amparo*, UNAM/ Porrúa / IMDPC, Séptima edición, México.

8.1.6. Instituciones de gobierno

8.1.6.1. Secretaría de la Función Pública[402]

En lo relativo a la Firma Electrónica, es importante destacar que la SFP tiene a su cargo el desempeño de las atribuciones y facultades que le encomiendan, entre otras, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP).

La LAASSP, faculta a la SFP a anunciar programas anuales de adquisiciones de servicios, emitir políticas, bases y lineamientos en ésta materia. Por ejemplo, la SFP es la que se encargó de dar a conocer el Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la Firma Electrónica Avanzada en la Administración Pública Federal[403].

8.1.6.2. Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE)

Es un órgano estratégico que fue creado mediante un Acuerdo Presidencial en diciembre de 2005. Su fin es promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones (TICs), mediante la coordinación de acciones entre la Secretaría de la Función Pública con las dependencias de la administración pública federal y las entidades paraestatales[404].

El “gobierno electrónico” se entiende como las políticas, acciones y criterios para el uso y aprovechamiento de las tecnologías de información y comunicaciones, con la finalidad de mejorar la entrega de servicios al ciudadano; la interacción del gobierno con la industria;

---

[402] Una descripción general de la SFP se encuentra en la página 1 de éste documento

[403] Dicho acuerdo se encuentra publicado en: http://cidge.gob.mx/cidge_hist/doc/Lineamientos.pdf

[404] Acuerdo en el que se crea de forma permanente la comisión intersecretarial para el desarrollo del gobierno electrónico, publicado en el diario oficial de la Federación 09/12/2005 http://www.normateca.gob.mx/Archivos/ACUERDO%20QUE%20TIENE%20POR%20OBJETO%20CREAR%20EN%20FORMA%20PERMANENTE%20LA%20COMISION%20INTERSECRETARIAL%20PARA%20EL%20DESARROLLO%20DEL%20GOBIERNO%20ELECTRONICO.PDF

facilitar el acceso del ciudadano a la información de éste, así como hacer más eficiente la gestión gubernamental para un mejor gobierno y facilitar la interoperabilidad entre las dependencias y Entidades.

Dentro de sus funciones se encuentra[405]: el conocer y opinar sobre el programa anual de actividades para el desarrollo del Gobierno Electrónico; promover el establecimiento de mecanismos de coordinación y colaboración con los poderes federales, los gobiernos de las entidades federativas y de los municipios, a fin de propiciar el intercambio de información y experiencias, el análisis de problemáticas comunes y la realización de proyectos conjuntos en materia de Gobierno Electrónico y TIC; promover el establecimiento de mecanismos de interoperabilidad que permitan el aprovechamiento de las infraestructuras tecnológicas y de los procesos horizontales a través de la Administración Pública Federal (APF); promover entre las Dependencias y Entidades, de acuerdo con los resultados y acciones que le informe la Subcomisión de los Sistemas Automatizados de Control de Gestión, los mecanismos para la aplicación de los criterios de interoperabilidad y los lineamientos para la estandarización de los sistemas automatizados de control de gestión y su comunicación a través del uso de medios electrónicos; establecer el marco normativo que sea indispensable para su operación y cualquier otra función necesaria para cumplir su objeto.

8.1.6.3. Subcomisión Firma Electrónica Avanzada

Con el fin de establecer las condiciones técnicas que permitan el reconocimiento de los Certificados Digitales de la Firma EA, así como la interoperabilidad entre las autoridades certificados que integran la subcomisión, en el 2006 se publicaron en el Diario Oficial, los Lineamientos para la Homologación, Implantación y Operación de la Firma Electrónica en la Administración Pública Federal.

Éste documento describe la Infraestructura Tecnológica de la Firma Electrónica Avanzada y los procedimientos que deberán seguir

[405] Ver más funciones de la CIDGE, en su página http://cidge.gob.mx/menu/gobernabilidad/cidge/funciones/

todas las Autoridades Certificadores para la emisión y operación de Certificados Digitales, así como, las características técnicas de la estructura de los mismos[406].

8.1.7. Jurisprudencia

Respecto a este tema, la Suprema Corte de Justicia se ha pronunciado en pocas ocasiones. Dichos pronunciamientos se han enfocado a la manera en que se regula la firma electrónica en el derecho fiscal, como se muestra en las siguientes tesis jurisprudenciales:

"**FIRMA ELECTRÓNICA AVANZADA. EL ARTÍCULO 19-A DEL CÓDIGO FISCAL DE LA FEDERACIÓN QUE LA PREVÉ COMO MEDIO PARA QUE LAS PERSONAS MORALES CUMPLAN CON SUS OBLIGACIONES FISCALES, NO VIOLA EL PRINCIPIO DE EXACTA APLICACIÓN DE LA LEY PENAL**" [Novena Época, Registro: 161623, Instancia: Primera Sala, Tipo de Tesis: Aislada, Fuente: Semanario Judicial de la Federación y su Gaceta, Tomo XXXIV, Julio de 2011, Materia(s): Constitucional Tesis: 1a. CXXVI/2011 , Página: 293];

"**FIRMA ELECTRÓNICA AVANZADA. EL ARTÍCULO 19-A, TERCER PÁRRAFO, DEL CÓDIGO FISCAL DE LA FEDERACIÓN, NO VIOLA EL PRINCIPIO DE DEFENSA ADECUADA**" [Novena Época, Registro: 161622, Instancia: Primera Sala, Tipo de Tesis: Aislada, Fuente: Semanario Judicial de la Federación y su Gaceta, Tomo XXXIV, Julio de 2011, Materia(s): Constitucional, Tesis: 1a. CXXVII/2011, Página: 294];

"**FIRMA ELECTRÓNICA AVANZADA. EL HECHO DE QUE EL CÓDIGO FISCAL DE LA FEDERACIÓN NO ESTABLEZCA SU DEFINICIÓN NO VIOLA LA GARANTÍA DE LEGALIDAD**" [Novena Época, Registro: 171757, Instancia: Segunda Sala, Tipo de Tesis:

[406] Página de la subcomisión http://cidge.gob.mx/cidge_hist/pag/docfea.html

Aislada, Fuente: Semanario Judicial de la Federación y su Gaceta, Tomo XXVI, Agosto de 2007, Materia(s): Constitucional, Administrativa, Tesis: 2a. XCVII/2007, Página: 638].

8.2. Documentos electrónicos

El documento electrónico se puede definir como el conjunto de impulsos eléctricos que recaen en un soporte de computadora y que permiten su traducción natural a través de una pantalla o una impresora. Las características del documento electrónico son: inalterabilidad, y puede ser usado como documento probatoria si cuenta con un sistema de cifrado y de firma digital ya que se entiende que así no habrá sido alterado[407].

Incluso las dependencias y entidades en las comunicaciones y, en su caso, actos jurídicos que realicen entre las mismas, harán uso de mensajes de datos y aceptarán la presentación de documentos electrónicos, los cuales deberán contar, cuando así se requiera, con la firma electrónica avanzada (Fiel) del servidor público facultado para ello (artículo 10 de la LFEA).

Conforme a las definiciones del Código de Comercio, hay que distinguir entre el documento electrónico, cuya definición ya hemos expuesto, y el mensaje de datos, siendo éste definido en el artículo 89, ya citado, como *"la información generada, enviada, recibida o archivada por medios electrónicos o cualquier otra tecnología."*

Ya se trate de un documento electrónico o de un mensaje de datos, la nube es una oportunidad para las organizaciones y las entidades y dependencias de la Administración Pública, dado que suponen la posibilidad de almacenar y procesar ingentes cantidades de información a un costo muy bajo. Y unido a esto, la posibilidad de acceder desde cualquier lugar y en cualquier momento facilita la

[407] Olmos Jasso, María Teresa, "Valor probatorio de los documentos electrónicos" publicado en: http://www.tfjfa.gob.mx/investigaciones/pdf/valorprobatoriodelosmedioselectronicos.pdf (2009) p.10

movilidad de los usuarios[408], lo que se convierte en una ventaja competitiva o redunda en le eficiencia de los clientes de servicios de cómputo en la nube.

8.2.1. Validez y eficacia probatoria

Las dependencias y entidades en la realización de actos oficiales deberán aceptar el uso de mensajes de datos y aceptarán la presentación de documentos electrónicos cuando las mismas ofrezcan esta posibilidad… (y) siempre que los particulares por sí o… a través de personas autorizadas… manifiesten expresamente su conformidad para que dichos actos se efectúen, desde su inicio hasta su conclusión a través de medios de comunicación electrónica (artículo 11 LFEA).

Dicha manifestación además deberá señalar que se acepta consultar el tablero electrónico, darse por notificado de las actuaciones electrónicas que emita la dependencia, y que en el supuesto de que por causeas imputables a la dependencia o entidad se encuentren imposibilitados para consultar el tablero electrónico o abrir los documentos electrónicos, lo harán del conocimiento de la dependencia o entidad (articulo 11 fracciones I, II y III).

En el artículo 2014-A del Código Federal de Procedimientos Civiles se reconocen como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Se señala que para valorar la fuerza probatoria, se estimará primordialmente la fiabilidad del método en que se haya obtenido, comunicado, recibido o archivado. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, el

---

[408] Véase, VV.AA., La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo, ya citado. En dicho documento se indica al respecto que: *"El cómputo en la nube supone una auténtica revolución para los usuarios ya que permite un nivel de movilidad; acceso a la información desde cualquier lugar, dispositivo y momento así como trabajo colaborativo que hasta la fecha no eran posibles en la medida en que el cómputo los facilita.*
Por último, el cómputo en la nube significa también que las pequeñas empresas puedan competir con las grandes, ya que los diferenciales competitivos que se daban en cuanto al uso tradicional de las tecnologías de la información desaparecen gracias a aquél "

requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos (ópticos o cualquier otra tecnología) se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vea en su forma definitiva y ésta puede ser accesible para su ulterior consulta.

9. Delitos informáticos

Los delitos informáticos son las actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (en donde la informática es el medio o instrumento para realizar el delito), o bien tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos per se).

La tipicidad del delito informático en México, está definida en cada una de las entidades federativas. Pero también el Código Penal Federal, con reformas que entraron en vigor el 7 de julio del 2014 en el título noveno, capítulo segundo contempla la tipificación del acceso ilícito a sistemas y equipos de informática:

Artículo 211 bis 1.- Al que sin autorización **modifique, destruya o provoque pérdida de información** contenida en sistemas o equipos de informática **protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a dos años de prisión…
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de 50 a 150 días de multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en **sistemas o equipos de informática del Estado**, protegidos por algún mecanismo de seguridad… (de 1 a 4 años de prisión)

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad… (de 6 meses a 2 años de prisión).

Artículo 211 bis 3.- tipifica el delito para quien estando autorizado para acceder sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de la información (de 2 a 8 años de prisión), la copie o la utilice (de forma indebida).

Artículo 211 bis 4.- tendrá diversa pena quien "modifique, destruya o provoque pérdida" de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero… o que conozca o copie información contenida en equipos o sistemas de informática de las instituciones que integran el sistema financiero…

Art 211 bis 5.- para quien estando autorizado para acceder a la información contenida en sistemas y equipos de informática de instituciones que integran el sistema financiero (indebidamente modifique, destruya o provoque pérdida de información… indebidamente copie la información contenida…)[409]

9.1. Notas sobre los delitos informáticos en el Código Penal Federal

Cabe aclarar que el Código Penal Federal sólo ampara sistemas informáticos protegidos por "mecanismos de seguridad". Además no define qué se entiende por un "mecanismo de seguridad".

[409] Más sobre delitos informáticos en:
http://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

Hay varios tipos de delitos informáticos que no están tipificados: virus, denegación de servicios, ciberacoso, *phishing*, *happySlapping*[410], CiberVandalismo, secuestro de datos informáticos, Hacktivismo, ciberterrorismo. Aunque hay indicios de que la ley va a cambiar, conforme al convenio de Budapest sobre Ciberdelincuencia, de 23 de noviembre de 2001[411].

Dicho lo anterior, a continuación nos referimos a algunas entidades e instituciones relevantes en materia de lucha contra los delitos informáticos.

Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX

Es un organismo acreditado para atender amenazas de ciberseguridad en México. Atiende denuncias de ataques a los activos tecnológicos de la infraestructura crítica de México, monitorea la seguridad de la red y los sistemas; y coordina la respuesta a incidentes a víctimas de ataques cibernéticos[412].

Ciperpolicía

En el Distrito Federal se creó la policía de ciberdelincuencia preventiva, como una medida para combatir delitos cibernéticos en

---

[410] Una de las primeras referencias al "happy slapping" la encontramos en la Resolución del Parlamento Europeo, de 21 de junio de 2007, sobre "La delincuencia juvenil: el papel de las mujeres, la familia y la sociedad". En su considerando "M", afirma que "en determinados Estados miembros, las inmediaciones e incluso los patios de los colegios, también los de barrios acomodados, se han convertido en zonas fuera de la ley (oferta de droga, violencia en ocasiones con armas blancas, extorsiones varias y desarrollo de juegos peligrosos, por ejemplo, el fenómeno del "happy slapping", consistente en colgar en sitios de internet fotos o vídeos con escenas de violencia captados con teléfonos móviles)". Vid. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0283+0+DOC+XML+V0//ES

[411] Velasco, Cristos en *Tejemaneje: Delitos cibernéticos en México*. 13.05.2014 Video publicado en: http://noticias.terra.com.mx/tejemaneje/videos/tejemaneje-delitos-ciberneticos-en-mexico,7444909.html. El Convenio de Budapest puede consultarse en http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

[412] Espina García, Eduardo, "Centro Nacional de Respuesta a Incidentes Cibernéticos", publicado: http://seguridad2012.politicadigital.com.mx/pdf/03.pdf

México y proporcionar las condiciones de seguridad para el desarrollo integral de la red Internet, es una secretaría técnica la PFP. Como principales líneas de acción, la Policía de Ciberdelincuencia Preventiva realiza monitoreo de redes sociales y sitios web en general; pláticas informativas en centros escolares instituciones del DF; ciberalertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de ciberdelincuencia preventiva[413].

El robo de identidad es el delito más común. Los empleados que se dedican a recolectar datos, han vendido información. Sin embargo, aún hay muchos delitos en cifras negras, debido a la bajísima denuncia en México de éstos delitos[414].

9.2. La ciberseguridad y la ciberdelincuencia.

Para completar la perspectiva de los delitos informáticos debemos hacer una referencia a la ciberseguridad y a la ciberdelincuencia.

La ciberseguridad, siguiendo la definición incluida en la fracción X del artículo segundo del Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal[415], puede ser entendida como:

> *"la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada."*

---

[413] Página de la Secretaría de Seguridad Pública: http://www.ssp.df.gob.mx/Pages/Ciberdelincuencia.aspx

[414] Zamora Piña, Miguel Ángel Tejemaneje: Delitos cibernéticos en México. Video publicado en: http://noticias.terra.com.mx/tejemaneje/videos/tejemaneje-delitos-ciberneticos-en-mexico,7444909.html

[415] Véase el Diario Oficial de la Federación de 6 de septiembre de 2011, disponible en la dirección de Internet http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011

Se trata de una cuestión que afecta a todas las empresas, con independencia de cuál sea su tamaño, así como entidades y dependencias de cualquier Administración Pública, ya que el hecho de estar conectados a Internet implica que todas sean un objetivo potencial de delito informático que puede concretarse, por ejemplo, en el robo de información, sean datos personales o no; la caída del sistema por efecto de un virus o ser víctimas, y quizás de manera inadvertida parte también, de un ataque de denegación de servicios a su vez contra otro.

La ciberdelincuencia es un fenómeno global que requiere de soluciones más allá de las fronteras nacionales. Al ser un fenómeno que supera las fronteras nacionales, la ciberdelincuencia tiene que ser abordada por países y organizaciones internacionales a través de instrumentos de cooperación y combate efectivos, tanto desde un punto de vista de derecho sustantivo como procesal.

Entre las organizaciones internacionales que tratan diversas cuestiones sobre la ciberdelincuencia, es posible indicar que la Unión Internacional de Telecomunicaciones –en adelante, UIT- (en inglés, *International Telecommunication Union*, ITU) ha llevado a cabo diversas iniciativas y acciones con la finalidad de fomentar la cooperación y armonización para combatir de manera efectiva contra la ciberdelincuencia. En particular, la UIT ha desarrollado, en colaboración con ABIresearch, un Índice Mundial de Ciberseguridad (en inglés, Global Cybersecurity Index[416]) que tiene como finalidad medir a nivel nacional el nivel de desarrollo de la ciberseguridad[417].

En su marco conceptual, la UIT menciona que[418]:

“el Secretario General de la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA), el mecanismo de cooperación multipartita internacional creado por la UIT para orientarse hacia

[416] Al que puede accederse a través de la siguiente dirección de Internet http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[417] Sobre el marco conceptual del Índice Global de Ciberseguridad de la ITU, puede verse http://www.itu.int/en/ITU-D/Cybersecurity/Documents/S_GCI_Conceptual%20Framework.pdf

[418] Marco conceptual ya citado. Pág. 2.

una sociedad de la información más segura y protegida, y que se focaliza en los cinco ámbitos de trabajo siguientes:

- *Medidas legales*
- *Medidas técnicas*
- *Medidas orgánicas*
- *Capacitación*
- *Cooperación"*[419]

Además, la UIT firmó, en Mayo de 2011, un acuerdo de cooperación (*Memorandum of Understanding*, MoU) con la Oficina de Drogas y Crimen de Naciones Unidas (*United Nations Office on Drugs and Crime*, UNODC) con la finalidad de colaborar a nivel global para ayudar a los países en la labor de combatir contra la ciberdelincuencia y garantizar un uso seguro de las Tecnologías de la Información y las Comunicaciones (TIC)[420].

Siguiendo con los instrumentos internacionales sobre ciberdelincuencia, México, en el marco de la Conferencia de Ministros de Justicia de los países Iberoamericanos (COMJIB)[421], se ha adherido, con fecha 9 de junio de 2014, al Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia[422] así como a la Recomendación de COMJIB relativa a la tipificación y Sanción de la Ciberdelincuencia[423].

La COMJIB fue creada en 1992 en virtud del Tratado Constitutivo de la Conferencia de Ministros de Justicia de los Países Iberoamericanos ("Tratado de Madrid"), hecho en Madrid el 7 octubre

---

[419] Esta Agenda Global sobre Ciberseguridad puede consultarse en la siguiente dirección electrónica http://www.itu.int/osg/csd/cybersecurity/gca/

[420] En relación a dicho MoU, puede verse más información en la dirección de Internet http://www.itu.int/en/ITU-D/Cybersecurity/Pages/UNODC.aspx

[421] Sobre la COMJIB, puede verse más información en la dirección de Internet http://www.comjib.org/contenido/comjib

[422] La noticia sobre la adhesión de México al referido Convenio puede verse en la dirección de Internet http://www.comjib.org/contenido/mexico-se-adhiere-convenio-iberoamericano-sobre-ciberdelincuencia

[423] Al respecto, puede verse la noticia publicada por la Procuraduría General de la República (PGR) y disponible en la dirección de Internet http://pgr.gob.mx/prensa/2007/bol14/Jun/b11114.shtm

de 1992, y está compuesta por los Ministerios de Justicia e instituciones homólogas de los 21 países de Iberoamérica[424].

También a nivel internacional, y como referente normativo, es necesario prestar atención al Convenio nº 185 del Consejo de Europa sobre la Ciberdelincuencia[425], firmado en Budapest el 23 de noviembre de 2001, y que entró en vigor el 1 de julio de 2004. Además, el Convenio se complementa con un Protocolo Adicional 189 relativo a la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos[426], que fue firmado en Estrasburgo el 28 de enero de 2003 y entró en vigor el 1 de marzo de 2006.

El Convenio del Consejo de Europa sobre la Ciberdelincuencia es el único instrumento internacional vinculante sobre esta materia e incluye estándares, tanto de derecho penal sustantivo y de derecho procesal, que se ven complementados con disposiciones sobre la cooperación internacional.

Como se indica en el Preámbulo del mismo, el *"Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos."*

Es importante tomar en consideración que México no ha firmado este Convenio, si bien está invitado a adherirse desde el 31 de enero del 2007. En relación con su posible adhesión, durante los días 31 de marzo a de 2 abril de 2014 tuvo lugar un "Taller de legislación en materia de ciberdelincuencia en América Latina", co-auspiciado por el

---

[424] El Tratado puede verse en la dirección de Internet http://www.comjib.org/sites/default/files/Tratado%20constitutivo_ES_0.pdf

[425] La traducción en español de este Convenio puede verse en la dirección de Internet http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

[426] En inglés, *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems*, CETS No. 189. Véase http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=07/08/2014&CL=ENG

Gobierno de México y el Consejo de Europa, y en la Memoria de dicho Taller se concluyó que:

> *"• La adhesión del Estado Mexicano al Convenio de Budapest, aunado a la aprobación de las reformas necesarias para actualizar el marco jurídico nacional, permitirán a México colocarse a la vanguardia, a fin de responder a las necesidades de la sociedad y convertirse en un líder en la zona en el combate a la ciberdelincuencia.*
> *• Están dadas las condiciones políticas y jurídicas para que a más tardar el próximo periodo legislativo se aprueben las medidas antes señaladas."*[427]

De esta manera México podría colocarse a la vanguardia pero también, y quizás más importante, actualizar su marco jurídico nacional de manera que pueda ofrecer seguridad y confianza, tanto a las empresas y Administraciones Públicas nacionales, como a los socios comerciales. Y al mismo tiempo avanzar para no quedarse rezagado en esta materia con respecto a los Estados Unidos de América o la Unión Europea[428].

De manera específica por lo que se refiere a las acciones pendientes en México, y que pueden tener un importante impacto para el impulso del cómputo en la nube y el uso de otras tecnologías de la información, *"es necesario tomar en consideración, especialmente, el "Programa para la Seguridad Nacional 2014-2018, Una política multidimensional para México en el siglo XXI". En concreto, el programa dedica un apartado específico a la ciberseguridad en el que*

---

[427] La Memoria del Taller está disponible en la siguiente dirección de Internet: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf

[428] Como ejemplo, en el caso de la Unión Europea, ésta cuenta con una Estrategia de ciberseguridad para un ciberespacio abierto, protegido y seguro, que puede verse, en inglés, en la dirección de Internet http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security Además, actualmente se está tramitando una Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión. La Propuesta de Directiva puede verse en la dirección de Internet http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1407398935517&uri=CELEX:52013PC0048

señala la necesidad de desarrollar una "política de Estado en materia de ciberseguridad" debido a que "quizás la principal vulnerabilidad del país actualmente" es "una acotada cultura de la seguridad de la información"."[429]

9.3. Protección penal de máquinas y servicios de comunicaciones electrónicas

Siguiendo con el Convenio sobre la Ciberdelincuencia, en la Sección 1, relativa al Derecho penal sustantivo, del Capítulo II, sobre Medidas que deberán adoptarse a nivel nacional, incluye disposiciones relativas al acceso ilícito a sistemas informáticos (art. 2)[430] y a la interceptación ilícita de comunicaciones (art. 3)[431].

Las máquinas, conectadas a Internet o a redes de comunicaciones electrónicas, y los servicios de comunicaciones electrónicas, se convierten también en el objetivo de los ataques de ciberdelincuentes ya que ello puede facilitar el acceso a un sistema de información así como a datos, personales o no, u otra información que son valiosos para los mismos.

---

[429] Véase VV.AA.; *La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo*, CIDE 2014, México. Disponible en la siguiente dirección de Internet https://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf

[430] El citado artículo del Convenio, ya mencionado, es como sigue:

> *"**Artículo 2 – Acceso ilícito***
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático."*

[431] El artículo 3, relativo a la interceptación ilícita, dice así:

> *"**Artículo 3 – Interceptación ilícita***
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transpone dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático."*

En el caso de las redes, que son el soporte de los servicios de comunicaciones electrónicas, a nivel internacional cabe señalar como ejemplo el caso de la Unión Europea, que con su Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión[432], busca precisamente proteger las redes de comunicaciones electrónicas y, por lo tanto, los servicios electrónicos.

Al respecto, el considerando 1 de la citada Propuesta de Directiva, indica que: *"Las redes y los sistemas y servicios de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para la actividad económica y el bienestar social."*

En el caso de los equipos, como ya indicamos anteriormente las reformas al Código Penal Federal que entrarán en vigor el 7 de julio del 2014 en el título noveno, capítulo segundo contempla la tipificación del acceso ilícito a sistemas y equipos de informática, el artículo 211 bis 1 incluye referencias expresas a la modificación, destrucción o pérdida de información *"en sistemas o equipos de informática protegidos por algún mecanismo de seguridad"* y el artículo 211 bis 2 incluirá ahora también una referencia a los *"sistemas o equipos de informática del Estado".*

Además de lo anterior, deben ser también objeto de medidas para garantizar su protección los proveedores de servicios que puedan ser considerados como críticos así como las infraestructuras críticas.

Esto supone que las acciones que se lleven a cabo para garantizar la ciberseguridad en México deban tomar en consideración que existen riesgos tecnológicos que incluyen ciberataques, interrupciones en la prestación de servicios e infraestructuras, así como pérdida de datos[433].

---

[432] Ya citada.

[433] Al respecto, puede verse el informe del Foro Económico Mundial titulado *Global Risk Report 2014* en su página 12. Disponible en la dirección de Internet http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

9.4. Otros bienes jurídicos objeto de protección

Con independencia de los bienes jurídicos objeto de protección ya indicados, hay que hacer referencia también a otros bienes, tales como los datos personales y el contenido de las comunicaciones electrónicas.

En el caso de los datos personales, la ya citada Ley Federal de Protección de Datos Personales en Posesión de los Particulares dedica su Capítulo XI a los Delitos en Materia del Tratamiento Indebido de Datos Personales. Sobre esta cuestión, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) ha publicado, en Julio de 2014, como ya hemos puesto de manifiesto en este estudio, una *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[434] que resume los artículos 67 a 69 a través de la siguiente tabla[435], la cual por su interés se cita aquí:

Materia/Cuestión	Acción	Elementos relevantes	Sanción
Medidas de seguridad	El que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a la bases de datos bajo su custodia.	• Ánimo de lucro	De tres meses a tres años de prisión.
Tratamiento de datos personales	Al que, con el fin de alcanzar un lucro indebido, trate datos	• Ánimo de lucro • Engaño	De seis meses a cinco años de prisión.

[434] Disponible en la dirección de Internet http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf

[435] Véase esta tabla en la página 93 del citado documento.

	personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.		
Datos personales sensibles	Las indicadas en los apartados anteriores.	Las indicadas en los apartados anteriores.	Se duplican.

Es así que la protección penal de los datos personales se suma a la protección del derecho fundamental a la protección de datos personales establecida en la LFPDPPP.

Y, por último, otro de los bienes jurídicos a proteger es el relativo al secreto de las comunicaciones, cuestión sobre la que es necesario tener en cuenta que no es objeto de la LFPDPPP, de manera que hay que tomar en consideración el artículo 16 Constitucional cuando dice:

> *"**Las comunicaciones privadas son inviolables**. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*
> *Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales*

de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor." (énfasis añadido).

El secreto de las comunicaciones es un derecho fundamental distinto a la protección de datos personales, de manera que hay que atender a las garantías establecidas en el texto constitucional y en el Código Penal.

En concreto, el artículo 210 del Código Penal Federal[436] tipifica el delito de revelación de secretos en los siguientes términos: *"Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto."*

También debe citarse el artículo 211 Bis, que tipifica la siguiente conducta: *"A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa."*

En conclusión, además de las máquinas o equipos, las redes de comunicaciones electrónicas y los datos personales, hay otros bienes jurídicos, tales como el secreto de las comunicaciones electrónicas, que requieren de una protección específica a la vista del escenario tecnológico que nos rodea, en el que la información y nuestros datos pueden ser objeto de ataques informáticos para hacerse con los mismos. Por tanto, es necesario alcanzar un alto nivel de seguridad cibernética, de manera que México esté alineado a nivel internacional con otros países y regiones, evitando así convertirse en un paraíso que

[436] Ya citado anteriormente.

implique que sus socios comerciales no tengan la confianza necesaria y, al mismo tiempo, suponga perder inversión y oportunidades tales como las que ofrece el cómputo en la nube.

10. Cuestiones contractuales

10.1. Acuerdo de nivel de servicio (SLA) entre el prestador de servicios y el usuario

En la primera parte de este estudio hemos hecho referencia detallada a los Acuerdos de Nivel de Servicio. A ello nos remitimos ahora, sin perjuicio de resaltar alguna otra cuestión en este momento.

El acuerdo de nivel de servicio (en inglés, *Service Level Agreement*, SLA) es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. En los contratos de prestación de servicios informáticos, algunos de los principales puntos a cubrir son:

- El tipo de servicio
- El soporte a clientes y asistencia
- Provisiones para seguridad y datos
- Garantías del sistema y tiempos de respuesta
- Disponibilidad del sistema
- Conectividad
- Multas por caída del sistema[437]

El acuerdo de nivel de servicio puede ser definido también como el *"[a]cuerdo contractual por el cual un proveedor de servicios define el nivel de servicio, las responsabilidades, las prioridades y las garantías con respecto a la disponibilidad, el rendimiento y otros aspectos del servicio"*[438]

[437] SLA, contratos informáticos http://www.contratosinformaticos.com/sla/

[438] Véase esta definición en el estudio del Parlamento Europeo sobre la Computación en Nube, ya citado. Pág. 7.

Un ejemplo de un acuerdo de nivel de servicio de soporte de sitios web entre una dependencia del Estado de México (Instituto de investigación y fomento de las artesanías) y el proveedor siendo la dirección general del sistema estatal de informática, se encuentra en la página de Transparencia del Estado de México[439].

10.2. Garantías legales y contractuales

En el caso del cómputo en la nube, el contrato de nivel de servicio es, como ya sabemos, una cuestión importante a tomar en consideración por los clientes y a la que se presta especial atención ya que define los términos del nivel de servicio[440]. Ya que el cliente, en muy pocos casos, tendrá la posibilidad de negociar las cláusulas de este contrato, es importante que las cláusulas establecidas en el mismo cumpla con el derecho de contratos, de manera que no sean abusivas.

Sobre dichos contratos, en un estudio del Parlamento Europeo sobre Computación en Nube[441], éste ha indicado que:

> *"los contratos son los instrumentos principales por los cuales los proveedores establecen los términos de su relación con los clientes, llamados acuerdos de nivel de servicio (SLA) y acuerdos*

[439] Acuerdo de nivel de servicio de soporte de sitios web entre el Instituto de Investigación y Fomento de las Artesanías del Estado de México, y la Dirección General del Sistema Estatal de Informática, firmado el 18 de enero del 2012, con vigencia del 19 de julio del 2012 al 19 de julio del 2013. Disponible en la página:
http://transparencia.edomex.gob.mx/iifaem/informacion/convenios/Acuerdo%20de%20servicio%20soporte%20sitios%20web.pdf

[440] Por ejemplo, en el caso de la Unión Europea, la Comisión Europea publicó la Comunicación de la Comisión al Parlamento Europeo, al Consejo, la Comité Económico y Social Europeo y al Comité de las Regiones – Liberar el potencial de la computación en la nube en Europa, COM(2012) 529 final, de 27 de septiembre de 2012, en la que se indica que *"La complejidad y la incertidumbre del marco jurídico para los proveedores de servicios en la nube hace que estos recurran con frecuencia a contratos o acuerdos de nivel de servicios de tipo complejo"* por lo que uno de los objetivos de la Unión Europea en su estrategia sobre la nube es elaborar "*las partes interesadas, cláusulas contractuales tipo para los acuerdos de nivel de servicios de computación en nube aplicables a los contratos entre proveedores de servicios en la nube y usuarios profesionales, teniendo en cuenta el acervo de la UE en curso de elaboración en este ámbito."* La Comunicación de la Comisión está disponible en
http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012DC0529&rid=1

[441] Ya citado. Pág. 80.

de licencia de usuario final (EULA). Los términos y condiciones sobre la privacidad aparecen por separado o integrados con el resto. En el caso de los consumidores y las PYME que utilizan nubes públicas, estos contratos son acuerdos estándar de «lo tomas o lo dejas», a menudo con casillas para marcar las opciones y esto no es de sorprender dadas las características de estas nubes y las economías de escala. Un análisis detallado de estos contratos respalda en gran medida las preocupaciones expresadas por las partes interesadas."

Entre los aspectos a tener en cuenta, es importante que el acuerdo de nivel de servicio establezca todas las garantías legales y contractuales necesarias para garantizar al cliente, ya sea éste una organización del sector privado o una entidad del sector público, que los servicios se proporcionarán conforme a altos estándares de calidad, de manera que el proveedor sea sancionado en caso de incumplir con sus obligaciones o tenga fallos en la prestación de servicio, por ejemplo, en caso de fallos en el suministro del servicio o pérdida de datos. Esto supone que dichos acuerdos de nivel de servicio tengan que reflejar de manera adecuada las garantías legales previstas para este tipo de contratos y contemplen expresamente qué responsabilidad podrá ser exigida por el cliente al prestador de servicios de cómputo en la nube.

Además, el acuerdo de nivel de servicio o el contrato entre el proveedor de servicios de cómputo en la nube y el cliente debe incluir también cláusulas relativas a la interoperabilidad y previsiones sobre la finalización del contrato, de manera que si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube, evitando así la situación de falta de reversibilidad o, también, conocida como el usuario no cautivo. Al respecto, el cliente es el propietario de la información que sube a la nube, de manera que el proveedor tiene que garantizarle en todo momento la posibilidad de recuperar dicha información, así como poder obtenerla en un formato que le permita seguir operando.

De lo contrario, el cliente estaría asumiendo un riesgo que le impediría seguir operando su negocio o, en el caso de las Administraciones Públicas, prestar el correspondiente servicio, lo que en la práctica sería un grave problema. Se trata, por lo tanto, de un aspecto a tomar en consideración desde el inicio mismo, a la hora de contratar servicios de cómputo en la nube, en la que el cliente o futuro cliente debe obtener información del proveedor de servicios de cómputo en la nube para evitar incidentes.

Entre las cuestiones a considerar por los prestadores de servicios de cómputo en la nube, el cliente debe atender si al final del contrato, por el motivo que fuese, o incluso en cualquier momento a lo largo de la prestación del servicio, el proveedor le facilita la recuperación de la información, de manera que aquél pueda guardarla o exportarla, y si pone a su disposición herramientas a tal fin o describe o proporciona ayuda para llevar a cabo dicho procedimiento.

En el caso de las Administraciones Públicas, como ya hemos hecho referencia anteriormente, hay normatividad específica que rige la contratación de servicios, entre los que debe entenderse incluido el cómputo en la nube, de manera que es necesario que las licitaciones que tengan como finalidad la contratación de servicios de cómputo en la nube incluyan las previsiones correspondientes con la finalidad de hacer un uso seguro de la nube.

En definitiva, los acuerdos de nivel de servicio pueden llegar a ser una barrera para la adopción del cómputo en la nube, siendo recomendable que la Secretaría de Economía, en el ejercicio de sus competencias, tome esta cuestión en consideración de manera que ayude a los clientes de servicios de cómputo en la nube a que antes de firmar contratos consideren los términos correspondientes y, en su caso, colabore con la industria para facilitar que dichos acuerdos cumplen con las condiciones necesarias, tanto garantías legales como contractuales, para evitar situaciones en las que se pudieran producir incumplimientos de la normatividad mexicana por la situación de prevalencia de los proveedores a la hora de redactar dichos acuerdos.

10.3. Responsabilidad del prestador de servicios

Como ya sabemos, la nueva ley de Telecomunicaciones fue promulgada el 14 de julio del 2014. En ella se establecen ciertas disposiciones a cargo de los concesionarios para colaborar con la justicia. infiere que los prestadores de servicios tendrán las obligaciones descritas en el Título octavo:

Artículo 190.- Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a permitir, que las autoridades facultadas por la ley ejerzan el control y ejecución de la intervención de las comunicaciones privadas y a brindarles el apoyo que éstas les soliciten, de conformidad con las leyes correspondientes.

10.4. Garantías de interoperabilidad, portabilidad de datos y reversibilidad: el usuario no cautivo

Se trata de cuestiones ya tratadas con anterioridad, en particular en el apartado 102., al que nos remitimos en cuanto a lo ya dicho sobre la interoperabilidad y previsiones sobre la finalización del contrato, de manera que si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube, evitando así la situación de falta de reversibilidad o, también, conocida como el usuario no cautivo.

No obstante, podemos ahora resaltar de nuevo que interoperabilidad es definida como las características técnicas de las redes públicas de telecomunicaciones que permiten la interconexión efectiva, por medio de las cuales se asegura la provisión de un servicio de telecomunicaciones específico de una manera consistente y predecible, en términos de la entrega funcional de servicios entre redes[442].

[442] Artículo 3 XXXIII de la nueva Ley Federal de Telecomunicaciones y Radiodifusión, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_140714.pdf

Por ora parte, la nueva Ley de Telecomunicaciones introduce la figura del "usuario visitante" la cual tiene como objetivo favorecer que, a lo largo de todo el país, los ciudadanos, independientemente del concesionario o autorizado de telecomunicaciones móviles que contraten, puedan realizar y recibir llamadas, mensajes y servicios de datos[443].

En cualquier caso, el cliente o futuro cliente de servicios de cómputo en la nube tiene que analizar a la hora de contratar estos servicios qué condiciones y garantías ofrece el prestador de servicios de cómputo en la nube en cuanto a interoperabilidad, portabilidad de datos y reversibilidad.

Si el acuerdo de nivel de servicios, al que ya hemos hecho referencia, o las condiciones de contratación del servicio no dicen nada o no ofrecen suficiente información al respecto, el cliente debe pedir más información y tomarlo en consideración, ya que ello podría ser un riesgo para la continuidad de su negocio.

Se trata también de evitar el riesgo de servicios de cómputo en la nube "incompatibles"[444]

Igualmente, si el cliente no tiene la posibilidad de portar su información, sean datos personales o no, de un prestador de servicios

---

[443] Iniciativa de la Ley Convergente p. 27 y 28, y artículo 3 fracción LXI, publicada en http://www.presidencia.gob.mx/wp-content/uploads/2014/03/INICIATIVA-LEY-CONVERGENTE.pdf

[444] Sobre esta cuestión, por ejemplo, el Parlamento Europeo, en su estudio sobre Computación en Nube, al que ya nos hemos referido, indica que existe:

> *"el riesgo del desarrollo de servicios en nube concentrados e incompatibles. Se produce un rendimiento a escala considerable con la infraestructura en nube y los proveedores predominantes tienen incentivos para levantar barreras que no dejen entrar a nuevos competidores. Como se ha descrito anteriormente, la infraestructura en nube surgió de los sistemas internos existentes de compañías como Amazon, Microsoft y Google, lo cual ha llevado a servicios e interfaces heterogéneos, reduciendo la interoperabilidad y la competencia y creando un riesgo de dependencia de proveedores concretos para los clientes. 123 Como señaló en una presentación Francisco García Morán, director general de la Dirección General de Informática (DIGIT) de la Comisión Europea, «La parte del suministro no está interesada [en las normas], es demasiado pronto: los operadores prefieren ganar cuota de mercado», mientras que «la parte de la demanda está indecisa, las soluciones actuales podrían dar lugar a situaciones de dependencia de proveedores concretos»."* Pág. 83.

de cómputo en la nube a otro, se encontrará con que puede depender únicamente de un prestador de servicios de cómputo en la nube, siendo necesario garantizar la interoperabilidad y portabilidad con la finalidad de que el mercado de servicios de cómputo en la nube ofrezca condiciones de competencia efectiva y no se trate de un monopolio.

Para conseguir garantizar la interoperabilidad y portabilidad, es importante que la estandarización y la interoperabilidad, conceptos a los que ya nos hemos referido, estén garantizados, siendo aspectos relevantes a tener en consideración en los ya mencionados acuerdos de nivel de servicio o, en su caso, condiciones de contratación cuando se trate de servicios a los que se adhiere el cliente[445].

Por lo que se refiere a la reversibilidad, es importante también que el cliente de servicios de cómputo en la nube se asegure de que en todo momento tiene acceso a los datos e información que sube a la nube así como que pueda hacer una copia de seguridad de dicha información, de la que depende la continuidad de su negocio. A tal fin, es importante que examine o evalúe qué ayuda le ofrece el prestador de servicios de cómputo en la nube y las condiciones en las que en todo momento pueda realizar dicha copia de seguridad

En definitiva, la interoperabilidad, la portabilidad y la reversibilidad de los datos o de la información son cuestiones clave para el éxito del cómputo en la nube, debiendo tenerlas en consideración en las condiciones contractuales entre el prestador de servicios de cómputo en la nube y el cliente, así como su supervisión en la práctica por las

---

[445] En el ámbito internacional, esta es una cuestión relevante, habiendo indicado el Parlamento Europeo en su estudio sobre Computación en Nube, ya citado, que:

> *"En la Comunicación de 2008 de la Comisión Europea sobre la Internet del futuro se señalaba que «las interfaces y las normas abiertas crean un círculo virtuoso en el que el mercado crece para todos… los operadores dominantes pueden intentar utilizar normas de su propiedad para mantener cautivos a los consumidores o para exigir derechos de utilización exorbitantes a otros operadores»; mientras que Pilar del Castillo Vera, diputada al Parlamento Europeo, en una conferencia reciente decía que la interoperabilidad y las especificaciones abiertas son esenciales para una nube abierta y competitiva, lo que requiere que «los usuarios puedan acceder o cambiar los servicios en nube con la misma facilidad con la que se cambia de proveedor de telefonía móvil»".* Pág. 83.

autoridades competentes de manera que se genere la confianza necesaria.

10.5. Cuestiones específicas de la contratación de cómputo en la nube en el sector público

Las cuestiones relativas a la contratación de servicios en el sector público, se encuentran en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público[446]. Dicha ley, es reglamentaria del artículo 134 de la Constitución Política de los EUM[447].

Los contratos de prestación de servicios de la nube quedan comprendidos en ésta ley, dado lo dispuesto en el artículo tercero: *"Para los efectos de esta Ley, entre las adquisiciones, arrendamientos y servicios, quedan comprendidos… IX. En general, los servicios de cualquier naturaleza cuya prestación genera una obligación de pago para las dependencias y entidades, salvo que la contratación se encuentre regulada en forma específica por otras disposiciones legales. Corresponderá a la Secretaría de la Función Pública, a solicitud de la dependencia o entidad de que se trate, determinar si un servicio se ubica en la hipótesis de esta fracción."*

El acuerdo que tiene por objeto emitir 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 establecer el manual administrativo de aplicación de dichas materias. A este acuerdo de nos hemos referido ya, haciendo mención

---

[446] Como la muestra la última reforma publicada en el Diario Oficial de la Federación el 16 de enero del 2012, en la página: http://www.diputados.gob.mx/LeyesBiblio/pdf/14.pdf

[447] En el artículo 134 de la Constitución se establece que "…las adquisiciones, arrendamientos y enajenaciones de todo tipo de bienes, prestación de servicios de cualquier naturaleza y la contratación de obra que realicen (la Federación, los Estados, el DF y los órganos político-administrativos en , se adjudicarán o llevarán a cabo a través de licitaciones públicas mediante convocatoria pública para que libremente se presenten proposiciones solventes en sobre cerrado, que será abierto públicamente, a fin de asegurar al Estado las mejores condiciones disponibles en cuanto a precio, calidad, financiamiento, oportunidad y demás circunstancias pertinentes…" Constitución Política de los EUM última reforma publicada el 7 de julio 2014 http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm

específica de la contratación de centros de datos, al desarrollar la Estrategia Digital Nacional, de manera que nos remitimos a lo ya dicho entonces.

No obstante, consideramos conveniente hacer referencia aquí a que en el caso de la contratación de servicios de cómputo en la nube deben tenerse en consideración todos los aspectos a los que nos hemos referido en relación con la interoperabilidad, portabilidad y reversibilidad, así como cuestiones relativas al derecho fundamental a la protección de datos personales y otros aspectos sustantivos que tienen que incluirse en los procedimientos de licitación pública.

Contratar servicios de cómputo en la nube por Administraciones Públicas implica tomar una decisión, de manera que *"en caso de que se recurriera a contratar servicios de centro de datos en lugar de utilizar un centro de datos propio o compartido con otra institución pública; tomar dicha decisión se debe hacer evaluando el beneficio de los siguientes factores conforme a lo que indica la fracción II del citado artículo 13 del Acuerdo: "económico, eficiencia, privacidad, seguridad de los datos y de la información"."*[448]

Es decir, la contratación de servicios de cómputo en la nube, tal y como indica el Acuerdo mencionado, debe hacerse previa evaluación, especialmente, de factores de tipo:

- Económico,
- Eficiencia,
- Privacidad, y
- Seguridad de los datos y de la información.

Además de lo relativo a la contratación de servicios de centro de datos, este Acuerdo también se refiere a la contratación de servicios de correo electrónico o servicios de plataformas de procesamiento de datos, por lo que se convierte en una especie de guía para quienes en

[448] Véase, VV.AA., La nube: nuevos paradigmas de seguridad y privacidad para un entorno innovador y competitivo. Ya citado. Pág. 24.

el sector público van a contratar dichos servicios. E igual que ocurre en el sector privado, es necesario analizar previamente a la contratación de servicios de cómputo en la nube la normatividad aplicable, por ejemplo en el caso del Expediente Clínico Electrónico[449], así como evaluar o analizar los riesgos de subir información, sean datos personales o no, a la nube, para de esta manera identificar riesgos legales y regulatorios para evitar incumplimientos.

Además, en el caso de las Administraciones Públicas, sean del ámbito que sea, federal, estatal o municipal, es necesario garantizar el cumplimiento de sus obligaciones de transparencia en virtud de la normatividad en la materia, a la que nos hemos referido anteriormente al mencionar específicamente la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Esta obligación de transparencia, que implica también garantizar el derecho de acceso a la información pública, requiere de que la información esté disponible y se guarde también con ciertas garantías específicas a las que los sujetos obligados tienen que atender, de manera que nuevamente la interoperabilidad y la portabilidad de los datos se convierten en cuestiones relevantes y específicas a la vez a tener en consideración en el caso de la contratación de servicios de cómputo en la nube por entidades y dependencias.

Por último, en el caso de dicha entidades y dependencias, es necesario que la contratación de servicios de cómputo en la nube se haga con todas las garantías aplicables, debiendo aquéllas evaluar tanto las condiciones del servicio como las prácticas que lleven a cabo los prestadores de servicios de cómputo en la nube con la finalidad de asegurarse de que la información del sector público es tratada de manera adecuada por sujetos privados a los que se confía dicha información. Es decir, se trata de supervisar, en todo momento, que la información sea tratada de manera correcta y de que el prestador de

[449] En particular, véanse la Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico publicada en el Diario Oficial de la Federación de 15 de octubre de 2012 y la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro para la salud. Intercambio de información en salud, publicada en el Diario Oficial de la Federación de 30 de noviembre de 2012.
.

servicios de cómputo en la nube ofrezca las garantías necesarias para evitar situaciones problemáticas en las que, por ejemplo, se pudiera llegar a producir la desaparición de dicho prestador de servicios por quiebra o un uso indebido de la información.

11. Cuestiones de política pública a considerar sobre la computación en la nube

El cómputo en la nube, como servicio electrónico que implica el uso de TIC, se desarrolla tanto en México como en otros países conforme a políticas públicas que deben ser pensadas para el éxito del país, en cuanto a competitividad del sector privado y eficiencia del sector público[450].

---

[450] Al respecto, puede verse VV.AA., La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo. Ya citado. En dicho documento se indica que:

> *"La competitividad del sector económico y la eficiencia del sector gubernamental deben ser uno de los objetivos prioritarios de todas las partes interesadas, ya que México, por su posición geo-política y otros factores relevantes tales como instituciones, políticas públicas, normatividad, debe seguir compitiendo con países y potencias económicas. Al respecto, según el Reporte Global de Competitividad 2012-2013, que con carácter anual elabora el Foro Económico Mundial, México está en el lugar 53, habiéndose producido un avance de cinco posiciones con respecto a 2011-2012. Pero en el mismo Reporte correspondiente a 2013-2014, México ha retrocedido dos posiciones, hasta el lugar 55.*
> *México sigue por detrás de otros países de Latinoamérica, como Chile, que ocupa el puesto 34; Panamá, puesto 40, o Costa Rica, puesto 54, y se pone por delante de Brasil, que ha retrocedido desde el puesto 48 hasta el 56.*
> *Cabe señalar también que en el Reporte Global de Tecnologías de la Información 2014, México aparece en el puesto 79, de un total de 148 países alrededor del mundo. Es así que México queda rezagado con respecto a países como Chile, puesto 35; Panamá, puesto 43; Costa Rica, puesto 53, o Colombia, puesto 63.*
> *El citado reporte indica que después de años de ascenso en el ranking, México ha caído en 2014 un total de 16 puestos. Entre las razones, se apuntan el hecho de que el costo de acceso a la infraestructura TIC permanezca alto y el hecho de que la calidad del sistema educativo siga siendo un reto a la hora de responder a las necesidades de una economía cambiante y cada vez más digital.*
> *Entre los pilares de dicho reporte cabe destacar que México ha avanzado 23 posiciones en Sofisticación Empresarial y 22 posiciones en Innovación. Tomando en consideración estos avances, una rápida adopción del cómputo en la nube puede mejorar todavía más la progresión de México en dichos rankings, sin perjuicio de poner foco en otros pilares que requieren de acciones específicas y que también están relacionadas con el cómputo en la nube, como por ejemplo la Eficiencia en el Mercado Laboral, que puede servir para crear oportunidades para los profesionistas mexicanos e incluso atraer intelecto internacional.*
> *En este sentido, el Reporte Global de Competitividad debe ser una llamada de atención para México, ya que se si se pone foco en Latinoamérica y el Caribe, México aparece como*

Como ya hemos indicado, en México, del 2003 al 2007 PROSOFT, *"ha logrado posicionarse en la percepción internacional como un país con capacidad de desarrollar tecnología y un destino de la subcontratación de servicios de TI. Analistas internacionales del sector consideran que México cuenta a clima general necesario para ser considerado como un lugar potencial para offshore/nearshore de servicios de TI y externalización de procesos de negocio (BPO por las siglas en inglés de business process outsourcing)."*[451]

Pero que el cómputo en la nube sea un éxito, que a su vez permita el desarrollo de una sólida industria de Tecnologías de la Información (TI) en el caso del sector privado, así como la eficiencia del sector público, requiere de políticas públicas claras por las autoridades competentes, entre las que la Secretaría de Economía tiene un claro papel dadas sus funciones.

11.1. (Des)regulación y/o adecuación de la normatividad aplicable

Impulsar el cómputo en la nube en México implica que sea necesario identificar normas que pueden haber quedado obsoletas y ser un obstáculo para el avance tecnológico y, en particular, el cómputo en la nube, así como considerar la necesidad y/o conveniencia de regular o desregular algunos aspectos con la finalidad de conseguir claros objetivos de competitividad para el sector privado y de eficiencia para el sector público.

En cuanto a la regulación, el marco normativo tiene que ser el adecuado para que la industria tecnológica y los servicios electrónicos puedan prestarse en condiciones competitivas y al mismo tiempo en un marco que favorezca la inversión nacional y extranjera. Al respecto,

---

el tercer país entre los 10 países más avanzados en materia de educación superior, preparación tecnológica e innovación.

Unido a lo anterior, es necesario tomar en consideración que el cómputo en la nube puede ser usado tanto por sectores regulados como no regulados, lo que pone de relieve la necesidad de adoptar medidas que sirvan para impulsar la competitividad en todos los sectores y áreas de actividad." Págs. 61 y 62.

[451] Véase Logros del PROSOFT a cinco años de su implementación, disponible en la dirección de Internet http://www.diputados.gob.mx/expo_foro/docs/proyectos/23_PROSOFT.pdf

como hemos señalado ya en nuestro estudio, es necesario que México por ejemplo avance sin dilación con la adhesión al Convenio nº 185 del Consejo de Europa sobre la Ciberdelincuencia y que se adhiera también al Convenio nº 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal.

Regular significa también monitorear de manera constante cambios y avances que se producen fundamentalmente a nivel global como consecuencia del uso de las TIC y que en la práctica pueden, y deben, implicar la necesidad de reformas legislativas y regulatorias Por ejemplo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), a la que también nos hemos referido y a cuyo análisis nos remitimos, fue promulgada en 2010, si bien en apenas los cuatro (4) años que han pasado se han producido importantes avances tecnológicos siendo necesario analizar si la misma está preparada para responder a los retos que se plantean, tales como el avance hacia una economía basada en los datos (*"data-driven economy"*); los cambios de paradigmas[452] en materia de privacidad[453] y seguridad que, entre otros ejemplos, dan y han dado lugar a la revisión de las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales[454], la actualización del Convenio nº 108 del Consejo de Europa, ya citado, así como que por ejemplo la Unión Europea comenzase en 2012 un proceso de revisión de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[455].

---

[452] Por ejemplo, en materia de cómputo en la nube, hemos hecho referencias en varias ocasiones al documento La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo.

[453] Véase, por ejemplo, el documento del World Economic Forum, *Rethinking Personal Data: A New Lens for Strengthening Trust,* de 12 de mayo de 2014 y disponible en http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf

[454] Vénse las OECD Guidelines governing the protection of privacy and transborder flows of personal data, publicadas el 11 de julio de 2013 y disponibles en http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[455] Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:01995L0046-20031120&rid=1

Es decir, al promulgar la LFPDPPP México comenzó un camino, más que finalizarlo, de manera que tiene que seguir de manera continua y constante con el análisis de que su normatividad en la materia responda a los retos que se plantean así como que le permita impulsar sus alianzas estratégicas con sus socios comerciales que, en particular en el caso de la Unión Europea y los Estados Unidos de América, siguen diferentes modelos.

Desregular puede ser una opción a tener en consideración en el caso de materias o cuestiones que pueda ser mejor dejar al mercado o que puedan ser objeto de autorregulación. Y sin perjuicio de lo anterior, por ejemplo impulsar la autorregulación en materia de protección de datos personales, siendo el mínimo el contenido de la LFPDPPP, es fundamental también en el caso de la prestación de servicios electrónicos ya que ello permitirá generar la confianza tanto de usuarios nacionales como extranjeros en productos o servicios hechos en o prestados desde México.

En conclusión, la normatividad aplicable es un factor a tener en cuenta a la hora de diseñar políticas públicas, especialmente por lo que se refiere al cómputo en la nube. Por tanto, es importante identificar y analizar si el marco normativo y regulatorio aplicable al cómputo en la nube, en los diferentes aspectos o cuestiones que se plantean en relación al mismo, tal y como hemos expuesto a lo largo del presente análisis, es el adecuado o si se requieren medidas que pueden consistir, en unos casos, en reformas legislativas ya sea para abrogar o actualizar las normas correspondientes y, en otros casos, impulsar la autorregulación.

11.2. Políticas públicas a considerar

11.2.1. Impulso de las Tecnologías de la Información (TI) en México

Continuar con las medidas para impulsar las Tecnologías de la Información (TI) en México es clave para conseguir que las empresas

puedan ser más competitivas y las Administraciones Públicas más eficientes.

Al impulso de las TI ya nos hemos referido en apartados anteriores, a los que nos remitimos para evitar repetir nuestra exposición, si bien queremos indicar aquí que la adopción de medidas al respecto debe producirse teniendo en consideración la realidad de una economía globalizada e interconectada electrónicamente, de manera que México tiene competidores a nivel internacional que también cuentan con estrategias que deben ser consideradas, en unos casos, como ejemplos de buenas prácticas y, en otros casos, como prácticas o medidas a evitar.

Al respecto, según un reciente informe del Foro Económico Mundial, titulado *Delivering Digital Infraestructure – Advancing the Internet Economy*[456], de Abril de 2014, son necesarias medidas que, básicamente, permitan eliminar barreras a la innovación así como alentar a las partes interesadas a desarrollar modelos de negocio cooperativos para conseguir una mayor utilización de la infraestructura y aumentar la demanda de servicios digitales o electrónicos.

En particular, por lo que se refiere a las TI, siguiendo la tendencia internacional o, más bien, global, se debe buscar la modernización y, en su caso, alinear las políticas públicas de manera que permitan conseguir inversiones[457].

Todo lo anterior unido también a impulsar la conectividad y el uso de las TIC, tal y como tratamos más adelante en el apartado específico sobre esta cuestión.

El impulso a las TI implica también la cooperación del gobierno con otros actores clave, tales como la industria y la academia o Universidad. En este último caso, resulta relevante el hecho de que

[456] El informe puede verse en http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf

[457] Véase el informe citado en la nota a pie de página anterior en su página 5.

recientemente se firmase un acuerdo para el impulso y fortalecimiento de la innovación y desarrollo tecnológico por parte del Congreso de la Unión, el Consejo Consultivo de Ciencia y Tecnología de la Presidencia de la República, instituciones académicas y científicas nacionales y estatales[458]. Es decir, el impulso de las TI pasa también por apoyar la investigación y el desarrollo e innovación (I+D+I), ya que México está rezagado con respecto a otros países como Japón y Corea *"donde el 40 por ciento de los científicos se dedican a proyectos de innovación, mientras que en México sólo 10 por ciento del profesorado hace investigación."*

En definitiva, México debe impulsar las TI a través de medidas y acciones que permitan aumentar el capital de conocimiento, así como el acceso a las TI, de manera que ello permita al país avanzar, tanto a nivel nacional como internacional.

11.2.2. Cuestiones fiscales a considerar

La fiscalidad es también un aspecto a considerar como política pública, ya que una alta fiscalidad aplicada al cómputo en la nube puede significar la pérdida de inversión por la industria así como un desincentivo para los usuarios de los servicios electrónicos correspondientes. Y al mismo tiempo, como tecnología y servicio electrónico, puede ser prestada desde cualquier lugar del mundo, lo que supone que los impuestos aplicables en su caso deban ser considerados a la luz de la realidad global.

Lo anterior implica que tanto por lo que se refiere a las TI en general como al cómputo en la nube en particular, el marco fiscal aplicable deba ser tenido también en consideración de manera que no sea una barrera o desincentivo, sino por el contrario un aspecto que permita atraer inversiones.

---

[458] Véase el Comunicado publicado con fecha 16 de junio de 2014 por el Senado de la República y disponible http://comunicacion.senado.gob.mx/index.php/informacion/boletines/13214-firman-acuerdo-para-el-impulso-y-fortalecimiento-de-la-innovacion-y-desarrollo-tecnologico.html

La fiscalidad de las TI y del cómputo en la nube es un aspecto importante y sensible, ya que si atendemos por ejemplo al caso de la Unión Europea, la Comisión Europea ha indicado que[459]:

> *"La transición a la economía digital plantea igualmente problemas en lo que respecta a la fiscalidad. Tradicionalmente, los beneficios se gravaban en el país en que se realizaban materialmente las actividades, que normalmente coincidía con el lugar de residencia del cliente. Con el paso al comercio en línea, son necesarios nuevas fórmulas para evitar la aparición de lagunas y la necesidad de recurrir al arbitraje."*

Y añade a continuación que:

> *"También es más fácil que las empresas digitales estén en condiciones de aplicar técnicas agresivas de planificación fiscal a disposición de todas las empresas multinacionales. La UE está contribuyendo activamente a la labor de la OCDE sobre la erosión de la base imponible y el traslado de los beneficios (BEPS en sus siglas en inglés) y, en especial, al desarrollo de soluciones para la economía digital."*[460]

Por lo tanto, México debe tener también en consideración las cuestiones fiscales que se plantean en relación a las TI, con especial atención al cómputo en la nube, de manera que además de analizar si se deben adoptar medidas para dar una respuesta efectiva sirva para evitar la pérdida de inversión como consecuencia de impuestos que no respondan a la realidad de la economía digital y que impliquen que los inversionistas decidan poner su atención en otros países antes que en México.

---

[459] Véase Comisión Europea, *El desafío digital de Europa,* Contribución de la Comisión al Consejo Europeo de 24-25 de octubre de 2013, disponible en http://ec.europa.eu/europe2020/pdf/20131010_es.pdf

[460] En relación con las medidas que está adoptando la OCDE para analizar las implicaciones de la erosión de la base imponible y el traslado de los beneficios (en inglés, Base Erosion and Profit Shifting, BEPS) en el caso de negocios basados en la economía digital, pueden verse los resultados de una consulta pública que ha llevado a cabo recientemente y disponibles en http://www.oecd.org/ctp/comments-action-1-tax-challenges-digital-economy.htm

11.2.3. Ancho de banda y otras cuestiones relativas a telecomunicaciones y comunicaciones electrónicas

El ancho de banda, específicamente, ha sido una de las cuestiones a las que ya nos hemos referido a lo largo del estudio y sobre las que México ha adoptado medidas para facilitar la conectividad en todo el país.

Con estas medidas será posible que los mexicanos, incluso en zonas geográficas alejadas, tengan la oportunidad de acceder a la Sociedad de la Información y del Conocimiento y, por lo que se refiere al cómputo en la nube, hacer uso de dichos servicios e, incluso, prestar servicios relacionados con el *cloud*.

En el caso de las empresas y de las Administraciones Públicas la conectividad es fundamental para poder ser competitivas y eficientes, respectivamente, con lo que ello implica también en cuanto al uso del cómputo en la nube.

Si se tienen en consideración los *rankings* internacionales sobre conectividad, en particular el elaborado por el Foro Económico Mundial, en su *Global Information Technology Report,* México ha caído varias posiciones por lo que se refiere a la banda ancha, pasando del puesto 63 al 93 en sólo un año[461]. Y esta caída se produce después de dos años de importantes avances, tal y como indica el informe del Foro Económico Mundial[462]. Esto supone que México se encuentre, a nivel regional, por detrás de países como Chile, Panamá, Costa Rica, Uruguay, Colombia y Brasil.

Cómo avance México en la materia puede depender, en buena medida, de la reforma en materia de telecomunicaciones que, entre otras medidas, se ha concretado en la nueva Ley de

[461] Véase el citado *ranking* en http://www.weforum.org/issues/global-information-technology

[462] Véase el informe, disponible en http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf, en su página 27.

Telecomunicaciones a la que ya hemos referencia de manera que nos remitimos a lo ya tratado con anterioridad.

Además de que México pueda contar con banda ancha en toda la República, para lo cual el Proyecto México Conectado, al que también nos hemos referido, es clave, es necesario facilitar el acceso y el uso de las TIC por los mexicanos, ya que ello también es un factor importante a la hora de conseguir objetivos tales como incrementar el nivel de conocimientos y habilidades de los mexicanos para que puedan tener más oportunidades laborales.

También, las tarifas aplicables a los servicios de telecomunicaciones y comunicaciones electrónicas son un aspecto importante a tener en consideración, ya que por ejemplo, en materia de celulares, según el informe ya ciado del Foro Económico Mundial, el costo por minuto es de 52 céntimos de dólar por minuto, lo que lleva a México a situarse en el puesto 129 del *ranking*[463].

Siguiendo con las cifras proporcionadas por dicho informe, el porcentaje de usuarios de Internet es del 38.4%, lo que lleva a México al puesto 85 del ranking. Y también son relevantes los datos relativos, por una parte, a uso de Internet en relaciones *business-to-business* (B2B), que es del 4.9% e implica que México se sitúe en el puesto 64 del *ranking*, así como en las relaciones *business-to-consumer* (B2C), que es del 4.4% lo que significa que México esté en el puesto 76 del *ranking*.

Lo anterior supone que, si bien conforme a los datos ofrecidos por AMIPCI en su *Estudio sobre los hábitos de los usuarios de internet en México 2014*, presentado durante la celebración del Día de Internet[464], el número de usuarios de Internet crece en 2013 en comparación con 2012, hasta incrementarse en un 13% y llegar a los 51.2 millones de ciudadanos, todavía quedan muchos usuarios por conectarse, de

[463] Véase la página 188 del informe citado en la nota a pie de página anterior.
[464] El pasado 16 de mayo de 2014. El estudio está disponible en https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

manera que impulsar la conectividad y el acceso a Internet es fundamental para México.

En cuanto al uso laboral de la conexión, según los datos de AMIPCI, el hecho de que sólo el 11% se refiera a transacciones de comercio electrónico hace que sea necesario que se reflexione sobre esta cuestión, ya que dicha cifra debería ser más alta.

En definitiva, México ha conseguido logros que requieren de medidas constantes para evitar, precisamente, caídas en *rankings* internacionales, y al mismo tiempo impulsar de manera decidida la conectividad y el acceso al uso de las TIC en el país si quiere ser un referente para otros países y un líder por lo que se refiere al cómputo en la nube, además de otras áreas de la economía digital.

11.2.4. Posibilidades de generar empleo

En cuanto a las posibilidades de generar empleo, nos hemos referido ya tanto al tratar el papel de la Secretaría de Economía y PROSOFT 3.0 como al mencionar, con anterioridad, las oportunidades de negocio que, de manera directa, ofrecer el cómputo en la nube en México.

No obstante, es posible ampliar aquí algunos datos sobre las posibilidades de que el cómputo en la nube genere empleo en particular en México, pudiendo señalar que según la información que maneja Microsoft y que dio a conocer en el marco del Foro de Líderes de Gobierno de América Latina[465], el cómputo en la nube podría suponer un aumento de hasta el 34% en la generación de empleos en toda América Latina[466] durante 2014.

[465] Que tuvo lugar en la Ciudad de México los días 7 y 8 de mayo de 2014.
[466] Puede verse la referencia en una noticia publicada en http://tecno.americaeconomia.com/noticias/generacion-de-empleo-por-la-nube-aumentaria-34-en-latina-este-ano

Según un estudio citado por la Comisión Económica para América Latina (CEPAL)[467] de Naciones Unidas *"entre 2011 y 2014 la nube generará alrededor de 14 millones de trabajos nuevos, de los cuales 700 mil serán en países como Brasil, México, Argentina y Colombia, que se proyectan como los países que más rápido la adoptarán y generarán aplicaciones."*[468]

Más allá de las cifras, la posibilidad de generar empleo relacionado con la nube, pero también con las aplicaciones ("apps"), el Internet de las Cosas o la ciberseguridad, pasa necesariamente por contar con medidas efectivas destinadas a la educación de los jóvenes, que son los futuros profesionistas, así como en su caso una nueva oportunidad para otras personas que ya tienen experiencia laboral y que a lo largo de su vida buscan nuevas oportunidades de trabajo.

Tal y como ha indicado el propio PROSOFT[469], y siendo aplicable al cómputo en la nube actualmente, uno de los retos planteados es *"incrementar la cantidad y calidad humano del sector de TI, a través del desarrollo de competencias y habilidades clave"*, y en concreto uno de los aspectos incluidos dentro de este reto es *"[f]lexibilizar las condiciones de contratación para el primer empleo de recién egresados de la universidad, y de trabajadores de medio tiempo."*

Esto es aplicable también al cómputo en la nube, así como a la economía que puede resultar de, por ejemplo, los tratamientos masivos de datos *("big data")*, el Internet de las Cosas, los vestibles *("wearables")*, las aplicaciones *("apps")* u otras oportunidades en las que México debe considerar competir con otros países y regiones.

---

[467] Para más información sobre CEPAL, véase http://www.cepal.org/

[468] Véase la referencia al estudio de Trend-Micro en http://www.cepal.org/socinfo/noticias/paginas/3/44733/newsletter19.pdf

[469] Véase el documento titulado *Desarrollo del sector de tecnologías de la información en México: retos identificados*, Resultados de las mesas de trabajo del evento "Avances y Retos del Sector de TI en México", celebradas el 12 y 13 de noviembre de 2012 en la Ciudad de México y disponibles en la siguiente dirección de Internet http://www.prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/GREF_10.pdf

De esta manera, el número de empleos generados, que según los datos de PROSOFT[470] en 2007, *"[l]os proyectos fondeados resultaron en la generación de 11,206 empleos en el sector del software y servicios relacionados, así como la mejora de 9,170 empleos a través de certificaciones y capacitaciones"*, podría aumentar, máxime cuando estamos también en un momento en el que la certificación de personas, en cuanto a competencias y conocimientos, es clave.

En el caso de México, según los datos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), cabe resaltar que *"el crecimiento anual de las tasas de graduación a nivel de educación media superior ha sido mayor al de los países de la OCDE, para los que existe información."*[471] No obstante, es importante prestar atención al hecho de que el *"porcentaje de egresados universitarios sigue siendo muy inferior a la media de la OCDE de 39%, los niveles de educación superior entre los jóvenes han aumentado 6 puntos porcentuales entre el año 2000 (17%) y el 2011 (23%); y ya superan a los de Austria (21%), Brasil (13%), Italia (21%) y Turquía (19%)"*. Y también que la realidad es que los jóvenes mexicanos *"tienen hoy niveles educativos más altos, y son sin embargo más vulnerables al desempleo. Cerca del 5.8% de las personas de 25 a 34 años de edad con educación media superior se encuentran desempleados, comparado con el 4% de las personas entre 35 y 44 años con el mismo nivel educativo. Asimismo, el 7.2% de los jóvenes de 25 a 34 años con educación superior están desempleados comparado con el 3.4% de los adultos de 35 a 44 años con una educación similar."*[472]

En definitiva, el cómputo en la nube es una oportunidad tanto presente como futura, ya que gracias al mismo será posible desarrollar oportunidades de negocio y trabajo en áreas como los tratamientos masivos de datos ("big data"), las aplicaciones ("apps") y el Internet de las Cosas, en las que se requieren profesionistas cualificados y que, dándose las condiciones necesarias, pueden competir a nivel global ya

[470] Véase el documento mencionado en la nota a pie anterior. Pág. 69.
[471] Véase el documento *Panorama de la Educación 2013*. Disponible en http://www.oecd.org/edu/Mexico_EAG2013%20Country%20note%20(ESP).pdf.
[472] Documento ya citada en la nota a pie anterior, pág. 7.

que las TIC permiten prestar servicios desde incluso zonas geográficamente alejadas. En cualquier caso, es necesario el despliegue de políticas públicas que se concreten en medidas que tengan en consideración todos los aspectos necesarios para que México pueda estar entre los líderes de la economía digital y, además, en la Sociedad de la Información y del Conocimiento.

12. Posibilidad de que México sea referente para otros países

La adopción de medidas con la finalidad de garantizar un marco adecuado para el desarrollo del cómputo en la nube, las tecnologías de la información y fomentar oportunidades de negocio y empleo, puede llevar al país a ser un referente tanto a nivel regional como internacional.

De hecho México es uno de los países identificados como parte de los MINT (México, Indonesia, Nigeria y Turquía), por contraposición a los BRIC (Brasil, Rusia, India y China)[473], de manera que puede ser uno de los gigantes y líderes económicos en los próximos años.

Unido a lo anterior, las reformas en diversos sectores[474] que México está llevando a cabo, entre ellos los de telecomunicaciones, laboral y educativa, ayudarán a que México tenga la oportunidad de ser un claro referente para otros países, además de crecer como socio comercial tanto con los otros países de Norteamérica (Estados Unidos de América y Canadá) así como con la Unión Europea e incluso en el ámbito de Asia-Pacífico.

Es decir, las reformas que se están llevando a cabo y las políticas públicas, en particular en el ámbito de TI, deben estar alineadas y tener como objetivo común y último impulsar a México de manera que este ascienda posiciones en los rankings internacionales de competitividad, por ejemplo en el The Global Competitiveness Report 2013-2014 del

[473] Al respecto, véase, por ejemplo, la nota de prensa publicada en http://www.bbc.com/news/magazine-25548060

[474] Véase más información sobre dichas reformas en http://reformas.gob.mx/

World Economic Forum[475]. En concreto, en dicho informe se hace referencia a que una de las claves para ser competitivo a nivel internacional está en el hecho de que se apoye la transición hacia una economía de alto valor agregado a través del impulso del uso de las TIC así como la capacidad de innovación, que todavía son bajas[476].

Lo anterior supone que deban adoptarse medidas, que deben ser integrales en el sentido de completar políticas públicas adecuadas a través de programas específicos, considerar las oportunidades de des/regulación adecuada y otros incentivos necesarios, para que los mexicanos tengan la oportunidad de ser líderes de la economía digital y, en particular, de la economía que gira en torno a los datos (*"data-driven economy"*). Al respecto, según un reciente estudio de IDC en relación con los tratamientos masivos de datos (*"big data"*), se estima que la tecnología y los servicios relacionados con aquéllos aumente en virtud de una tasa de crecimiento anual compuesto del 40% hasta 2015 a nivel mundial[477].

Y para que los tratamientos masivos de datos y otros fenómenos sean posibles, tales como el Internet de las Cosas, es necesaria la capacidad tecnológica que proporciona el cómputo en la nube, de manera que México tiene ante sí una clara oportunidad que le lleve a ser un referente para sus socios comerciales y otros países, tanto en Latinoamérica como a nivel global.

12.1. Recomendaciones para la Secretaría de Economía (SE)

A través del ejercicio de sus funciones, la Secretaría de Economía (SE), como autoridad reguladora, desempeña un papel esencial en el impulso del cómputo en la nube y otras tecnologías. Por ello es necesario señalar algunas recomendaciones dirigidas a esta entidad:

---

[475] Véase dicho ranking en http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2013-14.pdf

[476] Véase el informe en la página 38.

[477] Véase la referencia al estudio de IDC y de los datos correspondientes en https://ec.europa.eu/digital-agenda/en/towards-thriving-data-driven-economy

1. Como autoridad competente, el papel de la SE es fundamental a la hora de impulsar la adopción y uso de la computación en la nube, ya que a través de las medidas que adopte y de sus decisiones generará la confianza necesaria entre las partes interesadas que son, por una parte, los clientes de servicios de cómputo en la nube y, por otra parte, los proveedores de servicios de cómputo en la nube.

2. La SE ha apoyado, y debe seguir haciéndolo, el desarrollo de medidas relativas al impulso de las TI en México, entre las que se encuentra el cómputo en la nube. Como parte de las medidas adoptadas y a adoptar en relación con el cómputo en la nube, sería considerable potenciar su labor de información y concientización, especialmente dirigida a los clientes de servicios de cómputo en la nube que sean PYMEs.

3. Como autoridad competente, la SE puede desempeñar también un papel fundamental tanto en materia de protección de datos personales como en otras áreas que tienen implicaciones para el desarrollo de la actividad comerciales, tales como propiedad intelectual, ciberdelitos o aspectos tecnológicos como los principios de neutralidad tecnológica, interoperabilidad, estandarización y portabilidad.

4. En cuanto al cómputo en la nube, la SE como autoridad competente puede adoptar medidas para garantizar que los acuerdos de nivel de servicio (en inglés, *Service Level Agreements*, SLA) cumplan con la normatividad aplicable así como que los clientes que sean PYMEs puedan recibir información sobre el alcance de los mismos que les permitan entender su significado e implicaciones.

5. Como autoridad reguladora, específicamente en protección de datos personales, la SE puede desempeñar un papel relevante tanto en foros nacionales como internacionales por lo que se refiere a las implicaciones que tiene la nube en esta materia. Además, la SE puede actuar en coadyuvancia con el IFAI.

6. En definitiva, la SE, como autoridad competente, es una de las partes interesadas y a través de sus funciones y competencias puede

ayudar a impulsar el despliegue de tecnologías que, como el cómputo en la nube, permitan que el país sea competitivo tanto a nivel nacional como internacional.

IV. CONCLUSIONES

Conforme al análisis que hemos realizado a lo largo de todo el estudio sobre el cómputo en la nube, es posible presentar las siguientes conclusiones:

— Cuestiones generales sobre el cómputo en la nube y su uso en México:

1. El artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares incluye una definición de cómputo en la nube, indicando que: "*se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente".*

2. En cuanto a la nube, cabe señalar que hay cuatro clases de nubes: 1) públicas; 2) privadas; 3) híbridas y 4) comunitarias; cinco categorías de ofertas de servicios de nube: 1) infraestructura como servicio (*Infraestructure as a Service* –IaaS-; 2) plataforma como servicio (*Platform as a Service* –PaaS-; 3) software como servicio (*Software as a Service* –SaaS- y 4) *Business Process as a Service* –BPaaS-), y cinco características esenciales: 1) autoservicio *on-demand* o pago por evento; 2) acceso ubicuo a la red; 3) fondo común de recursos; 4) Rápida elasticidad, y 5) servicio medido.

3. Según el Instituto Mexicano para la Competitividad (IMCO), en 2012 un 26% de las empresas mexicanas ya utilizaban cómputo en la nube[478] y conforme a las respuestas recibidas de la encuesta realizada entre 214 MIPYMEs que fue parte del primer entregable, un 27,1% de éstas están haciendo actualmente uso de la nube, lo que supone que cada vez sean más las que suman a la misma. Además, un 28% no

[478] El IMCO cita dicha cifra en relación con una encuesta realizada por ISACA en su IT Risk/Reward Barometer – Mexico Edition, 2011, en el white paper *"Cómputo en la nube": nuevo detonador para la competitividad de México*. Pág. 27. Disponible en el vínculo electrónico http://imco.org.mx/wp-content/uploads/2012/6/computo_en_la_nube_detonador_de_competitividad_doc.pdf

está haciendo actualmente uso de servicios de cómputo en la nube, pero tiene pensado hacer en el futuro, lo cual determina que el futuro de las MIPYMEs esté en la nube y que sean relativamente pocas las que no están pensando en hacer uso de la misma.

4. Por lo que se refiere a los tipos de nube (pública, privada, híbrida o comunitaria), casi la mitad de las MIPYMEs encuestadas respondió a la encuesta realizada indicando que utiliza servicios estandarizados de nube pública, mientras que un 24,8% han respondió que prefieren hacer uso de una combinación entre servicios de nube pública y privada.

5. Un 39,58% de las empresas que han participado en la encuesta ha señalado que trata datos personales en la nube, mientras que el resto de empresas participantes en la misma han indicado que no lo hacen porque los datos personales solo se manejan en los sistemas en sitio (32,29%); existir riesgos legales (6,25%); o riesgos en materia de medidas de seguridad (7,29%) y de confidencialidad (3,65%).

6. Según las respuestas dadas por las MIPYMEs participantes en la encuesta, a la hora de contratar servicios de cómputo en la nube, los clientes buscan un alto de grado de cumplimiento por los proveedores de servicios de cómputo en la nube, siendo el cumplimiento normativo en materia de protección de datos personales (84,46%) y la seguridad (86,67%) los aspectos más relevantes para ellos. Adicionalmente, las certificaciones obtenidas por los proveedores de servicios de cómputo en la nube (64,21%) son también uno de los principales aspectos que los clientes valoran a la hora de usar la nube.

7. Según BSA | The Software Alliance, que en 2012 publicó su *Global Cloud Computing Scorecard*[479], México es el país de América Latina mejor posicionado para el desarrollo del *Cloud Computing,* por delante de Argentina y Brasil. Al respecto, la importancia del cómputo en la nube es cada vez más notable en el marco de la economía global en que nos movemos y puede representar una oportunidad excepcional

[479] http://cloudscorecard.bsa.org/2012/assets/PDFs/BSA_GlobalCloudScorecard.pdf

para el desarrollo de las empresas mexicanas a nivel nacional e internacional.

8. El uso del cómputo en la nube no está limitado a las empresas, ya que el gran tamaño, la complejidad y la gran expansión de los servicios de tecnología de los gobiernos hace que cada vez recurran más al cómputo en la nube. El uso de la nube en el caso de las Administraciones Públicas aporta que éstas puedan ser más eficientes.

9. La trascendencia de las cuestiones relacionadas con la protección de datos y el cómputo en la nube se ha puesto de manifiesto en el hecho de que ha merecido la atención de los más importantes actores de la protección de datos en México y a nivel internacional. Merece destacar, a título de ejemplo, la referencia expresa que le dedica el artículo 52 del Reglamento de desarrollo de la Ley Federal de Protección de Datos Personales en posesión de los Particulares.

10. La prestación de servicios de *cloud* requiere de la celebración de un contrato entre quien presta el servicio (la empresa de *cloud,* que a efectos de la protección de datos tiene la consideración de encargado) y quien lo demanda (el usuario, que a efectos de la protección de datos, tiene la consideración de responsable). En particular, una de las cuestiones más importantes en materia de contratación de servicios de cómputo en la nube es la de la necesidad de definir con claridad los sujetos participantes en la prestación del servicio.

11. A nivel internacional, países como Estados Unidos, la Unión Europea, Japón o Colombia cuentan ya con estrategias sobre el uso del cómputo en la nube en las que se tratan aspectos tales como el camino a seguir en materia de protección de datos personales y privacidad, estandarización, certificación, acuerdos de nivel de servicio u otras cuestiones relevantes para hacer un uso adecuado de la nube.

— Protección de datos personales y privacidad:

12. El tipo de nube que elija un cliente está relacionado con el hecho de que vaya a tratarse información, sean datos personales o no, que

pueda ser más o menos confidencial, de manera que clasificar la información y atender a su naturaleza es importante a la hora de contratar uno u otro tipo de nube. En particular, cuando se trata de datos personales sensibles, dicha clasificación es necesaria con la finalidad de que el cliente tenga garantías de que el proveedor de servicios de cómputo en la nube la tratará con las medidas de seguridad necesarias y, en su caso, poder tener en consideración si es necesario hacer uso de servicios de nube privada.

13. Cuando los datos almacenados en la nube sean considerados como información no confidencial o no se trate de datos personales sensibles, la opción de la nube pública puede ser la más adecuada por sus características y costo. Esto no quiere decir que los servicios de nube pública no sean seguros, sino que sus características son las más adecuadas para tratar información o datos personales que no estén sujetos a una especial reserva de confidencialidad.

14. Cuando los datos almacenados en la nube sean datos personales sensibles, la nube privada puede ser la opción más adecuada dadas sus características, sin perjuicio de que sea posible encontrar proveedores de servicios de cómputo en la nube que, por las medidas implementadas y las garantías que ofrezca, puedan tener una oferta adecuada de servicios que permita también tratar y almacenar estos datos en la nube pública. En cualquier caso, es necesario analizar con detalle las características y garantías ofrecidas en cada caso por los proveedores de servicios de cómputo en la nube.

15. La posibilidad de hacer uso de servicios de cómputo en la nube conlleva ventajas paras las PYMEs mexicanas, siendo uno de los aspectos relevantes a tener en consideración el hecho de que el acceso y uso de dichos servicios les bride la oportunidad de poder competir con las grandes empresas, que sí tienen los recursos necesarios para adquirir Tecnologías de la Información (TI) de una manera que es prohibitiva para las PYMEs. Esto significa que gracias a la nube, desaparecen algunos diferenciales competitivos que se daban en cuanto a la adquisición y uso de las TI.

16. El uso de la nube puede llevar a las empresas mexicanas a ser prestadores de servicios de TI y a competir a un alto nivel. A su vez, puede contribuir a eficientar el trabajo de las Administraciones Públicas. Al mismo tiempo, la nube es una clara oportunidad para el desarrollo de negocios y generación de empleos, ya que los jóvenes y emprendedores mexicanos que también pueden tener la posibilidad de ofrecer servicios relacionados con la nube.

17. La existencia de políticas públicas que impulsen la adopción de la nube por empresas, especialmente las PYMEs y, en su caso, las Administraciones Públicas, es necesaria para no perder oportunidades de competitividad, especialmente en una economía globalizada que día a día avanza más en la dirección de la prestación de servicios electrónicos y el uso de tecnologías innovadoras. Además, dicha economía se caracteriza, cada vez más, por girar en torno a los datos (en inglés, "*data-driven economy"*)

18. El cómputo en la nube también está relacionado con las aplicaciones ("apps"), los grandes tratamientos de datos ("big data") o el Internet de las Cosas ("Internet of Things"), entre otros avances, lo que se traduce en una oportunidad para jóvenes y emprendedores que debe ser tenida también en consideración.

19. El uso del cómputo en la nube también hace surgir otras oportunidades de negocio, como en el caso de la certificación. En este sentido, además de la certificación en protección de datos personales, la certificación en materia de nube puede ser otra oportunidad, estando además ambas estrechamente relacionados ya que los servicios de nube pueden implicar el tratamiento de datos personales, además de otras cuestiones que pueden ser objeto de certificaciones específicas, tales como la gestión documental, etc..

20. La posibilidad de prestar servicios relacionados con la nube, tanto tecnológicos como jurídicos o en otras áreas, es una realidad que debe ser tomada en consideración con la finalidad de aprovechar los logros alcanzados por México en la materia y seguir siendo competitivo con otras regiones y países alrededor del mundo. Por ejemplo, la nube abre

también posibilidades de ofrecer servicios de seguridad así como publicidad relacionados con la misma. En el caso de la publicidad (en inglés, "cloud advertising"), Gartner estima que entre 2013 y 2016 las empresas, a nivel global, invertirán un total de $310 billones de dólares[480].

21. No obstante, por lo que se refiere a la oferta de los servicios de cómputo en la nube, las empresas que actúan como proveedores deben garantizar que los servicios de cómputo en la nube y la tecnología necesaria para la misma cumplan con las Normas Oficiales Mexicanas aplicables en la materia, así como que la tecnología se desarrolle conforme a dichas normas. A su vez, dichos servicios tienen que estar alienados con las normas internacionales, tales como las normas ISO (*International Organization of Standards*). Lo anterior es una condición necesaria para generar confianza en las PYMEs mexicanas a la hora de hacer uso del cómputo en la nube y debe ser también una garantía que busquen éstas cuando vayan a contratar servicios de cómputo en la nube.

— *Estandarización e interoperabilidad:*

22. La estandarización, como garantía, tiene que ser un aspecto a tomar en consideración en los acuerdos de nivel de servicio, ya que de lo contrario se generarían problemas prácticos para los usuarios de servicios de cómputo en la nube. Se trata así de garantizar la interoperabilidad y la portabilidad, de manera que el cliente de servicios de cómputo en la nube cuente con una oferta real de servicios y pueda cambiar libremente según estime oportuno en cada momento sin encontrarse con problemas que podrían hacerle cautivo, lo que se conoce también como *"vendor lock-in"*.

23. La interoperabilidad es fundamental en el caso del uso de las TIC así como en relación al *cloud computing* y otros servicios tecnológicos, por lo que debe ser un principio rector o que gobierne el desarrollo de políticas públicas en relación con el cómputo en la nube y, al mismo

[480] Véase la cifra, según Gartner, en http://www.gartner.com/newsroom/id/2352816

tiempo, ser una garantía para los clientes de dichos servicios. Este principio de interoperabilidad debe aplicarse en conexión con otros principios clave, tales como el de neutralidad tecnológica.

24. Es importante que los servicios y la información sean interoperables para que los clientes no se vean cautivos de ningún prestador de servicios de cómputo en la nube. Como ya hemos dicho, es importante garantizar la portabilidad de la información, sean datos personales o no, ya que de ello depende en buena medida que se genere la confianza necesaria para los clientes de servicios de cómputo en la nube. Se trata, por tanto, de una garantía que debe darse en los servicios de cómputo en la nube y sobre las que las autoridades competentes pueden ayudar a través de medidas que sirvan para garantizar que, especialmente, las PYMEs queden protegidas al carecer de una capacidad de negociación que sólo tienen las grandes empresas y las multinacionales a la hora de contratar servicios.

— *Riesgos legales y regulatorios:*

25. Los riesgos legales y regulatorios pueden ir más allá de la protección de datos personales, de manera que es necesario que los clientes o potenciales clientes, ya sean estos PYMEs o entidades o dependencias de las Administraciones Públicas, adopten medidas para identificar dichos riesgos previamente a la contratación de servicios de cómputo en la nube o, en su caso, otras soluciones tecnológicas, de manera que se aseguren que la contratación se hace con todas las garantías y que se han evaluado los riesgos existentes en cada caso. Contar con herramientas como guías, *checklists* o cuestionarios así como con información al respecto es también importante a la hora de generar confianza en la contratación y prestación de dichos servicios.

26. El análisis de riesgos legales y regulatorios es fundamental para poder adoptar medidas tanto preventivas como correctivas y de gestión de dicho riesgo para minimizarlos. Estos análisis deben hacerse en una fase inicial, preferiblemente antes de contratar un servicio y deben tener continuidad a lo largo de todo el período de prestación del servicio y del tratamiento de datos personales por el cliente, como

responsable del tratamiento, o para el cumplimiento de la normatividad aplicable a su actividad y al cumplimiento de sus obligaciones, por ejemplo, en cuanto a la conservación de documentos con los fines que corresponda en cada caso.

27. El responsable del tratamiento de datos personales está obligado a velar porque los datos sean tratados cumpliendo con los principios previstos en la normativa y, en particular, observando la expectativa razonable de privacidad y prohibiendo la obtención de datos personales por medios engañosos o fraudulentos. Esto es importante en el caso del cliente de servicios de cómputo en la nube, ya que como responsable del tratamiento tiene que adoptar las medidas necesarias para garantizar el cumplimiento de la normatividad aplicable y en particular de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento.

28. En el caso del uso de servicios de cómputo en la nube, el tratamiento de datos personales que el cliente, como responsable, encomienda al proveedor de servicios de cómputo en la nube, como encargado del tratamiento, no requiere del consentimiento del titular de dichos datos, ya que se trata de un acceso para prestar un servicio al responsable, y por tanto considerado como una remisión de datos personales.. No obstante, las condiciones o cláusulas aplicables al servicio de cómputo en la nube tienen que *"estar acordes con el aviso de privacidad correspondiente"*, tal y como indica el último párrafo del artículo 50 del Reglamento de la LFPDPPP.

29. En el caso de que hubiera una transferencia de datos personales entre el cliente y el prestador de servicios, se puede requerir del consentimiento del titular de los datos personales, salvo que concurra alguna de las excepciones previstas en el artículo 37 de la LFPDPPP. En dicho caso, ya no se trataría de una relación contractual entre un responsable y un encargado del tratamiento, sino entre dos responsables del tratamiento.

30. Los responsables del tratamiento de datos personales se encuentran obligados a informar, a través del aviso de privacidad, a los

titulares de los dichos datos, las características principales del tratamiento al que será sometida dicha información personal.

31. Como ya hemos indicado con anterioridad, los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales deberán estar acordes con el aviso de privacidad correspondiente. Al respecto, es importante que el cliente de servicios de cómputo en la nube se asegure en todo momento de que el encargado del tratamiento trata los datos únicamente para la finalidad o finalidades previstas, es decir, la prestación del servicio correspondiente, ya que de otra manera ambos podrían incurrir en un incumplimiento de la LFPDPPP, pudiendo llegar a ser sancionados ambos.

32. Los responsables del tratamiento de datos personales están obligados a asegurarse de que la información recogida resulta exacta y actualizada, así a adoptar las medidas razonables para que dicha información responda a esa veracidad mientras persiste en su tratamiento. Por lo tanto, los clientes de servicios de cómputo en la nube tienen que adoptar medidas para asegurar el cumplimiento de dicha obligación y velar también porque el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, cumpla también.

33. El tratamiento de los datos personales por el responsable únicamente puede ser llevado a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del responsable. La posibilidad de proceder a este tratamiento para otros fines se limita únicamente para los casos que no sean incompatibles con los que motivaron el tratamiento inicial del dato.

34. La finalidad o finalidades del tratamiento de datos personales debe ser determinadas, es decir, debe especificarse para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

35. El responsable del tratamiento de datos personales debe impedir la creación de bases de datos que contengan datos personales sensibles,

salvo que esta acción se justifique atendiendo a su finalidad y que ésta sea legítima, concreta y acorde con las actividades o fines explícitos que procura el sujeto regulado.

36. El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. Es así que el responsable del tratamiento tiene que adoptar medidas para cumplir con este principio y obligación, de manera que se garantice que los datos personales no son tratados ilícitamente.

37. El responsable está obligado a velar y responder por el tratamiento de los datos personales que estén bajo su custodia o posesión o que sean tratados por un encargado al que los haya remitido. Por lo tanto, es necesario que el cliente que contrata servicios de cómputo en la nube, como responsable del tratamiento, se asegure de que el proveedor de servicios de cómputo en la nube, como encargado del tratamiento, ofrece garantías para el cumplimiento de la normatividad sobre protección de datos personales.

38. El cliente debe adoptar las medidas necesarias para identificar riesgos en materia de protección de datos personales, medidas para minimizar dichos riesgos y, a su vez, medidas para velar porque el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumple con sus obligaciones.

39. El cliente tendrá que verificar que el encargado del tratamiento de datos personales cumple con sus obligaciones a través de supervisores, auditores o certificadores. Las certificaciones emitidas por terceros pueden ser un instrumento adecuado para llevar a cabo dicha verificación. En este sentido la autorregulación puede jugar también un papel fundamental en el caso de prestación de servicios de cómputo en la nube.

40. Ya que, con carácter general, se considera al cliente como responsable del tratamiento y al proveedor de servicios de cómputo en la nube como encargado del tratamiento, es importante que ambos

conozcan la normatividad sobre protección de datos personales cuando contraten y ofrezcan, respectivamente, servicios de cómputo en la nube, ya que ello determinará las obligaciones que les corresponden a uno y a otro así como, en su caso, la responsabilidad aplicable en caso de infracción.

41. El establecimiento del responsable del tratamiento en México determina que las disposiciones de protección de datos que se refieren al encargado del tratamiento, sean aplicables al prestador de servicios de cómputo en la nube con independencia del país en el que se encuentre situado éste.

42. La Secretaría de Economía, como autoridad reguladora, puede desempeñar un papel importante a la hora de impedir que los proveedores de servicios incluyan cláusulas que lleven a los clientes a renunciar a las leyes o a la jurisdicción mexicanas en materia de protección de datos personales. Se trata así de ayudar a las PYMEs que contratan dichos servicios y generar la confianza necesaria para todas las partes implicadas.

43. La subcontratación de servicios de cómputo en la nube es posible siempre que el encargado del tratamiento de datos personales cuente con la autorización del responsable y que dicha subcontratación sea formalizada a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. Al respecto, es importante que los clientes de servicios de cómputo en la nube se informen antes de contratar con un proveedor sobre su cadena de subcontratación, de manera que este último tiene que ser transparente.

44. Los datos personales que se encuentren en la nube deben ser resguardados de tal forma que los derechos de acceso, rectificación, cancelación y oposición (también conocidos como derechos ARCO) puedan ejercitarse sin dilación alguna. El responsable del tratamiento debe garantizar lo interior, incluso cuando los datos personales estén siendo tratados por el proveedor de servicios de cómputo en la nube.

45. Los derechos ARCO se ejercerán ante el responsable por el titular o su representante, legal o voluntario. Al respecto, es importante que los clientes de servicios de cómputo en la nube adopten medidas para garantizar el ejercicio de dichos derechos, incluso cuando los datos personales estén siendo tratados por el proveedor de servicios de cómputo en la nube, que actuará como encargado del tratamiento.

— Autoridades competentes (el IFAIPD y la SE):

46. En protección de datos personales, la condición de autoridad garante la tiene el Instituto Federal de Acceso a la Información y Protección de Datos (citado como IFAIPD), siendo la Secretaría de Economía una de las autoridades reguladoras previstas en la materia. Y al respecto, ambas autoridades, en el ejercicio de sus respectivas funciones, tienen la oportunidad de cooperar con la finalidad de generar confianza en la prestación y contratación de servicios de cómputo en la nube.

47. El IFAIPD tiene atribuidas funciones informativas, normativas, de verificación, resolutorias y sancionadoras que deben ser tomadas en consideración, especialmente por lo que se refiere a la emisión de Lineamientos sobre cómputo en la nube.

48. La Secretaría de Economía (en adelante, SE) puede y debe desempeñar un papel fundamental tanto a nivel nacional como internacional en relación con el cómputo en la nube, promoviendo buenas prácticas y un marco regulador adecuado para garantizar el derecho fundamental a la protección de datos personales. Además, resulta claro que las funciones de la SE y el papel que está desempeñe en relación con el impulso del cómputo en la nube son clave por lo que se refiere a la economía que gira en torno a los datos (en inglés, *"data-driven economy"*) en México.

— Solicitudes de acceso por autoridades competentes:

49. Una cuestión específica a tener en consideración en relación con los servicios de cómputo en la nube es el hecho de que las autoridades

gubernamentales y judiciales pueden tener acceso a los datos personales, siendo necesario que el mismo se produzca con las garantías necesarias, de manera que se haga conforme a resolución de autoridad competente en ese sentido (administrativa, gubernamental o judicial) y que dicha resolución cumpla con los requisitos necesarios.

50. Igualmente, cuando la solicitud de acceso a los datos personales sea hecha por la autoridad de otro país, ésta debe producirse con todas las garantías jurídicas, legales y procesales aplicables al caso. Por lo tanto, la SE puede tener un papel importante al respecto al proporcionar información a las PYMEs y atender a las cuestiones que puedan plantearse con respecto a los proveedores de servicios de cómputo en la nube cuando éstos tengan que responder dichas solicitudes de acceso.

51. Cuando las autoridades gubernamentales y judiciales tengan acceso a los datos personales de los clientes, los proveedores de servicios de computación en la nube deben comunicarlo a los mismos , salvo que exista una obligación de mantener en secreto la solicitud de las autoridades.

52. Las autoridades deben adoptar medidas para que los proveedores de servicios de cómputo en la nube no se vean sujetos a situaciones en las que tengan que permitir el acceso a autoridades de otros países sin contar con un procedimiento administrativo o procesal que se lleve a cabo a través de las autoridades implicadas. Es decir, al velar porque se cumpla con las garantías necesarias se estará impulsando la confianza tanto de clientes de servicios de cómputo en la nube como de proveedores de los mismos.

53. Las transferencias internacionales de datos pueden provocar que cuestiones comerciales y de seguridad nacional entren en conflicto, por lo que la Secretaría de Economía debe adoptar medidas que permitan proteger a los usuarios y a los proveedores de servicios de cómputo en la nube y velar para que las solicitudes cumplan con las garantías procesales oportunas.

54. El proveedor de servicios de cómputo en la nube debe aplicar políticas de protección de datos personales afines a los principios y deberes que establecen las normas en la materia; transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio; y guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

55. El proveedor de servicios en la nube debe contar con mecanismos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos; e impedir el acceso a los datos 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.

— *Propiedad intelectual:*

56. Para un adecuado desarrollo del cómputo en la nube se requiere que el país cuente con normas claras y eficientes en materia de derechos de autor y de propiedad industrial. De lo contrario, se desincentivarían las inversiones por parte de los desarrolladores tanto de software necesario para el cómputo en la nube, como de aplicaciones (“apps”) u otras creaciones intelectuales.

57. Para tener un adecuado desarrollo del cómputo en la nube, las autoridades competentes deben establecer medidas efectivas e integrales (legislativas, procesales, educativas, etc.) para combatir la piratería así como impulsar el mantenimiento de aquéllas que ya se hayan implementado.

58. Junto con el impulso del cómputo en la nube, es importante que las políticas públicas favorezcan y estén dirigidas a atraer inversión de desarrolladores de software y aplicaciones de manera que México pueda ser competitivo y, al mismo tiempo, tener la oportunidad de convertirse en un líder regional e internacional en la prestación de servicios electrónicos y la industria de TI. Es decir, el cómputo en la nube es parte de una oportunidad que impulse definitivamente el desarrollo de aplicaciones, el tratamiento de datos masivos de datos personales y otros aspectos relacionados con la economía digital basada en los datos.

59. Reforzar el marco de protección de la propiedad intelectual e industrial, de manera que ello permita que los jóvenes y emprendedores estén protegidos y sea posible la inversión de otros países y de la industria, es clave en relación con el impulso de las TI y el papel de la SE al respecto es importante como autoridad competente que puede cooperar también con otras autoridades, tales como INDAUTOR o el IMPI.

60. Por lo que se refiere a obras y otras creaciones intelectuales, entre las que se encuentra el software, únicamente el titular de los derechos puede otorgar licencias de uso de software exclusivas o no exclusivas. Dichas licencias deben celebrarse por escrito y es importante que las PYMEs estén concientizadas también en cuanto al uso y respeto de la propiedad intelectual, evitando así incurrir en infracciones que puedan ser sancionadas.

61. En materia de licencias de software, tanto en el caso de empresas como de entidades y dependencias de las Administraciones Públicas, se puede tomar como guía sobre esta cuestión la norma internacional ISO/IEC 19770 sobre gestión de activos de software (en inglés, *Software Asset Management*, SAM).

62. También en materia de licencias de software, es posible que las empresas y las entidades y dependencias de la Administración Pública obtengan la certificación correspondiente en materia de SAM, lo que

puede ayudarles a reducir riesgos legales y asegurar el cumplimiento de la normatividad.

— Firma electrónica:

63. En México, la firma electrónica ha seguido un camino diferente, desde el punto de vista normativo, por lo que se refiere al sector privado y al público. Respecto al primero, el uso de la firma electrónica fue regulado en virtud del Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica, además de otra normatividad que desarrolla algunos aspectos de dicho Decreto.

64. En el caso del sector público, a nivel federal, la normatividad básica en la materia se encuentra en la Ley de Firma Electrónica Avanzada (LFEA) y su Reglamento. A su vez, en este sector deben tomarse en consideración las normas publicadas por los diferentes órganos que tiene competencia en la materia, tales como el Servicio de Administración Tributaria (SAT), el Instituto Federal Electoral (IFE) o la Suprema Corte de Justicia de la Nación (SCJN).

65. Los documentos electrónicos y los mensajes de datos que cuenten con firma electrónica avanzada producirán los mismos efectos que los presentados con firma autógrafa y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables a éstos. Igualmente, dicha firma electrónica avanzada, que cumpla con los requisitos establecidos en la LFEA, tendrá la misma validez jurídica y efectos que una firma manuscrita. El uso de la firma electrónica y de la criptografía debe tenerse en consideración en el caso de los servicios de cómputo en la nube, ya que permite proporcionar garantías jurídicas al igual que se requieren en el caso del papel y la firma autógrafa.

66. La nube constituye una ventaja competitiva para las organizaciones y entidades que traten con documentos electrónicos o mensajes de datos, ya que supone la posibilidad de almacenar y procesar ingentes cantidades de información a un costo muy bajo. Además, permite

acceder desde cualquier lugar y en cualquier momento a los datos y la información, con lo que facilita la movilidad de los usuarios.

— *Ciberdelincuencia:*

67. Los delitos informáticos son las actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (en donde la informática es el medio o instrumento para realizar el delito), o bien tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos *per se*). La ciberdelincuencia es una cuestión que requiere de la adopción de medidas con la finalidad de garantizar el uso del cómputo en la nube y la prestación de servicios, ya que de otra manera las partes interesadas, tanto clientes como proveedores de servicios, podrían ver en un alto índice de ciberdelincuencia un obstáculo.

68. El Código Penal Federal, actualmente, sólo ampara sistemas informáticos protegidos por “mecanismos de seguridad”. Además no define qué se entiende por un “mecanismo de seguridad”.

69. Lo anterior implica que se deba tener en consideración la oportunidad de adherirse al Convenio nº 185 del Consejo de Europa sobre la Ciberdelincuencia, de manera se lleven a cabo reformas legislativas que puedan ser necesarias y lo que, sin duda, apoyará la generación de confianza para las partes interesadas al contar México con un marco normativo robusto en la materia. Proteger los negocios y los servicios electrónicos frente a los ciberataques es también importante para atraer inversión.

70. La ciberdelincuencia es una cuestión que afecta a todas las empresas, entidades y dependencias de la Administración Pública, con independencia de cuál sea su tamaño, ya que el hecho de estar conectados a Internet implica que todas sean un objetivo potencial de delito informático. Es necesario también ofrecer a las empresas y otros sujetos información al respecto, de manera que no estén desprevenidos frente a la amenaza que supone la ciberdelincuencia y

adopten medidas para proteger sus activos, ya sean datos personales u otra información, que son críticos para el desarrollo de su actividad.

71. La ciberdelincuencia es un fenómeno que supera las fronteras nacionales, por lo que tiene que ser abordada por países y organizaciones internacionales a través de instrumentos de cooperación y combate efectivos, tanto desde un punto de vista de derecho sustantivo como procesal. Al respecto, es importante que México participe activamente en foros internacionales y considere la adhesión a Tratados o Convenios internacionales, así como que la SE, en el desempeño de sus funciones, apoye dichos procesos para proteger tanto a los clientes como a los proveedores de servicios de cómputo en la nube.

72. Resulta claro que pese a los avances que se han producido durante los últimos años, México requiere actualizar su marco jurídico en materia de ciberdelincuencia, de manera que pueda ofrecer seguridad y confianza tanto a las empresas y Administraciones Públicas nacionales, como a los socios comerciales, lo cual es importante para impulsar el despegue del cómputo en la nube en el país y tener así una clara oportunidad de competitividad a nivel internacional.

73. A la hora de desplegar acciones para garantizar la ciberseguridad, se deben tomar en consideración que existen riesgos tecnológicos que incluyen ciberataques, interrupciones en la prestación de servicios e infraestructuras, así como pérdida de datos. Es, por tanto, necesario que los clientes de servicios de cómputo en la nube y de otras tecnologías, especialmente cuando se trata de PYMEs, estén concientizadas sobre dichos riesgos.

74. Hay otros bienes jurídicos, tales como el secreto de las comunicaciones electrónicas, que requieren de una protección específica, ya que los correspondientes servicios de comunicaciones pueden ser objeto de ataques informáticos para hacerse con los mismos. Y el contenido de las comunicaciones electrónicas, en el caso de las organizaciones, pueden ser también secretos comerciales o creaciones objeto de protección mediante derechos de propiedad

intelectual, que en manos de terceros no autorizados pueden suponer la quiebra de un negocio. También en el caso de dependencias y entidades de las Administraciones Públicas, puede tratarse de información reservada o confidencial, la cual es necesario proteger.

75. Tomando en consideración lo anterior, es necesario alcanzar un alto nivel de seguridad cibernética, de manera que México esté alineado a nivel internacional con otros países y regiones, evitando así convertirse en un paraíso que implique que sus socios comerciales no tengan la confianza necesaria y, al mismo tiempo, suponga perder inversión y oportunidades tales como las que ofrece el cómputo en la nube.

— *Acuerdo de nivel de servicio (Service Level Agreement, SLA):*

76. El acuerdo de nivel de servicio (en inglés, *Service Level Agreement*, SLA) es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. En el caso del cómputo en la nube es importante que dicho acuerdo establezca cláusulas legales y contractuales que garanticen al cliente que los servicios se proporcionarán conforme a altos estándares de calidad, de manera que el proveedor sea sancionado en caso de incumplir con sus obligaciones o tenga fallos en la prestación de servicio. No obstante, es necesario tener en consideración que la realidad es que las PYMEs carecen de la posibilidad de negociar dichas cláusulas y que pueden necesitar información para entender los términos de las mismas.

77. El acuerdo de nivel de servicio debe incluir también cláusulas relativas a la interoperabilidad y previsiones sobre la finalización del contrato, de manera que si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube, evitando así la situación de falta de reversibilidad o, también, conocida como el usuario no cautivo.

78. En el caso de las Administraciones Públicas, es necesario que las licitaciones que tengan como finalidad la contratación de servicios de

cómputo en la nube incluyan previsiones sobre interoperabilidad y finalización del contrato, correspondientes con la finalidad de hacer un uso seguro de la nube.

79. Los acuerdos de nivel de servicio mal redactados o que no cumplan con las condiciones legales y contractuales necesarias pueden llegar a ser una barrera para la adopción del cómputo en la nube, por lo que la Secretaría de Economía, en el ámbito de sus competencias, puede desempeñar una importante labor al proporcionar información a los clientes de dichos servicios así como verificar el cumplimiento de la normatividad para que dichos acuerdos cumplan con la garantías legales y contractuales.

80. La interoperabilidad, la portabilidad y la reversibilidad de los datos o de la información son cuestiones clave para el éxito del cómputo en la nube, debiendo tenerlas en consideración en las condiciones contractuales entre el prestador de servicios de cómputo en la nube y el cliente, así como su supervisión en la práctica por las autoridades competentes.

81. En el caso de entidades y dependencias de la administración pública, es necesario que la contratación de servicios de cómputo en la nube se haga con todas las garantías aplicables, debiendo aquéllas evaluar tanto las condiciones del servicio como las prácticas que lleven a cabo los prestadores de servicios de cómputo en la nube, con la finalidad de asegurarse de que la información del sector público es tratada de manera adecuada por sujetos privados a los que se confía dicha información.

— La nube como oportunidad para México:

82. La nube es una clara oportunidad para México, siendo las PYMEs las principales beneficiarias en cuanto al uso de tecnología y servicios que les pueden permitir competir incluso a nivel internacional así como a ser más eficientes a las Administraciones Públicas. Que lo anterior sea posible requiere de la cooperación de las autoridades competentes para impulsar la confianza necesaria en dichos servicios y supervisar

que se cumple con la normatividad aplicable, la cual puede requerir, en su caso, adecuaciones en el sentido de tomar en consideración qué debe dejarse en manos de la autorregulación, y si son necesarias reformas legislativas para adecuar normas obsoletas o para adecuar las ya existentes a las exigencias de la realidad.

83. El papel de la SE es fundamental en el impulso del cómputo en la nube y a través de éste de la economía que gira en torno a los datos *("data-driven economy")*, ya que la nube puede ser clave para el desarrollo de una economía en torno a aplicaciones *("apps")*, grandes tratamientos de datos personales *("big data")* o el Internet de las Cosas *("Internet of Things")*, de manera que también las PYMEs pueden beneficiarse de estas oportunidades al poder tener acceso a tecnología que les permita competir tanto a nivel nacional como internacional.

84. En definitiva, la nube debe ser tomada en consideración como una cuestión respecto a la que la responsabilidad es compartida entre clientes de servicios de cómputo en la nube, que tienen que analizar los riesgos legales y regulatorios al igual que en cualquier otro ámbito de su actividad; los proveedores de servicios de cómputo en la nube, que deben cumplir con altos estándares contractuales y regulatorios a la hora de proporcionar sus servicios, con independencia de dónde estén establecidos, y las autoridades competentes, que son quienes tienen que apoyar el desarrollo de marcos adecuados para hacer posible que México pueda llegar a ser un líder regional e internacional, además de un destino para inversores internacionales.

V. GUÍA PRÁCTICA EN MATERIA DE ADOPCIÓN DE SERVICIOS DE CÓMPUTO EN LA NUBE PARA EMPRESAS

1. Implicaciones de la contratación de servicios en la nube (cloud computing), sobre todo en lo relativo a protección de datos personales y seguridad de la información

A lo largo del estudio se ha hecho referencia en varias ocasiones a que la protección de datos personales y la seguridad de la información son fundamentales, tanto por lo que se refiere al uso del cómputo en la nube como de otras tecnologías, de manera que es uno de los aspectos torales sobre los que es necesario mantener la concientización por parte de la Secretaría de Economía, ya que ello redunda en la garantía del derecho a la protección de datos personales.

Sin repetir lo ya dicho a lo largo del estudio, la encuesta inicial a más de 200 empresas que participaron en la misma y los pilotos que se han llevado a cabo, permiten confirmar que la protección de datos personales y la seguridad es una de las principales cuestiones que se plantean para las organizaciones a la hora de adoptar la nube, de manera que es necesario despejar las dudas que se plantean a la vez que se adoptan medidas para fomentar un alto grado de cumplimiento en la materia y otras áreas del Derecho de las TIC con la finalidad de que México sea visto como un país competitivo y un marco regulador y autorregulatorio efectivo que permita atraer inversiones.

Por lo tanto, es necesario que las autoridades competentes, entre ellas la Secretaría de Economía con un papel fundamental en esta materia, adopten medidas que sirvan para que tanto los responsables como los encargados del tratamiento, hagan uso o no del cómputo en la nube o de otras tecnologías, cumplan con la normatividad que les es aplicable ya que es clave para el desarrollo de productos o servicios competitivos, especialmente cuando éstos cumple con un alto grado de protección de datos personales y seguridad como consecuencia de las

medidas implementadas por quienes están obligados a ello. Y al respecto, poder contar por ejemplo con una guía sobre cómputo en la nube, puede marcar una clara diferencia a la hora de cumplir, ya que las organizaciones pueden contar en su caso con un documento o instrumento de referencia.

2. Potenciales oportunidades de negocio que el *cloud computing* ofrece para las organizaciones

Como hemos señalado a lo largo del estudio y destacamos de nuevo aquí por su importancia, el cómputo en la nube es una clara oportunidad para México ya que profesionistas y organizaciones tienen la oportunidad de hacer uso de, y al mismo tiempo ofrecer en su caso, una tecnología y de servicios tecnológicos que son necesarios para poder desarrollar aplicaciones *("apps")*, realizar tratamientos masivos de datos *("big data")* o aprovechar las posibilidades que brinda el Internet de las Cosas *("Internet of Things")*.

El cómputo en la nube ofrece también a emprendedores y organizaciones oportunidades de negocio que, en su caso, requieren de un claro impulso por las autoridades competentes de manera que ello permitirá que México pueda convertirse en uno de los actores principales de la economía digital y exporte tecnología y servicios tecnológicos a otros países.

Con relación al cómputo en la nube y específicamente por lo que se refiere a las oportunidades de negocio, es posible indicar, entre otras, las siguientes:

- ***Cloud computing* y publicidad:** Una de las oportunidades relacionada con el cómputo en la nube es la relativa a la publicidad. Citando a Gartner como fuente, cabe señalar que tal y como se indica en el estudio sobre La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y

competitivo[481] *"el crecimiento de los servicios basados en nube pública, a nivel mundial, seguirá en aumento hasta 2017. Dicho crecimiento aumentará un 17.4% en comparación con 2011 y pasará de 132 billones de dólares que los usuarios invirtieron en 2011 a casi 250 billones de dólares en 2017, incluyendo la publicidad."* Y también, citando de nuevo a Gartner, que *"por segmentos de mercado […] el primero es el relativo a la publicidad ("cloud advertising"), respecto del que se predice que desde 2013 hasta 2016 las empresas gastarán un total de 310 billones de dólares en todo el mundo."*

Estas cifras significan que hay una oportunidad de negocio en cuanto a la publicidad relativa a la nube *("cloud advertising")* previéndose una curva de ascenso en los recursos dedicados por las empresas a hacer publicidad.

- **Certificaciones relacionadas con el *cloud computing*:** La certificación, especialmente en materia de protección de datos personales[482], es una clara oportunidad de negocio[483] y en la que cada vez se requerirán más profesionistas y organizaciones dedicadas a ello. Resulta claro que el certificador debe ser un tercero independiente que emita la certificación con base en controles y requisitos que la organización que lo reciba mantenga en el tiempo. Además, la certificación en materia de cómputo en la nube es relevante a nivel internacional, siendo una de las

[481] Este documento ya ha sido citado y puede consultarse en http://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf. Pág. 8

[482] En cuanto a la certificación en protección de datos personales en México, deben tenerse en consideración los Parámetros de Autorregulación en materia de Protección de Datos Personales, a los que ya hemos hecho referencia.

[483] En México cabe señalar que en marzo de 2014 ya se había presentado la primera solicitud de autorización para fungir como entidad de acreditación en materia de protección de datos personales, indicándose en el Informe de actividades del IFAI Enero-Abril 2014 que el expediente se encontraba "en proceso de estudio a fin de determinar lo conducente en relación con la autorización solicitada para operar como entidad de acreditación, con fundamento en lo dispuesto en los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección Datos Personales en Posesión de los Particulares", por entonces aún vigentes. El Informe de actividades del IFAI, de fecha 2 de junio de 2014, está disponible en la dirección de Internet http://inicio.ifai.org.mx/Otros/InformeCuatrimestralEnero%20_Abril2014.pdf

cuestiones torales a las que la Comisión Europea está prestando atención ya que es parte de su estrategia sobre cómputo en la nube[484]. Junto con la protección de datos personales, la seguridad es otra de las materias objeto de certificación, y ello sin perjuicio de otras que también lo sean o puedan ser.

En cualquier caso, la certificación emitida por un tercero independiente que cumpla con sólidos requisitos de conocimientos técnicos; experiencia profesional; recursos humanos y tecnológicos, puede impulsar el despegue del cómputo en la nube en México y, al mismo tiempo, ser una oportunidad de negocio para muchos profesionistas y organizaciones.

- **Agregadores de nube *("cloud aggregator")*:** Un servicio relacionado con la nube es el relativo a agregar nubes, a través del que un usuario puede hacer uso de varias cuentas de diferentes proveedores de servicios de cómputo en la nube para almacenar información, en lugar de hacerlo con un solo proveedor de servicios de cómputo en la nube. De esta manera el cliente puede elegir de manera alternativa con un solo usuario entre varios servicios de almacenamiento que le son proporcionados por varios proveedores de servicios de cómputo en la nube[485].

- **Servicios de monitorización:** A través de los que se ofrece a los clientes, mediante el uso de un tablero de mandos o *"dashboard"*,

[484] En su Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Liberar el potencial de la computación en nube en Europa, COM (2012) 529 final, Bruselas, 27 de septiembre de 2012, la Comisión destaca *"la necesidad de disponer de marcos específicos para la computación en nube en relación tanto con las normas y la certificación como con las condiciones contractuales."*. Y añade que *"El despegue de las actividades en nube se verá favorecido por un mayor uso de las normas, por la certificación de los servicios en la nube para demostrar que cumplen estas normas y por el refrendo de tales certificados por parte de las autoridades normativas para indicar el cumplimiento de las obligaciones jurídicas."* Pág. 11 La Comunicación está disponible en la dirección de Internet http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF

[485] En relación con esta posibilidad, puede verse el artículo disponible en la dirección de Internet http://talkincloud.com/cloud-services-aggregator/cloud-services-aggregators-brokerages-list-35-and-counting

la posibilidad de monitorear el nivel de uso de servicios de cómputo en la nube con la finalidad de ahorrar costos y poder tomar mejores decisiones en cuanto al uso de dichos servicios. De esta manera, se trata de hacer un uso eficiente de los servicios de cómputo en la nube proporcionados por los proveedores y tener un mejor control de las TI, con lo que ello supone en materia de inversiones y costos asociados[486].

También es posible la monitorización de la seguridad, siendo otra de las áreas en las que se demandarán cada vez más profesionistas y que, por tanto, constituye una oportunidad de prestar servicios relacionados con la nube[487].

Las oportunidades aquí indicadas son sólo algunas de las posibilidades, ya que día a día los emprendedores y las organizaciones desarrollan nuevas oportunidades. En cualquier caso, el cómputo en la nube implica que las organizaciones tengan ante sí la posibilidad de crear nuevos negocios proporcionando servicios tecnológicos y desarrollando tecnología a través de los que México pueda ser innovador, competitivo y crear nuevos empleados.

3. Guía práctica para empresas en la adopción de servicios de cómputo en la nube

Este apartado tiene por objeto establecer una serie de pasos que las empresas deben seguir para contratar servicios de cómputo en la nube. Con ello se pretende que dichas entidades cumplan con las obligaciones establecidas en la legislación aplicable, sobre todo en materia de protección de datos personales.

Para ello, en la primera parte se describen las características del cómputo en la nube que las empresas deben conocer antes de

[486] Sobre esta cuestión, puede verse, por ejemplo http://blogs.sap.com/innovation/cloud-computing/the-rise-of-cloud-service-management-services-0108040

[487] Al respecto, puede verse, por ejemplo la información disponible en la dirección de Internet https://www.gartner.com/doc/2007315

contratar estos servicios, tales como los tipos de nube, los servicios que se ofrecen, los sujetos obligados, la legislación aplicable, etcétera. Posteriormente se señalan los aspectos que las empresas deben considerar antes y durante la contratación de los servicios de cómputo en la nube para evitar el incumplimiento de la normatividad aplicable. En la parte final se detallan recomendaciones específicas para PYMEs que pretendan contratar servicios de cómputo en la nube.

3.1. Qué es el cómputo en la nube y qué sujetos participan

Según el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) por cómputo en la nube "se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente".

En cuanto al cómputo en la nube suele considerarse que hay:

- Cuatro clases de nubes:
  - 1) públicas;
  - 2) privadas;
  - 3) híbridas; y
  - 4) comunitarias;
- Cuatro categorías de ofertas de servicios de nube:
  - 1) infraestructura como servicio (*Infraestructure as a Service* –IaaS-;
  - 2) plataforma como servicio (*Platform as a Service* –PaaS-;
  - 3) software como servicio (*Software as a Service* –SaaS-; y
  - 4) *Business Process as a Service* –BPaaS-);
- Cinco características esenciales:
  - 1) autoservicio on-demand o pago por evento;
  - 2) acceso ubicuo a la red;

- 3) fondo común de recursos;
- 4) Rápida elasticidad; y
- 5) servicio medido.

El cómputo en la nube ofrece grandes posibilidades a las empresas para incrementar su actividad y negocio, tales como la reducción de costos y la posibilidad de acceder a la información en cualquier momento y desde cualquier lugar y reduciendo costes. Sin embargo, es imprescindible que a la hora de contratar servicios de cómputo en la nube se tengan en cuenta las implicaciones que ello tiene en materia de protección de datos.

Es importante que el usuario de los servicios cómputo en la nube tenga claro en quién recae la responsabilidad del tratamiento de los datos personales. Por ello que deberá tener en cuenta que:

1.- Una vez contratados los servicios de cómputo en la nube, el usuario sigue siendo el **responsable** del tratamiento de los datos personales[488] y por tanto quien tiene que adoptar las medidas necesarias para cumplir con los principios y deberes establecidos en la normatividad sobre protección de datos personales que, en general, es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento. Asimismo, en relación con los sujetos obligados públicos, deben tenerse en cuenta las regulaciones sobre protección de datos contenidas en la Ley Federal de Transparencia y Acceso a la Información y en las respectivas leyes estatales de transparencia.

2.- Se entiende que el prestador de servicios de cómputo en la nube es un **encargado** del tratamiento[489].

Por lo tanto, el usuario del servicio, como responsable del tratamiento de los datos personales, que incorpore dichos datos a

[488] De acuerdo con el artículo 3º, fracción XIV, de la LFPDPPP el responsable del tratamiento de los datos personales es la *"persona física o moral de carácter privado que decide sobre el tratamiento de datos personales".*

[489] El artículo 3º, fracción IX, define al encargado del tratamiento como " La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

servicios de cómputo en la nube, puede observar las recomendaciones que se establecen en esta guía práctica a la hora de contratar dichos servicios, de manera que se asegure antes de firmar ningún contrato o adherirse a condiciones o cláusulas generales de la contratación.

3.2. Legislación aplicable

Por las características del cómputo en la nube, los datos pueden encontrarse en distintos países, por lo que el usuario deberá conocer cuál es la legislación aplicable al contratar estos servicios.

Cuando se utilizan servicios de cómputo en la nube, los datos proporcionados por el usuario pueden localizarse en cualquier parte del mundo. Sin embargo, teniendo en cuenta que el responsable del tratamiento de los datos personales es el cliente de dichos servicios, las normas aplicables a dicha relación son las del domicilio del responsable del tratamiento. Por lo tanto, la normatividad aplicable sería la LFPDPPP y su Reglamento[490], independientemente de la ubicación del proveedor del servicio.

Por ende, en cuanto a la protección de los datos personales, lo relevante es dónde se encuentra el responsable del tratamiento y no la ubicación de los datos personales o de su tratamiento.

3.3. Aspectos a considerar previo al contrato de los servicios

Antes de decidir si es conveniente contratar servicios de cómputo en la nube, deberá tener en cuenta los siguientes aspectos:

---

[490] El Artículo 4 del Reglamento de la LFPDPPP señala que: "El presente Reglamento será de aplicación obligatoria a todo tratamiento cuando:
I. Sea efectuado en un establecimiento del responsable ubicado en territorio mexicano;
II. Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano;…"
La normatividad aplicable no puede ser modificada contractualmente.

a. Analizar los tratamientos de datos que realiza para identificar las partes que podrían ser transferidas a servicios de cómputo en la nube, considerando tanto los beneficios que traería la utilización del servicio, como los riegos que pudieran ocurrir (entendiendo por riesgos, por ejemplo, falta de control, etcétera).

b. Identificar claramente los tipos de datos personales que son tratados, clasificándolos en datos sensibles y no sensibles. Esto es importante porque la legislación otorga un nivel de protección más alto a los datos sensibles[491] y por tanto será necesario asegurarse de que el encargado del tratamiento implementa las medidas necesarias para protegerlos de manera adecuada.

c. Revisar los tipos de nube que se ofertan y determinar cuál es el más conveniente para las necesidades del usuario, tomando en cuenta que dicha elección afectará directamente al tratamiento de los datos personales (los tipos de nubes son: públicas, privadas, híbridas y comunitarias. Se recomienda el uso de nubes privadas para entidades que requieran centralizar los datos y tener un control directo de los mismos sin compartir recursos con nadie más, como es el caso de las Administraciones Públicas. En el caso de una PYME una nube pública puede ser una solución adecuada, o dependiendo de los requisitos de cumplimiento, se podría optar por una nube híbrida (pública + privada) en atención a los tratamientos de datos personales concretos que se lleven a cabo.

d. Analizar las modalidades de servicios de cómputo en la nube que existen y elegir la más conveniente tomando en consideración que pueden existir soluciones mixtas (las modalidades del servicio son: infraestructura como servicio, plataforma como servicio, *software* como servicio y "*Business Process as a Service*").

---

[491] El artículo 3º, fracción VI, define a los datos personales sensibles como: "Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

e. Seleccionar los datos personales que deben ser tratados en el cómputo en la nube y reservar el resto para otros sistemas que son utilizados por el usuario.

3.4. Aspectos a considerar al contratar el servicio

Para elegir adecuadamente al proveedor de los servicios de cómputo en la nube, deberá verificar si las condiciones en las que se presta el servicio tienen un adecuado nivel de protección de los datos personales. Para ello resulta necesario tener en cuenta las siguientes consideraciones:

3.4.1. Las obligaciones legales del proveedor del servicio.

El Reglamento de la LFPDPPP establece la prohibición de adherirse a servicios de cómputo en la nube que no reúnan los requisitos establecidos en su artículo 52[492]. El usuario de servicios de

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

I. Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y

II. Cuente con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

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

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

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

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

cómputo en la nube deberá firmar un contrato de prestación de servicios con el proveedor y asegurarse de que dicho contrato incorpore las condiciones establecidas en dicho precepto, para la prestación de servicios de cómputo en la nube. De no ser así, el cliente debería buscar un proveedor que sí cumpla con los requisitos previstos en la normatividad.

3.4.2. La ubicación del tratamiento de los datos personales

Es importante que el cliente se asegure de que el proveedor ha implementado medidas para garantizar la protección de datos personales y la seguridad en los tratamientos que lleva a cabo para prestar los servicios de cómputo en la nube. El usuario debe poder obtener información sobre dónde están los datos personales, preguntando al proveedor de servicios de cómputo en la nube y, preferiblemente pudiendo consultar esta información en el contrato que firme con el mismo, en su sitio web o de otra manera que permita un fácil y rápido acceso a la información.

3.4.3. La existencia de subencargados del tratamiento de los datos

Cuando el proveedor de servicios de cómputo en la nube no cuenta con todos los recursos necesarios para ofrecer dicho servicio o para proporcionar un mejor servicio realiza subcontrataciones a terceros. El proveedor debe proporcionar al cliente de sus servicios información sobre las subcontrataciones que realice. Dichos subcontratos tienen que ser autorizados por el proveedor. Más aún, los subcontratistas pueden a su vez subcontratar ciertos servicios, por lo que puede darse el caso de que existan cadenas de subcontrataciones que, en su caso, tienen que estar autorizadas por el usuario del servicio.

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

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

Por lo anterior, al contratar el servicio el usuario deberá:

1.- Informarse sobre la existencia de subcontratos en la prestación del servicio. El prestador del servicio deberá indicarle qué servicios son susceptibles de subcontratación y quiénes son los subcontratados que intervienen en el tratamiento de los datos.
2.- Después de revisar la información mencionada anteriormente deberá manifestar su conformidad con la misma.
3.- Asegurarse de que los contratos celebrados entre el proveedor y los subcontratistas contengan garantías jurídicas idénticas a las establecidas en el contrato de prestación de servicios celebrado con el proveedor[493].

3.4.4. La portabilidad de los datos

El usuario del servicio de cómputo en la nube, como responsable de los datos, debe tener la posibilidad de recuperar los datos personales que ha puesto a disposición del proveedor cuando la relación con éste llegue a su fin o en cualquier momento a lo largo de la prestación del servicio por cualquier razón que el responsable del tratamiento considere oportuna. El responsable de los datos en todo momento debe tener control sobre los mismos y cuidar que no sean alterados hasta que éstos lleguen a su destino final.

El formato en el que deberá entregarse la información debe ser pactado previamente, con el objeto de que ésta pueda ser almacenada nuevamente en los sistemas del usuario o, en su caso, sea trasladada a los sistemas de un nuevo proveedor.

[493] El artículo 74 de la LFPDPPP señala que “sin perjuicio de lo dispuesto en el artículo 37 de la Ley, las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales. A su vez, el artículo 75 establece que “A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales”.

A su vez, debe garantizarse que los datos puedan ser utilizados en todo momento, que se conserven íntegramente y que su transferencia a un nuevo proveedor o quién el responsable indique se realice fácilmente, ya que de lo contrario se entendería que el usuario se encuentra cautivo.

El usuario debe tener la posibilidad de que se realice la portabilidad de los datos cuando no esté de acuerdo con la prestación del servicio, ya sea en relación con la intervención de algún subcontratista en el tratamiento de los datos, por diferencias significativas en los términos y condiciones aplicables al contrato o cuando el proveedor modifique las condiciones del servicio de manera unilateral.

3.4.5. Las políticas y las medidas de seguridad

Ya que los datos personales van a ser tratados por un encargado del tratamiento a quien el responsable se los encomienda, es necesario que este último se asegure de que aquél adopta las medidas de seguridad necesarias para garantizar que los datos personales queden protegidos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado

Por lo anterior, el proveedor tiene la obligación de dar información precisa al usuario sobre todos los detalles del tratamiento de los datos, tales como las medidas de seguridad, quién tiene acceso a los datos, la existencia de subencargados, etc. De esta forma el usuario podrá evaluar los riesgos y los beneficios de la contratación del servicio y asegurarse de que se cumple con la normatividad sobre protección de datos personales y, en particular, el deber de seguridad.

A su vez, el responsable del tratamiento de los datos debe conocer en todo momento la ubicación de los datos y tener la posibilidad de gestionar su tratamiento, así como de disponer de dichos datos en un formato válido e interoperable.

El usuario de servicios de cómputo en la nube deberá asegurarse de que el proveedor implementará medidas de seguridad que le permitan:

1.- Garantizar la integridad y confidencialidad de los datos personales.

2.- Impedir el acceso a los datos de personas no autorizadas.

3.- La recuperación de la información en caso de que exista una incidencia en la seguridad.

Como se ha señalado anteriormente, los datos sensibles cuentan con un nivel más alto de protección, por lo que el usuario deberá cerciorarse de que el proveedor servicios de cómputo en la nube cuente con las medidas organizativas y técnicas que permitan reducir los riesgos. En este caso se recomienda la utilización de nubes privadas.

Por otro lado, si se accede a la información mediante redes de comunicación, deberá implementarse un nivel de seguridad igual al de los accesos de modo local. Es importante, por lo tanto, que el usuario se asegure de si hay una conexión encriptada con el servidor o plataforma de acceso del proveedor de servicios de cómputo en la nube, de manera que la información viaje encriptada y no sea accesible por terceros no autorizados.

El usuario deberá preferir a los proveedores que ofrezcan el servicio con las siguientes características:

1.- Que permitan al usuario comprobar en todo momento las medidas de seguridad, entre las que deberán incluirse los registros de las personas que han accedido a los datos.

2.- Que el proveedor cuente con una (o varias) certificación de seguridad adecuada. Por ejemplo, estándares como la norma ISO 27001 u otras certificaciones.

3.- Que el usuario tenga la posibilidad de solicitar a una entidad auditora reconocida que realice una auditoría de seguridad al proveedor del servicio o, en su caso, de acceder al informe de auditoría, o un resumen del mismo, de un tercero independiente

que la haya llevado a cabo para el proveedor de servicios de cómputo en la nube.
4.- Que el propio proveedor realice auditorías a las medidas de seguridad que ha implementado e informe a sus clientes, a través de un mecanismo adecuado, de los resultados de dicha auditoría.
5.- Que los datos personales que estén almacenados o en tránsito se encuentren cifrados.
6.- Que la seguridad sea atendida y auditada por personal cualificado.

Cuando exista una incidencia de seguridad que afecte a los datos personales que son responsabilidad del usuario, éste deberá ser informado por el proveedor inmediatamente. A su vez, deberá recibir información detallada sobre las medidas adoptadas para resolver dicha incidencia, ya que podría ser necesario avisar a los titulares de los datos personales sobre lo ocurrido.

3.4.6. Las condiciones de las transferencias de los datos personales

La comunicación de los datos personales a personas distintas del responsable o el encargado del tratamiento se considera como una transferencia de datos[494], por lo que, en este caso, deberá observarse lo establecido en los artículo 36 y 37 de la LFPDPPP [495], así como en el capítulo IV del Reglamento de dicha norma.

---

[494] El artículo 3º, fracción XIX de la LFPDPPP define como transferencia a "toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento". A su vez, el artículo 67 del Reglamento de la LFPDPPP señala que "La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado".

[495] "Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.
El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.
Artículo 37.- Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:
I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

De acuerdo con la legislación en la materia dicha transferencia se encuentra sujeta al consentimiento del titular de los datos (salvo las excepciones establecida en el artículo 37 de la LFPDPPP, mencionado anteriormente), deberá ser informada a este último mediante el aviso de privacidad y tiene que limitarse a la finalidad que la justifique[496].

En el caso de que se realice una transferencia internacional de datos, el usuario, como responsable del tratamiento, puede solicitar la opinión del IFAI respecto a si dicha transferencia cumple con lo dispuesto por la legislación nacional de protección de datos[497].

Cuando los datos personales se encuentren en el extranjero, si existe la posibilidad de que la autoridad competente esté facultada para solicitar información sobre dichos datos, el proveedor deberá informarlo al usuario, salvo que esté prohibido por la legislación de dicho país.

3.4.7. El borrado de los datos personales

Es muy importante que se implementen medidas que garanticen que, cuando se termine la prestación del servicio de cómputo en la nube, el proveedor no conservará los datos personales que el usuario le ha encomendado para su tratamiento. Una medida adecuada podría

---

II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular".

[496] Artículo 68 del reglamento de la LFPDPPP. A su vez, el artículo 69 del Reglamento señala que "para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realizó conforme a lo que establece la Ley y el presente Reglamento la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales".

[497] Artículo 76 del Reglamento de la LFPDPPP.

ser la emisión de una certificación de la destrucción por el proveedor o por un tercero independiente.

3.4.8. El ejercicio de los derechos ARCO

El usuario del servicio, como responsable del tratamiento de los datos, debe garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) a los titulares de los datos tratados. Por lo tanto, el proveedor debe establecer herramientas adecuadas para facilitar el ejercicio de dichos derechos[498]. Es decir, el usuario debe asegurarse de que el proveedor de servicios de nube le facilite la atención al ejercicio de los derechos ARCO por el titular de los datos personales.

3.5. Recomendaciones prácticas para las PYMEs

En este epígrafe se establecen algunas recomendaciones prácticas dirigidas específicamente a las PYMEs que son o pueden ser clientes de servicios de cómputo en la nube.

a. El cómputo en la nube (*cloud computing*) es una oportunidad para ser competitivos ya que permite el acceso a tecnología que hasta el momento sólo podían permitirse las grandes empresas que cuentan con los recursos necesarios para ello. No obstante, como cualquier otra tecnología, el cómputo en la nube tiene implicaciones que es necesario analizar previamente a la contratación de dichos servicios y tomando en consideración los riesgos derivados de la actividad de toda organización.

b. En particular, las PYMEs tienen que ser conscientes de que si tratan datos personales tienen que cumplir con la normatividad en la materia, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento, además de otra normatividad que sea aplicable a su actividad. En el caso del uso del

[498] Ver los capítulos III y IV de la LFPDPPP, así como los capítulos VII y VIII del reglamento respectivo.

cómputo en la nube es importante tener en consideración si el proveedor de dichos servicios actúa como un encargado del tratamiento, siendo ésta la norma general, y de manera que se garantice el cumplimiento de las obligaciones que corresponden al responsable del tratamiento.

c. Además de la normatividad sobre protección de datos, las PYMEs tienen que estar concientizadas en cuanto al cumplimento de otra normatividad, como por ejemplo, la relativa a la propiedad intelectual, de manera que cuando hagan uso de activos como el software no vulneren los derechos de autor, ya que ello implicaría la exigencia de responsabilidad. Igualmente, tienen que adoptar medidas para protegerse frente a los ciberdelitos ya que de lo contrario pondrían en riesgo sus activos, sean datos personales o información, pudiendo llegar a perder sus negocios.

d. Alcanzar las ventajas a que da lugar el uso del cómputo en la nube, implica tener que actuar de manera diligente, cumpliendo con las obligaciones previstas en la normatividad aplicable a las diferentes áreas de la actividad de cualquier organización y hacer un uso responsable de la tecnología. Además, es necesario también que las PYMEs se informen sobre las implicaciones del uso de la tecnología y sobre sus obligaciones para evitar incumplimientos.

e. Las dependencias y entidades de las Administraciones Públicas son o pueden ser también clientes de servicios de cómputo en la nube, siendo aplicables las recomendaciones anteriores, además de que éstas tienen que velar específicamente porque en la contratación de dichos servicios se cumpla con la normatividad y directrices relativas a la contratación de tecnología y servicios en el sector público.

f. Los clientes o futuros clientes de servicios de cómputo en la nube son una parte fundamental en cuanto al desarrollo tecnológico de México, debiendo actuar con responsabilidad y de manera activa en cuanto a construir un país cada vez más competitivo y eficiente, lo cual puede ser posible gracias al uso del cómputo en la nube y otras Tecnologías de la Información (TI).

4. *Checklist* para la revisión del cumplimiento

En este apartado se incluyen un *cheklist* general y un *checklist* específico que las empresas pueden utilizar para revisar por sí mismas su estado de cumplimento en las diferentes áreas de Derecho de las TIC, así como analizar los riesgos que asumen al contratar productos y servicios en la nube.

El primer *cheklist* incluye preguntas que, en diversas áreas, tienen por finalidad que pueda ser utilizada por los clientes o futuros clientes de cómputo en la nube para saber si cumplen con la normatividad y, de esta manera, conocer su situación actual. En concreto, el esta lista de comprobación incluye preguntas relativas a:

- Riesgos legales y regulatorios;
- Protección de datos personales;
- Seguridad;
- Propiedad intelectual;
- SLA[499] y otras cuestiones contractuales;
- Ciberdelitos, y
- Administraciones Públicas (en particular, dependencias y entidades de la Administración Pública Federal).

El segundo *cheklist* pretende que las empresas puedan evaluar los principales aspectos a considerar antes y durante la contratación de servicios de cómputo en la nube.

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

[499] Acuerdo de nivel de servicio (en inglés, *Service Level Agrement*, SLA).

4.1. *Checklist* general sobre cómputo en la nube

RIESGOS LEGALES Y REGULATORIOS		
¿Ha adoptado medidas para identificar riesgos legales y regulatorios previamente a la contratación de servicios de cómputo en la nube?	Sí	No
Cuando contrata servicios de cómputo en la nube, ¿ha adoptado medidas de gestión para minimizar los riegos legales y regulatorios que pudieran ocurrir?	Sí	No
¿Ha verificado que los servicios de cómputo en la nube y la tecnología necesaria para la misma cumplan con las Normas Oficiales Mexicanas y las normas internacionales aplicables en la materia?	Sí	No
En caso de que se produzca algún incumplimiento, ¿tiene previsto un procedimiento para adoptar medidas correctivas que le permitan responder ante dicha situación?	Sí	No
En relación con los servicios que pudiera subcontratar el proveedor de servicios de cómputo en la nube, ¿le ha proporcionado información sobre si existen políticas específicas sobre el uso de subcontratistas?	Sí	No
Con respecto al proveedor de servicios de cómputo en la nube, ¿sabe si se somete esporádicamente a algún procedimiento de evaluación de su desempeño?	Sí	No
¿Tiene suficiente ancho de banda para hacer uso del servicio y se ha informado sobre las características del mismo en cuanto a necesidad de hardware y conexión?	Sí	No

PROTECCIÓN DE DATOS PERSONALES		
Al contratar servicios de cómputo en la nube, ¿ha visto si en el contrato correspondiente se considera al cliente de servicios de cómputo en la nube como responsable del tratamiento de los datos personales?	Sí	No
Al contratar servicios de cómputo en la nube, ¿ha visto si en el contrato se considera al prestador de servicios de cómputo en la nube como encargado del tratamiento de datos personales?	Sí	No

Al firmar el contrato u otro instrumento jurídico con el proveedor de servicios de cómputo en la nube, ¿se asegura de que el acuerdo esté acorde con el aviso de privacidad correspondiente?	Sí	No
¿Ha adoptado las medidas necesarias para identificar riesgos en materia de protección de datos personales y para minimizar dichos riesgos?	Sí	No
¿Los datos personales se recaban y se tratan conforme a las disposiciones legales establecidas?	Sí	No
¿Los datos personales que se tratan cumplen con los principios previstos en la normatividad?	Sí	No
¿Ha establecido políticas de protección de datos personales afines a los principios y deberes que establecen las normas en la materia?	Sí	No
¿Cuenta con políticas de protección de datos y privacidad que se refieran a todos los tratamientos de datos personales que lleva a cabo, incluido el uso de la nube?	Sí	No
¿Cuenta con alguna certificación en materia de protección de datos personales y si es así, dicha certificación se refiere también a tratamientos de datos por encargados y en la nube?	Sí	No
Antes de contratar los servicios de cómputo en la nube, ¿se ha asegurado de que el proveedor de servicios de cómputo en la nube se abstiene de incluir condiciones relativas a la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio?	Sí	No
¿En el aviso de privacidad se ha informado a los titulares de los datos personales que se tratan sobre las características principales del tratamiento al que será sometida dicha información?	Sí	No
¿Ha adoptado medidas para asegurarse de que los datos personales que recoge son exactos y están actualizados?	Sí	No
¿Ha adoptado medidas para asegurarse de que los datos personales que trata sean veraces mientras persiste su tratamiento?	Sí	No
¿El tratamiento de los datos personales se lleva a cabo en el ámbito de finalidades determinadas, explícitas y legítimas	Sí	No

relacionadas con la actividad del usuario del servicio?		
¿Ha verificado que el tratamiento de datos personales sea únicamente el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad?	Sí	No
¿Ha verificado si el proveedor de servicios de cómputo en la nube ha adoptado medidas para guardar confidencialidad respecto de los datos personales sobre los que se presta el servicio?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para impedir el acceso a los datos a personas que no cuenten con privilegios de acceso?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube ha implementado medidas para informar al responsable de los datos personales cuando exista una solicitud fundada y motivada de autoridad competente?	Sí	No
¿Maneja datos sensibles que hagan referencia a salud, ideología, afiliación sindical, religión, etc.?	Sí	No
¿Verifica que las bases de datos que contengan datos personales sensibles se únicamente se creen cuando exista una finalidad legítima, concreta y acorde con las actividades o fines explícitos que procura el sujeto regulado?	Sí	No
¿Ha considerado la posibilidad de hacer uso de una nube privada para el tratamiento de datos sensibles?	Sí	No
¿Cuenta con mecanismos para resguardar los datos personales de tal forma que los derechos de acceso, rectificación, cancelación y oposición puedan ser ejercidos sin dilación?	Sí	No
Antes de contratar los servicios de cómputo en la nube, ¿ha revisado si el proveedor de servicios transparenta las subcontrataciones que involucren la información sobre la que se presta el servicio?	Sí	No
Se ha asegurado de que si el proveedor de servicios subcontrata el servicio de cómputo en la nube o servicios relacionados con el mismo, ¿cuenta con la autorización necesaria?	Sí	No

¿La subcontratación de servicios de cómputo se formaliza a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido?	Sí	No
¿Ha adoptado medidas, tales como supervisiones, auditorias o certificaciones, para velar porque el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumpla con sus obligaciones en materia de protección de datos personales?	Sí	No
¿Empleas mecanismos de autorregulación para verificar que el prestador de servicios de cómputo en la nube cumple con sus obligaciones en materia de protección de datos?	Sí	No
¿Ha verificado si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta?	Sí	No
¿Se ha informado de que el proveedor de servicios de cómputo en la nube le permite recuperar sus datos una vez que haya concluido el servicio?	Sí	No
¿Los plazos para la eliminación de los datos al finalizar el servicio son razonables?	Sí	No
¿Se ha informado o le han informado de cómo garantiza el proveedor de servicios de cómputo en la nube la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable?	Sí	No
¿Puede asegurarse de que los datos se borrarán al final del servicio por el proveedor de servicios de cómputo en la nube?	Sí	No
SEGURIDAD		
¿Conoce qué normatividad le aplica en materia de seguridad?	Sí	No
Antes de contratar servicios de cómputo en la nube, ¿el proveedor de servicios de cómputo en la nube le ha informado o usted ha solicitado información sobre qué medidas de seguridad ha adoptado para la protección de los datos personales sobre los que se presta el servicio?	Sí	No
¿Cuenta con medidas de seguridad para proteger los datos	Sí	No

personales que trata?		
¿Los datos sensibles están protegidos de tal forma que sólo las personas autorizadas pueden tener acceso a los mismos?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube ha adoptado medidas para evitar que terceros no autorizados accedan a los datos personales u otra información que trata para prestarle el servicio?	Sí	No
¿Existen mecanismos de protección de la identidad de los usuarios que acceden a datos personales para tratarlos en el desarrollo de sus funciones?	Sí	No
¿Existen reglas para el acceso de los empleados a los datos de los clientes?	Sí	No
¿Documenta el acceso de los empleados a los datos de los clientes?	Sí	No
¿Existen medidas disciplinarias para el caso de que los empleados vulneren las reglas de acceso a los datos de los clientes?	Sí	No
Aunque los datos personales u otra información esté almacenada en la nube, ¿realiza con frecuencias copias de seguridad de los datos?	Sí	No
¿Las copias de seguridad están almacenadas en un lugar seguro?	Sí	No
Si sufre una pérdida de datos, ¿puede restaurarlos fácilmente a partir de una copia de seguridad?	Sí	No
¿Existen medidas de seguridad para prevenir la fuga de datos?	Sí	No
¿Existen procedimientos para el manejo de fugas de datos?	Sí	No
¿Se escanea con frecuencia en busca de vulnerabilidades de la red y las aplicaciones?	Sí	No
En caso de que exista un fallo en la seguridad, ¿cuenta con medidas para notificar a los titulares de los datos personales que trata en la nube?	Sí	No
¿Cuenta con procedimientos de reparación de vulnerabilidades?	Sí	No
¿Los plazos para reaccionar a una vulneración de la seguridad son razonables?	Sí	No

PROPIEDAD INTELECTUAL		
¿En los contratos SLA se estipula que todos los datos del usuario (incluyendo los que son objeto de copias duplicadas) son propiedad del mismo de manera que el proveedor de servicios de cómputo en la nube no adquiere ningún derecho de propiedad intelectual u otro título sobre los mismos?	Sí	No
¿Los SLA o las condiciones de contratación que le ofrece el proveedor de servicios de cómputo en la nube, prevén de alguna manera la transferencia derechos de propiedad intelectual?	Sí	No
¿Cuenta con contratos de licencias de software?	Sí	No
¿Cuándo contrata servicios de cómputo en la nube se asegura de obtener las licencias necesarias?	Sí	No
¿Ha adoptado medidas para gestionar los activos de software, como por ejemplo cumplir con la norma ISO/IEC 19770 sobre gestión de activos de software (en inglés, *Software Asset Management*, SAM)	Sí	No
¿Se ha asegurado de que el proveedor de servicios de cómputo en la nube garantice la confidencialidad respecto a la información sujeta a derechos de propiedad intelectual que transfiera a la nube?	Sí	No
SLA Y OTRAS CUESTIONES CONTRACTUALES		
¿Los contratos incluyen cláusulas relativas a la interoperabilidad?	Sí	No
¿Se estipulan algunas medidas de compensación adecuadas para los usuarios en caso de que ocurra un incidente de seguridad o se incumpla con la prestación del servicio?	Sí	No
¿En el contrato de nivel de servicio se establecen cláusulas legales y contractuales que garanticen al cliente que el proveedor será sancionado en caso de incumplir con sus obligaciones o tenga fallos en la prestación de servicio?	Sí	No
¿El usuario tiene derecho a rescindir el contrato si el proveedor realiza modificaciones sustanciales a los términos estipulados en el contrato?	Sí	No

¿El usuario tiene derecho de rescindir el contrato si se incumple con las obligaciones de privacidad y seguridad estipuladas en el contrato?	Sí	No
¿Existen cláusulas de responsabilidad por pérdida de los datos o revelación indebida de los mismos por parte del proveedor o cualquier subcontratista?	Sí	No
¿Los contratos contienen previsiones sobre la finalización de los mismos?	Sí	No
¿El acuerdo de nivel de servicio contiene previsiones sobre la finalización del contrato, de manera que si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube?	Sí	No
¿Al finalizar el contrato se entrega el cliente una copia completa de todos sus datos?	Sí	No
CIBERDELITOS		
¿Se ha asegurado de que el proveedor de servicios de cómputo en la nube tenga implementadas medidas para prevenir y, en su caso, reaccionar ante ataques informáticos?	Sí	No
¿Se ha informado antes de contratar servicios de cómputo en la nube si el proveedor cuenta con procedimientos para descubrir e investigar ataques informáticos a sus redes y servidores?	Sí	No
Con independencia de las medidas adoptadas por el proveedor de servicios de cómputo en la nube, ¿cuenta usted con medidas de seguridad para prevenir ataques informáticos?	Sí	No
¿Sabe si el proveedor de servicios de cómputo en la nube audita periódicamente que sus redes y sistemas de información sean seguros frente a ataques informáticos?	Sí	No
Ante una fuga de datos como consecuencia de un ataque informático, ¿el contrato o SLA con el proveedor de servicios de cómputo en la nube prevé un mecanismo de notificación al cliente y de respuesta ante la incidencia por el proveedor?	Sí	No
¿Se ha informado sobre si la arquitectura del proveedor de servicios ha sido desarrollada conforme a estándares y normas para evitar intrusiones o ataques informáticos?	Sí	No

¿Ha considerado si el proveedor de servicios de cómputo en la nube ha incluido en el contrato previsiones sobre responsabilidad en caso de que sea objeto de un ataque informático que produzca pérdida de datos o fuga de los mismos?	Sí	No
¿Ha analizado si el proveedor de servicios de cómputo en la nube cuenta con alguna póliza de seguro frente a ciberataques?	Sí	No

ADMINISTRACIONES PÚBLICAS (EN PARTICULAR, DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA FEDERAL)		
¿Ha considerado las ventajas en cuanto a costos y eficiencia que puede tener el uso de servicios de cómputo en la nube?	Sí	No
¿Se ha asegurado que la contratación de servicios de cómputo en la nube cumple con la normatividad aplicable a la contratación de TIC en el sector público?	Sí	No
En el caso de dependencias de la Administración Pública, ¿las licitaciones públicas para la contratación de servicios incluyen previsiones sobre interoperabilidad y finalización del contrato?	Sí	No
En el caso de dependencias de la Administración Pública, ¿establecen cláusulas contractuales que permitan asegurar que la información del sector público es tratada de manera adecuada por sujetos privados a los que se confía dicha información?	Sí	No
En los términos de referencia de la licitación pública, ¿se contempla al proveedor de servicios de cómputo en la nube como encargado del tratamiento y se prevén garantías contractuales que éste tendrá que hacer firmar también a los subcontratistas que, en su caso, hayan sido identificados o autorizados?	Sí	No
¿Se ha asegurado a través de los términos de referencia de la licitación pública que la información que se almacene o trate en los servicios de cómputo en la nube es propiedad de la dependencia o entidad de manera que el proveedor de servicios de cómputo en la nube no adquiere ningún título	Sí	No

sobre la misma y que los derechos de autor u otra propiedad intelectual corresponde a la Administración Pública correspondiente?		
Cuando contrata servicios de cómputo en la nube, ¿se ha asegurado de que el proveedor se obliga contractualmente o a través de otras garantías a no utilizar los datos personales con fines distintos a proporcionar los servicios de cómputo en la nube?	Sí	No
Antes de contratar servicios de cómputo en la nube, ¿ha clasificado la información para identificar cuál es reservada y confidencial?	Sí	No
El servicio de cómputo contratado, ¿garantiza que si la dependencia o entidad tiene que responder a una solicitud de acceso a la información pública gubernamental, está disponible aunque sea tratada por el proveedor de servicios de cómputo en la nube?	Sí	No
¿Ha analizado con qué certificaciones cuenta el proveedor de servicios de cómputo en la nube, tales como ISO/IEC 27001, ISO/EC 27018 u otras similares que impliquen que ha sido certificado por un tercero?	Sí	No
¿Se ha previsto la posibilidad de auditar o tener acceso al informe de auditoría o certificación correspondiente a lo largo del contrato para monitorear en todo momento que se cumplen con las métricas correspondientes en cuanto a nivel de servicio, seguridad, etc.?	Sí	No
¿Le ha proporcionado o, en su caso, ha pedido información al proveedor de servicios de cómputo en la nube sobre la región o lugares donde almacenará los datos personales y otra información para prestarle el servicio?	Sí	No
Los términos de referencia para una licitación pública en la contratación, ¿incluyen cuestiones relativas al nivel de servicio en cuanto a la disponibilidad y accesibilidad del mismo así como las correspondientes penalidades a las que quedará sujeto el proveedor del servicio en caso de que el servicio no esté disponible por causas no atribuibles al mismo?	Sí	No
¿Ha considerado si el proveedor de servicios de cómputo en la nube aplica criptografía para garantizar que la información se	Sí	No

almacene (en reposo) y transmita de forma segura así como que los certificados electrónicos y la firma electrónica utilizada cumplan con las disposiciones de la Ley de Firma Electrónica Avanzada?		
¿Se ha asegurado, en su caso a través de los términos de referencia de la licitación pública, que la información que será almacenada y tratada en la nube estará disponible en todo momento y podrán obtenerse copias de seguridad en todo momento a través de formatos definidos de manera que se garantice la interoperabilidad y la portabilidad?	Sí	No
¿Se ha asegurado en los términos de referencia de la licitación pública que el proveedor de servicios de cómputo está obligado a notificar cualquier cambio en los términos del servicio con anterioridad a su implementación y el derecho de la dependencia o entidad a rescindir el contrato en su caso?	Sí	No
¿Se han previsto cláusulas en los términos de referencia en virtud de las que se asegure que el proveedor de servicios de cómputo en la nube responderá de la responsabilidad que le sea exigible con respecto a las cuestiones que surjan a lo largo de la prestación del servicio?	Sí	No

4.2. *Checklist* específico sobre cómputo en la nube

En el desarrollo de sus actividades, ¿utiliza o tiene planeado utilizar servicios de cómputo en la nube?	Sí	No
En el desarrollo de sus actividades, ¿tiene planeado prestar servicios de cómputo en la nube o relacionados con el cómputo en la nube? (Por ejemplo: desarrollo de aplicaciones, desarrollo de *software*, etc.?	Sí	No
¿Conoce las ventajas que le proporcionaría el uso de servicios de cómputo en la nube para el desarrollo de sus actividades? (Por ejemplo: ahorro de costos, la posibilidad de acceder a la información en cualquier momento y desde cualquier lugar, etc.).	Sí	No
Si usted es usuario de servicios de cómputo en la nube, ¿conoce sus obligaciones legales como responsable del	Sí	No

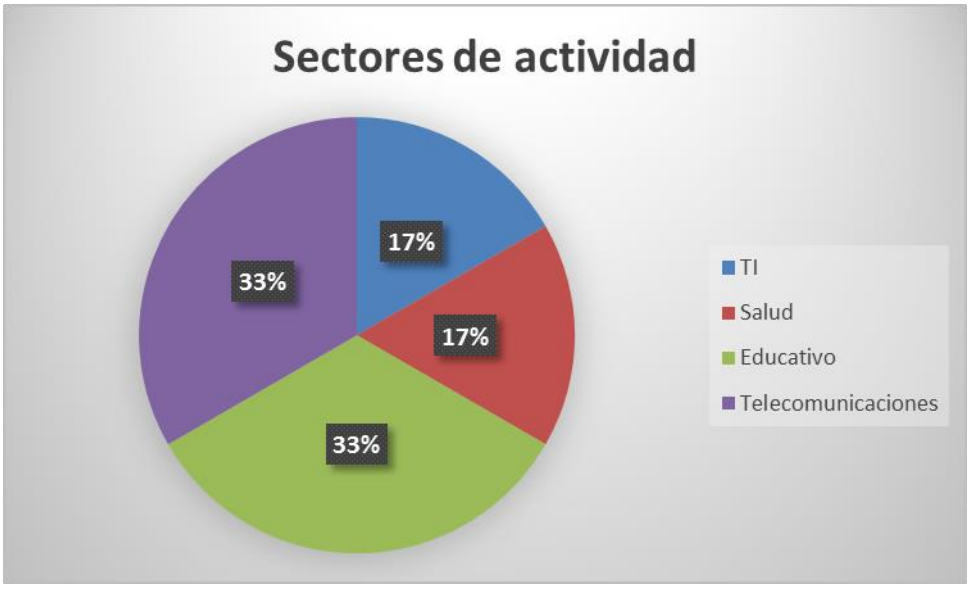
tratamiento de datos personales?		
Si usted presta servicios de cómputo en la nube, ¿conoce sus obligaciones legales como encargado del tratamiento de datos personales?	Sí	No
¿Ha analizado o identificado qué datos personales va a transferir a la nube?	Sí	No
¿Ha clasificado los datos personales en atención a su sensibilidad?	Sí	No
¿Ha analizado los diferentes tipos de nubes?	Sí	No
¿Ha analizado las modalidades de servicios de nube?	Sí	No
¿Cuenta con un contrato de prestación de servicios que reúna los requisitos establecido en el artículo 52 de la LPDP?	Sí	No
¿El proveedor tiene algún mecanismo que le permita conocer la ubicación exacta de los datos personales?	Sí	No
¿Sabe si existen subcontratos para la prestación de los servicios de cómputo en la nube?	Sí	No
¿Conoce qué servicios se prestan por los subcontratistas?	Sí	No
¿Conoce quiénes son los subcontratados?	Sí	No
¿El proveedor le ha pedido su consentimiento para realizar las subcontrataciones?	Sí	No
¿Sabe si los contratos celebrados con los subcontratistas contienen las mismas garantías judiciales que están establecidas en el contrato que usted ha celebrado con el proveedor?	Sí	No
¿El titular de los datos ha dado su consentimiento para que sus datos sean transferidos a subcontratistas?	Sí	No
¿Se ha informado al titular de los datos sobre las transferencias realizadas a sus datos en el aviso de privacidad?	Sí	No
¿Existe algún mecanismo para que usted pueda recuperar los datos personales que ha puesto a disposición del proveedor cuando se termine la relación con éste?	Sí	No
¿Ha pactado el formato en el que el proveedor deberá entregarle esta información?	Sí	No
¿En todo momento puede utilizar los datos personales que ha puesto a disposición del proveedor?	Sí	No
¿Conoce las medidas de seguridad que ha adoptado el	Sí	No

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

VI. RESULTADOS DE LA APLICACIÓN DE LA "GUÍA PARA EMPRESAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL USO DEL CÓMPUTO EN LA NUBE"

Las empresas piloto participantes en la implementación de esta guía han dado su autorización para utilizar la información proporcionada únicamente con fines estadísticos, por lo que no es posible proporcionar sus datos de identificación.

Las organizaciones participantes, tanto del sector público (34%) como del privado (66%), en el proyecto piloto fueron un total de seis (6), que por sectores de actividad se distribuyen en los relativos a Tecnologías de Información (TI), educativo, telecomunicaciones y salud. Gráficamente es posible presentar dicha participación de la siguiente manera:



De la implementación de esta guía práctica a las organizaciones mencionadas anteriormente, se desprenden los siguientes resultados:

1. Uso general del cómputo en la nube

Del análisis realizado a las organizaciones participantes en el proyecto piloto, se destacan los siguientes aspectos sobre el uso general del cómputo en la nube:

- 100% está utilizando o tiene planeado utilizar servicios de cómputo en la nube en el desarrollo de sus actividades.
- 90% tiene planeado prestar servicios de cómputo en la nube o relacionados con el cómputo en la nube, como por ejemplo, desarrollo de software o de apps.

2. Riesgos legales y regulatorios

Del estudio realizado sobre la existencia de riesgos legales y regulatorios se desprende lo siguiente:

- En casi todas las organizaciones (83.4%) en las que se ha realizado el proyecto piloto, se indica que han adoptado medidas para identificar riesgos legales y regulatorios previamente a la contratación de servicios de cómputo en la nube.
- El 50% de las organizaciones ha verificado que los servicios de cómputo en la nube y la tecnología necesaria para la misma cumplan con las Normas Oficiales Mexicanas y las normas internacionales aplicables en la materia.
- Un 66.6%, lo que representa la mayoría de las organizaciones participantes en el piloto, tiene previsto un procedimiento para adoptar medidas correctivas que le permitan responder en caso de que se produzca algún incumplimiento.
- También el 66.6% de las organizaciones participantes en el piloto, como cliente de servicios de cómputo en la nube, es considerada como responsable del tratamiento.
- Casi todas las organizaciones (83.4%) han indicado que han

Casi todas las organizaciones (83.4%) indican haber adoptado las medidas necesarias para identificar riesgos en materia de protección de datos personales y para minimizar dichos riesgos.

adoptado las medidas necesarias para identificar riesgos en materia de protección de datos personales y para minimizar dichos riesgos.

3. Datos Personales

En materia de protección de datos personales, el análisis de las organizaciones participantes en el piloto arroja los siguientes resultados:

- La mayoría (66.6%) no conoce sus obligaciones legales como usuario de servicios de cómputo en la nube cuando actúa como responsable del tratamiento.
- El 50% ha analizado o identificado qué datos personales podría transferir a la nube.
- El 50% ha clasificado los datos personales en atención a su sensibilidad.
- La mayoría (66.6%) ha analizado los diferentes tipos de nubes.
- Ninguna de las organizaciones participantes dice tener un contrato de prestación de servicios que reúna los requisitos establecidos en el artículo 52 del Reglamento de la LFPDPPP.
- La mitad de las organizaciones participantes afirma que su proveedor de servicios de cómputo en la nube tiene mecanismos que les permiten conocer la ubicación exacta de los datos personales.
- El 50% indica que sabe de la existencia de sub-contratos para la prestación de servicios de cómputo en la nube. De ese 50%, la mayoría indica que conoce los servicios que prestan, en su caso, los subcontratistas.
- El 50% ha respondido que conoce la existencia de un mecanismo para que pueda recuperar los datos personales que ha puesto a disposición del proveedor de servicios de cómputo en la nube cuando termine la relación contractual.
- Excepto una de las organizaciones participantes (16.6%), las demás (83.4%) han contestado que pueden utilizar los datos personales que han puesto a disposición del proveedor de servicios de cómputo en la nube.

- En el 50% de los casos el proveedor cuenta con medidas para garantizar que, cuando termine la prestación del servicio, no conservará los datos personales que le han sido encomendados, como por ejemplo la emisión de una certificación o de algún documento oficial.
- También en el 50% de los casos el proveedor cuenta con mecanismos para facilitar la atención al ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) de los titulares de los datos.
- La mitad de las organizaciones (50%) han indicado que los datos personales que se tratan cumplen con los principios aplicables en la materia.
- La mayoría de las organizaciones (66.6%) han establecido políticas de protección de datos personales afines a los principios y deberes que establecen las normas en la materia y casi todas (83.4%) cuentan con políticas de protección de datos y privacidad que se refieran a todos los tratamientos de datos personales que lleva a cabo, incluido el uso de la nube.
- En el 33.2% de los casos, las organizaciones han indicado que cuentan con alguna certificación en materia de protección de datos personales y dicha certificación se refiere también a tratamientos de datos por encargados y en la nube.
- En la mayoría de las organizaciones (66.6%) se observa que antes de contratar los servicios de cómputo en la nube, **no** se han asegurado de que el proveedor de servicios de cómputo en la nube se abstenga de incluir condiciones relativas a la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.

En la mayoría de los casos (66.6%) las organizaciones no han adoptado medidas tales como auditorías o certificaciones para velar porque el proveedor de servicios de cómputo en la nube cumpla, como encargado del tratamiento, con sus obligaciones en protección de datos personales.

- En el caso de la subcontratación por el proveedor de servicios de cómputo en la nube, la mayoría (66.6%) de las organizaciones han indicado que ésta se formaliza a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.

- La mayoría de las organizaciones (66.6%) **no** han adoptado medidas, tales como supervisiones, auditorias o certificaciones, para velar porque el prestador de servicios de cómputo en la nube, como encargado del tratamiento, cumpla con sus obligaciones en materia de protección de datos personales.
- La mitad de las organizaciones (50%) emplean mecanismos de autorregulación para verificar que el prestador de servicios de cómputo en la nube cumple con sus obligaciones en materia de protección de datos.
- Se observó que en casi todas las organizaciones (83.4%) **no** se ha verificado si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
- La mayoría de las organizaciones (66.6%) se han informado de que el proveedor de servicios de cómputo en la nube le permite recuperar sus datos una vez que haya concluido el servicio.
- Casi todas las organizaciones (83.4%) consideran que los plazos para la eliminación de los datos al finalizar el servicio son razonables.
- La mitad de las organizaciones (50%) indican que se ha informado o le han informado de cómo garantiza el proveedor de servicios de cómputo en la nube la supresión de los datos personales una vez que haya concluido el servicio prestado.
- Por último, el 33.2% de las organizaciones pueden asegurarse de que los datos se borrarán al final del servicio por el proveedor de servicios de cómputo en la nube.

Casi todas las organizaciones (83.4%) indican que no han verificado si el proveedor de servicios de cómputo en la nube cuenta con mecanismos para dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.

4. Medidas de seguridad

En el caso de las medidas de seguridad, del análisis de las organizaciones participantes en el piloto se concluye lo siguiente:

- La mayoría (66.6%) dice conocer las medidas de seguridad que ha adoptado el proveedor de servicios de cómputo en la nube, aunque sólo un 40% puede comprobar en todo momento las medidas de seguridad que aquél ha adoptado y también conoce qué personas tienen y, en su caso, han tenido acceso a los datos personales que trata el proveedor.
- En cuanto a si el proveedor cuenta con alguna certificación de seguridad, como por ejemplo la ISO/IEC 27001, sólo una de las organizaciones que son clientes de servicios de cómputo en la nube ha respondido afirmativamente.
- El 50% de las organizaciones que son clientes de servicios de cómputo en la nube han indicado que pueden solicitar una auditoría de las medidas de seguridad del proveedor, si bien sólo una de las organizaciones participantes puede acceder a los informes de auditoría que se hayan realizado por el proveedor.
- El 80% de las organizaciones han señalado que en caso de que hayan existido incidencias de seguridad el proveedor de servicios de cómputo en la nube ha informado sobre las mismas así como de las medidas adoptadas para resolverlas.
- Sólo dos (33.2%) de las organizaciones participantes han señalado que el proveedor de servicios de cómputo en la nube cuenta con mecanismos reforzados de protección para datos sensibles, siendo también destacable el hecho de que la mayoría de las organizaciones (66.6%) hayan indicado que los datos sensibles se encuentran en nubes privadas.
- En casi todos los casos (83.4%) los clientes de servicios de cómputo en la nube disponen de una conexión encriptada con el servidor o la plataforma de acceso del proveedor.
- En la mayoría de las ocasiones (66.6%) los datos personales almacenados o en tránsito se encuentran encriptados.

- En todos los casos (100%), las organizaciones han indicado que los datos sensibles están protegidos de tal forma que sólo las personas autorizadas pueden tener acceso a los mismos
- La mitad de las organizaciones (50%) señalaron que antes de contratar servicios de cómputo en la nube el proveedor de servicios les ha informado o, a su vez, les ha solicitado información sobre qué medidas de seguridad ha adoptado para la protección de los datos personales sobre los que se presta el servicio.
- En la mayoría de los casos (66.6%) las organizaciones señalan que existen reglas de los proveedores de servicios de cómputo en la nube para el acceso de los empleados a los datos de los clientes; que dicho acceso está documentado y que existen medidas disciplinarias para el caso de que los empleados vulneren las reglas de acceso a los datos de los clientes.
- En todos los casos (100%) las organizaciones han indicado que aunque los datos personales u otra información esté almacenada en la nube, realizan con frecuencias copias de seguridad de los datos; y también que pueden restaurar los datos personales fácilmente a partir de una copia de seguridad en caso de que se sufra una pérdida.
- Casi en todos los casos (83.4%) las organizaciones señalan que las copias de seguridad están almacenadas en un lugar seguro.
- En la mitad los casos (50%) existen medidas de seguridad para prevenir la fuga de datos y también se escanea con frecuencia en busca de vulnerabilidades de la red y las aplicaciones.
- Por lo que se refiere a la notificación de fuga de datos, sólo algunas organizaciones (33.2%) cuentan con medidas para notificarlo a los titulares de los datos personales.
- La mayoría de las organizaciones (66.6%) cuenta con procedimientos de reparación de vulnerabilidades.
- Por último, casi todas las organizaciones (83.4%) tienen plazos razonables para reaccionar ante una vulneración de la seguridad.

5. Propiedad intelectual

En relación con la propiedad intelectual, de la implementación del piloto a las organizaciones participantes se puede derivar lo siguiente:

- En la mitad de las organizaciones (50%), en los contratos SLA se estipula que todos los datos del usuario (incluyendo los que son objeto de copias duplicadas) son propiedad del mismo de manera que el proveedor de servicios de cómputo en la nube no adquiere ningún derecho de propiedad intelectual u otro título sobre los mismos.
- Casi todas las organizaciones (83.4%) se asegura de obtener las licencias necesarias cuando contrata servicios de cómputo en la nube. No obstante, casi todas las organizaciones (83.4%) han indicado que no han adoptado medidas para gestionar los activos de software (como por ejemplo cumplir con la norma ISO/IEC 19770 sobre gestión de activos de software; en inglés, Software Asset Management, SAM).
- Por último, la mitad de las organizaciones se ha asegurado de que el proveedor de servicios de cómputo en la nube garantice la confidencialidad respecto a la información sujeta a derechos de propiedad intelectual que transfiera a la nube.

6. Acuerdos de nivel de servicio (SLA) y otras cuestiones contractuales

La guía también se refiere a los acuerdos de nivel de servicio (*Service Level Agreement*, SLA) y otras cuestiones contractuales, siendo relevantes los siguientes aspectos en virtud de lo manifestado por las organizaciones participantes en el piloto:

- La mitad (50%) ha indicado que los contratos de servicio que tienen incluyen cláusulas relativas a la interoperabilidad.
- También la mitad afirma que en el correspondiente contrato se estipulan algunas medidas de compensación adecuadas para los

usuarios en caso de que ocurra un incidente de seguridad o se incumpla con la prestación del servicio.

- Casi la totalidad de las organizaciones (83.4%) señalan que en el contrato de nivel de servicio se establecen cláusulas legales y contractuales que garanticen al cliente que el proveedor será sancionado en caso de incumplir con sus obligaciones o tenga fallos en la prestación de servicio.
- La mayoría de las organizaciones (66.6%), en virtud del correspondiente contrato, tienen derecho a rescindir el contrato si el proveedor realiza modificaciones sustanciales a los términos estipulados en el contrato así como si se incumple con las obligaciones de privacidad y seguridad estipuladas en el contrato.
- También en la mayoría de los casos (66.6%) las organizaciones participantes han indicado que existen cláusulas de responsabilidad por pérdida de los datos o revelación indebida de los mismos por parte del proveedor o cualquier subcontratista.
- En la totalidad de los casos, las organizaciones los contratos incluyen previsiones sobre su finalización. No obstante, en el 50% de los casos el acuerdo de nivel de servicio **no** contiene previsiones sobre la finalización del contrato, de manera que si el cliente lo desea, pueda recuperar la información y llevarla a otro proveedor de servicios de cómputo en la nube.
- Por último, en la mayoría de los casos (66.6%) se observa que al finalizar el contrato se le entregará a la organización, como cliente de servicios de cómputo en la nube, una copia de todos los datos.

7. Ciberdelitos

Sobre la posibilidad de que se cometan ciberdelitos, las organizaciones participantes en el piloto han puesto de manifiesto lo siguiente:

- Casi todas las organizaciones (83.4%) **no** han analizado específicamente si el proveedor de servicios de cómputo en la nube tiene implementadas medidas para

Casi todas las organizaciones (83.4%) no han analizado si el proveedor de servicios de cómputo en la nube tiene implementadas medidas para prevenir y, en su caso, reaccionar ante ataques informáticos.

prevenir y, en su caso, reaccionar ante ataques informáticos, si bien el 33.2% sí se ha informado antes de contratar servicios de cómputo en la nube si el proveedor cuenta con procedimientos para descubrir e investigar ataques informáticos a sus redes y servidores.

- La mayoría de las organizaciones (66.6%) han indicado que, con independencia de las medidas adoptadas por el proveedor de servicios de cómputo en la nube, tiene medidas de seguridad para prevenir ataques informáticos.
- La mitad de las organizaciones (50%) saben que el proveedor de servicios de cómputo en la nube audita periódicamente que sus redes y sistemas de información sean seguros frente a ataques informáticos.
- También la mitad de las organizaciones afirma haberse informado sobre si la arquitectura del proveedor de servicios ha sido desarrollada conforme a estándares y normas para evitar intrusiones o ataques informáticos.
- Casi todas las organizaciones (83.4%) no han considerado si el proveedor de servicios de cómputo en la nube ha incluido en el contrato previsiones sobre responsabilidad en caso de que sea objeto de un ataque informático que produzca pérdida de datos o fuga de los mismos.
- También casi todas las organizaciones (83.4%) no han analizado si el proveedor de servicios de cómputo en la nube cuenta con alguna póliza de seguro frente a ciberataques.

8. Administraciones Públicas

Dos de las seis organizaciones participantes en el proyecto piloto son una dependencia o entidad de la Administración Federal, por lo que algunos aspectos específicos de la guía estaban dirigidos a las mismas. Las conclusiones obtenidas son las siguientes:

- Una de las organizaciones participantes sí incluye en las licitaciones públicas para la contratación de servicios previsiones

Resulta llamativo que ninguna de las dos organizaciones del sector público haya analizado si el proveedor de servicios de cómputo en la nube cuenta con alguna certificación, como por ejemplo la ISO/IEC 27001.

sobre interoperabilidad y finalización del contrato, habiéndose asegurado de que la contratación de servicios de cómputo en la nube cumpla con los requisitos aplicables a la contratación TIC en el sector público.

- Es relevante que ninguna de las dos organizaciones del sector público haya analizado si el proveedor de servicios de cómputo en la nube cuenta con alguna certificación, como por ejemplo la ISO/IEC 27001.
- Una de las organizaciones ha considerado si el proveedor de servicios de cómputo en la nube aplica criptografía para garantizar que la información se almacene (en reposo) y transmita de forma segura así como que los certificados electrónicos y la firma electrónica utilizada cumplan con las disposiciones de la Ley de Firma Electrónica Avanzada.
- También se observó que sólo una de las organizaciones se ha asegurado, en los términos de referencia de la licitación pública, que el proveedor de servicios de cómputo esté obligado a notificar cualquier cambio en los términos del servicio con anterioridad a su implementación y que tiene derecho a rescindir el contrato en su caso.
- Por último, una de las organizaciones participantes en el proyecto piloto ha previsto cláusulas en los términos de referencia en virtud de las que se asegure que el proveedor de servicios de cómputo en la nube responderá de la responsabilidad que le sea exigible con respecto a las cuestiones que surjan a lo largo de la prestación del servicio.